

| | | |
|---|--|---|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 1 de 17 |

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

2020 - 2023

El plan de tratamiento de riesgos de seguridad digital se formuló considerando la tecnología como herramienta transversal que soporta la prestación de servicios y ejecución de actividades misionales de cara al ciudadano, para generar valor y cumplir de manera efectiva las metas del Plan de Desarrollo Departamental.

**Grupo de Tecnologías de la Información
y la Comunicación**

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Versión: 1 |
| | | Página 2 de 117 |

Contenido

| | |
|---|-------------------------------------|
| Introducción | 4 |
| 1. Objetivo Estratégico | 4 |
| 1.1 Objetivo Específicos | 4 |
| 2. Alcance del documento | 5 |
| 3. Marco Normativo | 5 |
| 4. Rupturas estratégicas | 6 |
| 5. Entendimiento estratégico | 6 |
| 6. Resumen de inventario de infraestructura tecnológica de la Gobernación del Huila | 17 |
| 7. Descripción de los Sistemas de Información que Apoyan las Dependencias de la Entidad | 18 |
| 8. Descripción de Servicios de TI ofertados por el proceso de Gestión Tecnológica | 23 |
| 9. DIAGNÓSTICO DE ACTIVOS | 24 |
| 10. VALORACIÓN DE RIESGOS | 25 |
| 10.1 Identificación de Amenazas y Vulnerabilidades | 26 |
| 10.2 Identificación de Consecuencias | 27 |
| 10.3 Valoración de probabilidad | 27 |
| 10.4 Valoración de impacto | 28 |
| 10.5 Determinación de riesgo inherente | 29 |
| 10.6 Identificación de controles existentes | 35 |
| 11. TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | 35 |
| 11.1 Declaración de Aplicabilidad SOA | 38 |
| 11.2 Plan de Implementación de Controles para Mitigación de Riesgos | 52 |
| 12. CONCLUSIONES | 69 |
| 13. RECOMENDACIONES | 70 |
| 14. FUENTES DE INFORMACIÓN | 72 |
| ANEXOS | 74 |
| 1. Matrices de Identificación de Activos de Seguridad Digital | 74 |
| 2. Matrices de Identificación y Valoración de Riesgos de Seguridad Digital | 95 |
| 3. Matrices de Evaluación de Controles de Riesgos de Seguridad Digital | Error! Marcador no definido. |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 3 de 117 |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 4 de 117 |

Introducción

El Plan de Tratamiento de Riesgos de Seguridad Digital de la GOBERNACIÓN DEL HUILA es resultado de un ejercicio de planeación estratégica realizado por el proceso GESTION TECNOLÓGICA Y DE TELECOMUNICACIONES, para determinar acciones específicas que permitan gestionar los riesgos de seguridad de la información que se deben mitigar, e implantar los controles necesarios para minimizar los riesgos que persistan, propendiendo por el buen uso y la privacidad de los datos y la información que los ciudadanos brindan a la entidad para su tratamiento a través de diferentes trámites y servicios ofertados, y contribuir al cumplimiento de los objetivos estratégicos, y al incremento de los índices de transparencia en la gestión pública, y metas del plan de desarrollo.

El presente plan es formulado para la vigencia 2020 - 2023 y se encuentra enmarcado en los planes de desarrollo nacional y departamental, así como en los lineamientos del Modelo Integrado de Planeación y Gestión y la política de Gobierno Digital.

1. Objetivo Estratégico

Establecer estrategias y definir acciones que conlleven a la disminución de amenazas y vulnerabilidades asociadas a los activos de información de la GOBERNACIÓN DEL HUILA, y que pueden afectar o impedir el logro de los objetivos institucionales y estratégicos, fortaleciendo el enfoque preventivo referente a la seguridad y privacidad de la Información, y garantizando su confidencialidad, integridad y disponibilidad, bajo los lineamientos establecidos por el Ministerio TIC, y la norma NTC-ISO/IEC 27001:2013.

1.1 Objetivos Específicos

- Diagnosticar los activos de información de la GOBERNACIÓN DEL HUILA, de acuerdo a los lineamientos del Ministerio TIC y de la norma ISO/IEC 27001.
- Realizar la valoración de riesgos de seguridad de la información en la GOBERNACIÓN DEL HUILA, que incluya el análisis de causas, probabilidad de ocurrencia, y el nivel de impacto.
- Identificar brechas y no conformidades, para la posterior definición de controles y tratamiento de riesgos inherentes de seguridad de la información, de acuerdo a los lineamientos del Ministerio TIC y de la Norma ISO/IEC 27001.

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Versión: 1 |
| | | Página 5 de 117 |

2. Alcance del documento

El Plan de Tratamiento de Riesgos de Seguridad Digital inicia con un diagnóstico de los activos de información de cada uno de los procesos de gestión de la GOBERNACIÓN DEL HUILA, determinando su nivel de criticidad en base a la confidencialidad, integridad y disponibilidad de dichos activos. De igual manera, realiza un análisis de los riesgos de seguridad existentes de la GOBERNACIÓN DEL HUILA, en base a causas, probabilidad de ocurrencia, nivel de impacto, vulnerabilidades, amenazas relacionadas. Finalmente, presenta una identificación de brechas y no conformidades, para la posterior definición de controles y tratamiento a aplicar sobre las causas de los riesgos inherentes de seguridad de la información analizados para cada uno de los procesos de gestión de la GOBERNACIÓN DEL HUILA.

3. Marco Normativo

- Decreto 1008 del 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 415 de 2016, definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- Artículo 232 de la Ley 1450 de 2011, racionalización de trámites y procedimientos al interior de las entidades públicas.
- 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 2573 de 2014, reglamenta parcialmente la Ley 1341 de 2009 y que en el mismo decreto se define el componente de Privacidad y Seguridad de la información que incluye el modelo de seguridad y privacidad de la información (MSPI).
- Resolución N 2710 de 2017, por la cual se establecen lineamientos para la adopción del protocolo IPv6
- Decreto 1499 de 2017, definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
- 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 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 6 de 117 |

- 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.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- CONPES 3701 de 2011, Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016, Política Nacional de Seguridad digital.

4. Rupturas estratégicas

En este punto se determinan algunos de los paradigmas que debe romper la entidad para adelantar el proceso de implementación del sistema de gestión de seguridad y privacidad de la información:

- Falta de articulación entre el proceso de gestión TIC y los procesos de planeación y dirección, para contribuir en el desarrollo del plan estratégico institucional y la elaboración y alineación del plan estratégico de tecnologías de la información –PETI
- Fortalecer las capacidades para el uso y apropiación de TIC por parte de los funcionarios y contratistas en aspectos relacionados con la seguridad y privacidad de la información, que permita hacer uso eficiente y seguro de los activos de TI a su cargo, introduciendo así dichos aspectos en la cultura organizacional de la GOBERNACIÓN DEL HUILA.
- Implementar buenas prácticas y estándares para la gestión de seguridad y privacidad de la información, que permitan garantizar la continuidad en la prestación de los servicios, y cumpliendo los planes, políticas y objetivos estratégicos de la entidad.

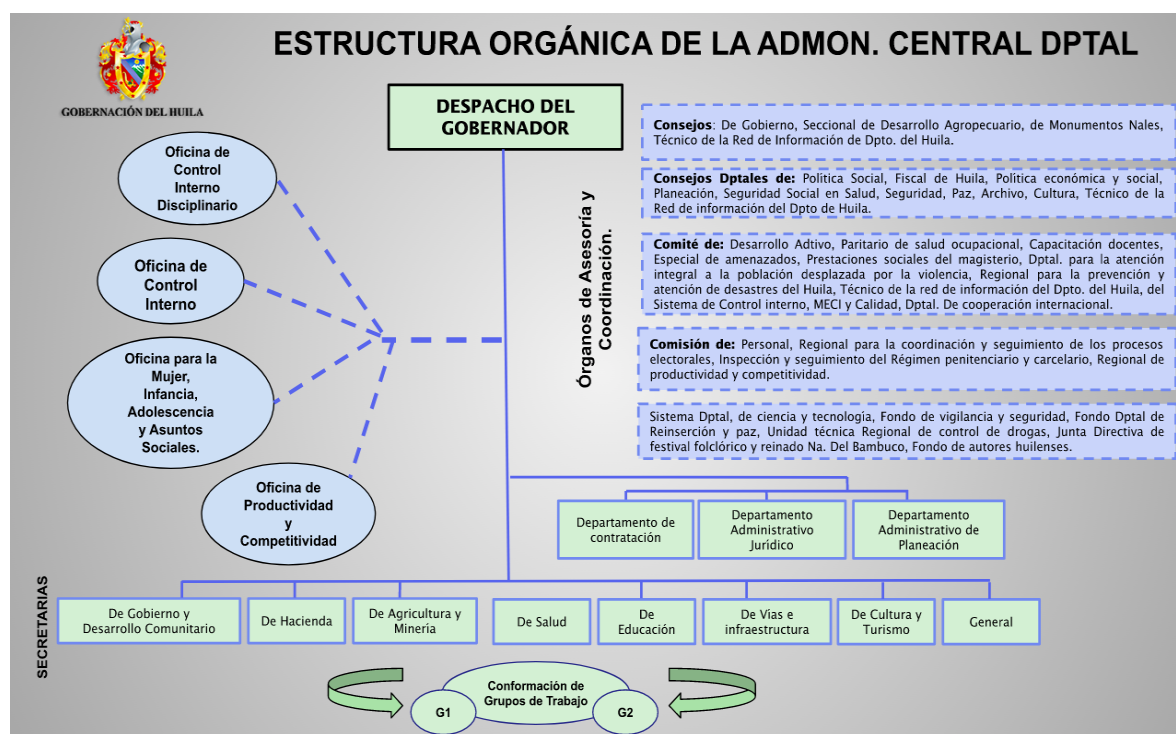
5. Entendimiento estratégico

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Versión: 1 |
| | | Página 7 de 117 |

Misión: El Departamento del Huila, según la Constitución Política, tiene autonomía para la administración de los asuntos seccionales y la planificación y promoción del desarrollo económico y social de su territorio. Ejerce funciones administrativas de coordinación, de complementariedad de la acción municipal, de intermediación entre el Gobierno Nacional y los Municipios y prestador de los servicios determinados por la Constitución y la ley".

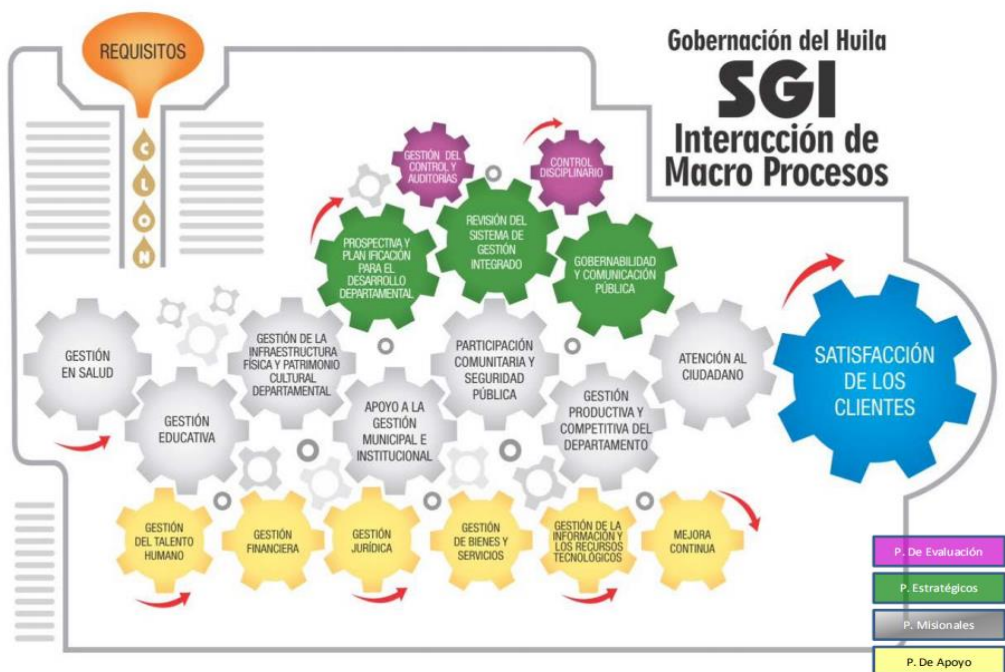
Visión: En el año 2020 el Huila será el corazón verde de Colombia, pacífico, solidario y emprendedor; líder de una región dinámica donde florecen los sueños de todos.

Organigrama:



Mapa de procesos:

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 8 de 117 |



Portafolio de servicios que presta la Gobernación del Huila en relación a sus procesos y grupos de valor

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | | |
|---|---|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|---------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO | ORGANISMOS PRIVADOS |
| GESTION A LA DIRECCION DEL SISTEMA GENERAL DE | Direcciones locales de salud en el Departamento orientados para asumir las competencias en el | | | X | X | X | | X | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 9 de 117 |

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | | |
|---|---|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|---------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO | ORGANISMOS PRIVADOS |
| SEGURIDAD SOCIAL EN SALUD | componente de dirección del S.G.S.S.S | | | | | | | | |
| | IPS acompañadas en el proceso del saneamiento de los aportes patronales | | | X | X | X | | X | |
| GESTION DEL ASEGURAMIENTO AL SISTEMA GENERAL DE SEGURIDAD SOCIAL EN SALUD | Sistema de aseguramiento en salud asistido, vigilado y controlado | X | | X | X | X | | X | |
| GESTIÓN EN LA PRESTACIÓN DE LOS SERVICIOS DE SALUD | Prestadores de servicios de salud inscritos y habilitados. | | | | X | X | | | |
| | Recurso humano en salud inscrito mediante certificado y autorizado mediante acto administrativo | | | X | | | | | |
| | Orden de prestación de servicios de salud y/o ayudas técnicas | | | X | | | | | |

| | | |
|---|---|---|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 10 de 117 |

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | | |
|--------------------------|---|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|---------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO | ORGANISMOS PRIVADOS |
| | Urgencias, emergencias y desastres, coordinados y regulados oportunamente | | | | | X | | | X |
| | Órganos sólidos asignados según los lineamientos de la coordinación Nacional de la red de donación y trasplante | | | | | X | | | |
| | Proyectos de inversión para infraestructura, dotación y equipos de salud viabilizados | X | | X | | X | | | |
| | Red de servicios de salud estructurada y en funcionamiento. | | | X | | X | | | |
| | Medicamentos entregados | | | X | | | | | |
| GESTION EN SALUD PUBLICA | Población huilense con bajos índices de morbilidad y mortalidad en eventos de interés en salud pública | X | | X | | X | | X | |

| | | |
|---|--|---|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 11 de 117 |

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | | |
|--|---|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|---------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO | ORGANISMOS PRIVADOS |
| | Actores del SGSSS asistidos y capacitados en los programas contemplados en el Plan de Salud Pública | | | X | X | X | | X | |
| | Resultados de laboratorio de salud pública | | | X | X | X | | X | |
| GESTIÓN DEL TALENTO HUMANO ASIGNADO AL SECTOR EDUCATIVO DEL DEPARTAMENTO | Estudio Técnico de Planta de cargos presentada al MEN | | | | | | X | | |
| | Decreto de adopción de planta de cargos | | | | | | X | | |
| | Decreto de Distribución de planta de cargos | | | X | | | | | |
| | Actos administrativos de nombramiento de personal | | | X | | | | | |
| | Manual de funciones y perfiles para Personal Administrativo de la Instituciones Educativas | | | | | | X | | |
| GESTIÓN DE LA INSPECCIÓN Y VIGILANCIA DE | Decreto de Reglamento Territorial de Inspección y vigilancia y Resolución del | | | X | | | X | X | |

| | | |
|---|--|---|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 12 de117 |

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | | |
|--|---|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|---------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO | ORGANISMOS PRIVADOS |
| LOS ESTABLECIMIENTOS EDUCATIVOS | Plan operativo anual de Inspección y vigilancia | | | | | | | | |
| | Informe de resultados de las visitas a los establecimientos educativos | X | | X | | | X | X | |
| | Actos administrativos de legalización de los establecimientos educativos oficiales y no oficiales | | | X | | | X | | |
| GESTIÓN DE LA COBERTURA DEL SERVICIO EDUCATIVO | Niños, niñas y jóvenes en edad escolar matriculados, atendidos y con el cupo garantizado en el servicio educativo | | | X | | | | | |
| | Decreto que define la gestión de la cobertura para el proceso de matrícula en los municipios no certificados del Huila sector oficial y no oficial. | | X | X | | | | | |

| | | |
|---|--|---|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 13 de117 |

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | | |
|---|--|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|---------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO | ORGANISMOS PRIVADOS |
| GESTIÓN DE LA CALIDAD DEL SERVICIO EDUCATIVO EN EDUCACIÓN PRE-ESCOLAR, BÁSICA Y MEDIA | Plan de apoyo al mejoramiento _ PAM | | | | | | X | X | |
| | Asistencia técnica para el mejoramiento del PEI y PMI | | | | | | X | | |
| | Plan de formación y desarrollo profesional de educadores | | | | | | X | | |
| | Coordinación interinstitucional para la ejecución de procesos de articulación | | | | | | | | |
| GESTIÓN Y CONSTRUCCIÓN DE LA INFRAESTRUCTURA | Vías e Infraestructuras construidas, rehabilitadas mejoradas y conservadas | | X | X | | | | | |
| | Necesidades identificadas y priorizadas | | | X | | | | | |
| | Entidades centralizadas y descentralizadas apoyadas en el mejoramiento de su infraestructura | | | | | | | X | |

| | | |
|---|--|---|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 14 de117 |

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | | |
|--|--|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|---------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO | ORGANISMOS PRIVADOS |
| VALORACIÓN, PROTECCIÓN Y DIFUSIÓN DEL PATRIMONIO CULTURAL | Patrimonio cultural Valorado, Protegido y Difundido | | X | X | | | | | |
| ASISTENCIA TECNICA Y ASESORIA | Funcionarios y servidores públicos asesorados técnicamente | | X | | | | | X | |
| GESTION DEL RIESGO DE DESASTRES | Estudios de conocimiento del riesgo. | | | X | | | | X | X |
| | Obras de prevención y mitigación | | | X | | | | | |
| | Apoyo humanitario (alimentario y no alimentario), y/o económico. | | | X | | | | | |
| | Asistencia y visitas técnicas | | X | | | | | | |
| SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN Y DESEMPEÑO DE LOS ENTES MUNICIPALES | Documento de medición y análisis del desempeño integral municipal. | | X | | | | | | |

| | | |
|---|--|---|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 15 de117 |

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | |
|---|---|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO |
| SEGURIDAD Y ORDEN PUBLICO | Actividades coordinadas y articuladas con la fuerza pública y organismos de seguridad del estado para la preservación y mantenimiento del orden público | | | X | | | | |
| ASISTENCIA EN LEGISLACION COMUNITARIA Y PARTICIPACION CIUDADANA | Comunidad asistida y capacitada en legislación comunitaria | | | X | | | | X |
| | Entidades y organizaciones comunitarias Controladas y vigiladas | | | | | | | X |
| | Personerías Jurídicas y dignatarios reconocidos | | | X | | | | X |
| | *Dignatarios Inscritos. *Certificación de Personería Jurídica y Representación Legal. *Reforma de Estatutos. *Reconocimiento de Personería Jurídica. | | | X | | | | X |

| | | |
|---|--|---|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 16 de117 |

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | | |
|---|--|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|---------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO | ORGANISMOS PRIVADOS |
| | *Certificados de Existencia y Representación Legal | | | | | | | | |
| | Apertura y Registro de Libros | | | | | | | | X |
| | Cancelación de Personería Jurídica. | | | X | | | | | |
| ASISTENCIA SOCIAL A POBLACION VULNERABLE | Población Vulnerable beneficiada mediante programas sociales | | | X | | | | | |
| ADECUACION Y ORDENAMIENTO A LA INFRAESTRUCTURA PRODUCTIVA AGROPECUARIA, AMBIENTAL Y MINERA DEL DPTO | Infraestructura productiva del departamento orientada, desarrollada y modernizada. | | X | X | | | | | |
| FORMACION Y PROMOCION DE LOS DESTINOS TURISTICOS DEL DEPARTAMENTO | Destinos turísticos estructurados, cualificados y promocionados | | X | X | | | | | X |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 17 de 117 |

| PROCESO | PRODUCTOS O SERVICIOS | GRUPOS DE VALOR | | | | | | | |
|-----------------------|--|------------------|----------|-----------|------------------------------|--------------------------|---------------------------------|------------------------------|---------------------|
| | | ENTES DE CONTROL | ALCALDES | COMUNIDAD | PROVEEDORES Y PRESTADORES DE | EMPRESAS, SOCIEDADES DEL | ESTABLECIMIENTOS EDUCATIVOS Y/O | ENTIDADES DEL SECTOR PÚBLICO | ORGANISMOS PRIVADOS |
| ATENCION AL CIUDADANO | Respuestas a las Comunicaciones oficiales, PQR, y requerimientos realizados a través del PBX, telefax 8712705 o de la línea gratuita 01800968716, atendidos. | | | X | | | | X | |
| | Pasaporte | | | X | | | | | |

6. Resumen de inventario de infraestructura tecnológica de la Gobernación del Huila

El inventario de la infraestructura tecnológica de la Gobernación del Huila incluye la información (marca, modelo, año de adquisición, uso, y ubicación) sobre equipos de cómputo, impresoras, escáners, UPS, servidores, access point, sistemas de información y licenciamiento propiedad de la entidad, y se puede resumir en las siguientes cantidades:

- Equipos de Cómputo: 709
- Impresoras: 141
- Escáner: 51
- UPS: 34
- Servidores: 16
- Switches: 58
- Access Point: 39
- Sistemas de Información: 13
- Licenciamiento:
- Microsoft Servers y Clientes: 2234

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 18 de 117 |

- Microsoft Office: 937
- Gestor de Base de Datos: 2
- Antivirus: 720
- Firewall: 2

7. Descripción de los Sistemas de Información que Apoyan las Dependencias de la Entidad

El catálogo de sistemas de información presenta cada una de las soluciones tecnológicas que soportan los procesos de la entidad y una descripción de los mismos, con base en sus funcionalidades.

| Nombre | Descripción | Categoría/Usos | Tipo |
|---|--|----------------|------------------|
| SISTEMA DE INFORMACIÓN FINANCIERO Y ADMINISTRATIVO-SIFA (Módulos: Presupuesto, Tesorería, Contabilidad, Nómina, Almacén, Seguridad, Planeación y Trazabilidad) | Este sistema apoya la automatización de procesos de administración del recurso financiero, contabilidad pública Departamental, ejecución y control del presupuesto Departamental así como los procesos de administración de nómina y almacén. | Administrativo | Cliente/Servidor |
| | El módulo de Presupuesto y Tesorería permiten el manejo de las operaciones que realiza la entidad, con el manejo de este instrumento de desarrollo anual tanto para ingresos como para egresos, apropiaciones, disponibilidades, ejecución, compromisos y órdenes de pago. | | |
| | El módulo de Contabilidad es el puerto donde llegan todas las transacciones de los otros módulos que componen el SIFA© y que hace que el sistema sea confiable, seguro | | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 19 de 117 |

| | | | |
|--|--|--|--|
| | para la presentación de los informes concernientes a esta área. | | |
| | El módulo de Nómina facilita el manejo de las operaciones que realizan la entidad en esta área como son los pagos a los empleados, sus historias laborales, certificaciones. | | |
| | El módulo de Almacén permite el manejo manejo de las operaciones que realiza la entidad en esta área como son los inventarios, activos fijos, elementos devolutivos, salidas y entradas. | | |
| | El módulo de Planeación permite establecer la ejecución presupuestal, en términos financieros, de los planes de desarrollo establecidos por el Departamento Administrativo de Planeación – DAP. | | |
| | El módulo de Trazabilidad facilita el seguimiento y control de facturas que son presentadas por entidades prestadoras de servicios de salud (EPS, IPS, etc.) por medio de archivos RIPS (Registro Individual de Prestación de Servicios de Salud) y archivos de Reco-bros. | | |
| | Mediante el módulo de seguridad se administra los accesos a cada una de las opciones de todos los módulos, así como la creación de usuarios y asignación de permisos. | | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 20 de 117 |

| | | | |
|--|---|----------------|---|
| SISTEMA DE INFORMACIÓN TRIBUTARIO - CITY | Sistema de información que apoya la Gestión y Control de la Renta Departamental: Impuestos de vehículos, registro, otras rentas y registro cámara de Comercio | Administrativo | Cliente/Servidor Interfaz web para liquidaciones y pago en línea |
| PORTAL WEB INSTITUCIONAL - Nexura Platform e-gov | Solución enfocada a interacción, participación, trámites y servicios en línea que posibilita cambiar el modelo de comunicación ciudadano-estado | Misional | Web |
| PORTAL DE CONTRATACIÓN | Sistema para la publicación, seguimiento y convocatoria de los procesos de contratación que adelanta la Entidad | Administrativo | Web |
| Sistema de Gestión Documental - Sistema de Comunicaciones Oficiales (Módulo de ventanilla única de atención al ciudadano, módulo de archivo) | Módulo de Ventanilla Única: Proceso de radicación de todos los documentos - comunicaciones (peticiones, quejas, reclamos, sugerencias, felicitaciones y denuncias) de entrada, salida, e internos, PQRSFD de la Entidad. Gestiona flujos documentales de la Entidad y genera informes de gestión de la atención al ciudadano. | Misional | Web |
| | Módulo de Archivo: Almacena, clasifica y conserva de forma adecuada todos los documentos electrónicos que se gestionan en la Entidad y también los documentos de archivos físicos que se indexen y clasifiquen a través de procesos de digitalización. | | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 21 de 117 |

| | | | |
|---|--|----------|--------------------------|
| Sistema Integral de Salud - SISHUILA (Módulo de aseguramiento SSGSS, Módulo de Autorizaciones, Módulo regulador de urgencias y emergencias CRUEH, Módulo 4505, Módulo de laboratorio) | Sistema de información que apoya el desarrollo de los procesos Gestión a la Dirección del Sistema General de Seguridad Social en Salud, Gestión del aseguramiento al Sistema General de Seguridad Social en Salud y Gestión en Salud Pública y laboratorio. | Misional | Web |
| Sistema de Información Geográfica del Departamento del Huila - SIGDEHU | El Sistema de Información Geográfica del Huila - SIGDEHU, tiene por objetivo tener la cartografía actualizada y real (base de datos Georreferenciada, que permite visualizar, digitalizar, procesar, desplegar y reportar información temática y sintetizada en forma de cartografía digital). Esto ayuda a tomar decisiones en materia de ordenamiento territorial para los municipios y el departamento. | Misional | Aplicación de escritorio |
| Sistema de Información Regional - SIRHUILA | A través del Sistema de Información Regional del Departamento del Huila se busca apoyar la planificación integral de mediano y largo plazo para la ejecución y evaluación del departamento y los municipios; de tal forma que permita dinamizar el desarrollo regional y la inversión pública ejerciendo control social. Además, el sistema sirve de apoyo ante las necesidades de información de las entidades y usuarios sobre diferentes aspectos del departamento del Huila. | Misional | Web |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 22 de 117 |

| | | | |
|---|--|----------|-----|
| Sistema de información Turística y Cultural del Huila - SITYC | Es el Sistema de información Turística y Cultural del Huila, una herramienta tecnológica que a través del uso de las TIC's, tiene como objetivo el fortalecimiento del desarrollo sostenible del sector turístico y cultural. Representa la alianza pública privada en búsqueda de mejorar la competitividad regional, valorando la importancia del trabajo en equipo y aportando a procesos de investigación, desarrollo e innovación en el presente y a futuro. El SITYC es una plataforma multi-servicios, que integra funciones de estadística, divulgación y promoción. | Misional | Web |
| Sistema de Información de Procesos Judiciales SIPROJ | Este sistema le permite a la Gobernación, conocer el estado en el que se encuentran los procesos judiciales iniciados por la entidad y en contra de la misma. | Misional | Web |
| El Sistema de Información de Personas Jurídicas SIPEJ | El Sistema de Información de Personas Jurídicas SIPEJ es un aplicativo que cumple la función de administrar, hacer seguimiento y vigilar el cumplimiento de su razón social, parámetros, estatutos, funciones y objeto social a todas aquellas entidades sin ánimo de lucro, que existen a lo largo y ancho de todo el departamento del Huila. | Misional | Web |
| Sistema de Información de Control Interno Disciplinario SIID | El Sistema de Información de Control Interno Disciplinario SIID, apoya a los operadores disciplinarios, en el seguimiento a los procesos basados en la investigación de conductas que no se ajustan a las normas de los servidores públicos de la Gobernación del Huila. | Misional | Web |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 23 de 117 |

| | | | |
|-------------|---|----------|-----|
| TBG - Huila | Este es sistema está basado en Balanced Scorecard y está enfocado en seguimiento del plan de desarrollo, la información que arroja permite evaluar y proyectar políticas públicas e inversiones | Misional | Web |
|-------------|---|----------|-----|

8. Descripción de Servicios de TI ofertados por el proceso de Gestión Tecnológica

El proceso de GESTION TECNOLÓGICA Y DE TELECOMUNICACIONES cuenta con el siguiente listado de servicios TI en oferta para el cliente interno y apoyo a los diferentes procesos de la entidad.

| | Servicio | Descripción |
|---|------------------------|--|
| 1 | Internet | Conexión a internet para el edificio central y sedes de la Gobernación del Huila |
| 2 | Soporte a usuarios | Asistencia técnica, de manera presencial o virtual, a equipos informáticos de puestos de trabajo |
| 3 | Conexión red WiFi | Acceso a la red de datos a través de conexión inalámbrica para equipos de la entidad y usuarios externos |
| 4 | Gestión de usuarios | Creación y administración de usuarios del domino de la entidad |
| 5 | Correo electrónico | Medio de intercambio externo e interno de información institucional, a través de internet de manera confiable y fácil - Creación y gestión de cuentas |
| 6 | Extranet | Portal de información y comunicación interno, mediante el cual se tiene acceso a información institucional y herramientas que apoyan la gestión de las diferentes dependencias |
| 7 | Mensajería instantánea | Medio de comunicación a través de internet, tipo chat, que permita la comunicación en tiempo real y de manera segura |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 24 de 117 |

| | | |
|----|--|---|
| 8 | Página web | Publicación de información en el portal oficial de comunicación, transparencia e interacción de la entidad, dirigido a la ciudadanía y a otras entidades www.huila.gov.co |
| 9 | Sistemas de información | Gestión de requerimientos no funcionales de los diferentes sistemas de información que soportan procesos de la entidad |
| 10 | Soporte a la operación del sistema financiero SIFA | Apoyo técnico a la gestión de usuarios y operación del SIFA |
| 11 | Soporte a la operación del sistema de Comunicaciones Oficiales | Apoyo técnico a la gestión de usuarios y operación del Sistema de Comunicaciones Oficiales |
| 12 | Telefonía fija | Medio de comunicación por voz a través de la red de telefonía fija que permite la comunicación entre dependencias y con el exterior - Soporte y mantenimiento |
| 13 | Backup | Almacenamiento y respaldo de información relevante que respalde procesos de la entidad |
| 14 | Conceptos técnicos | Elaboración conceptos técnicos relacionados con las adquisiciones tecnológicas en hardware, sistemas de información y aplicaciones |

9. DIAGNÓSTICO DE ACTIVOS

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la GOBERNACIÓN DEL HUILA para su funcionamiento.

Es necesario identificar los activos 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.

Para la generación de este inventario, se realizaron los siguientes pasos:

| | | |
|---|--|---|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 25 de 117 |

- **Listar y clasificar activos por cada proceso:** En cada proceso de gestión, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno. Así mismo, cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza como, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros.
- **Identificar el dueño y el custodio de los activos:** Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.
- **Determinar criticidad del activo:** En primer lugar, se debe realizar 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 debe evaluar 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.
- **Identificar infraestructuras críticas cibernéticas - ICC:** Se debe identificar y reportar a las instancias y autoridades respectivas en el Gobierno nacional si la Gobernación del Huila posee ICC. Un activo es considerado infraestructura crítica 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.

10. VALORACIÓN DE RIESGOS

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: "Integridad, confidencialidad o disponibilidad"

Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Cabe añadir que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 26 de 117 |

10.1 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).

Cabe añadir que la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

En base a los pasos antes descritos, la Gobernación del Huila estableció el siguiente formato para generar tanto su procedimiento de identificación y levantamiento de inventario de activos en cada uno de los procesos de gestión, como la identificación de amenazas, posibles causas y vulnerabilidades existentes en cada uno de los activos (Ver Anexo 1. Matrices de Identificación de Activos de Seguridad Digital).

| 1 | 2 | 3 | 4 | 5 | | | 6 |
|---|----------------|---------------------------------|--|------------------------------|------------|----------------|-----------------------|
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Criticidad del activo |
| | | | | Confidencialidad | Integridad | Disponibilidad | |
| Base de datos de calidad de datos | Información | Entidades propietarias del dato | Líder de proceso Sistemas de Información | 3 | 1 | 1 | Alta |
| Base de datos de seguridad de datos | Información | Entidades propietarias del dato | Líder de proceso Sistemas de Información | 3 | 1 | 1 | Alta |

| | | | |
|---|--|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 | |
| | | Fecha Aprobación: 31 de Enero de 2020 | |
| | | Versión: 1 | |
| | | Página 27 de 117 | |

| 7 | | | | 8 | | | 9 | 10 |
|---------------------|--------------|------------------|-----------------------|---|------|------|-------------------------------------|---------------|
| Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| Naturales | Industriales | Errores y fallas | Ataques intencionados | | | | | |
| N.A. | N.A. | N.A. | Corrupción de datos | Ausencia formal para la supervisión de registro de SGSI | N.A. | N.A. | N.A. | N.A. |
| N.A. | N.A. | Error de uso | N.A. | Uso incorrecto de software y hardware | N.A. | N.A. | N.A. | N.A. |

10.2 Identificación de Consecuencias

Para cada uno de los riesgos identificados, se identifican posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano).

10.3 Valoración de probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 28 de 117 |

| NIVEL | DESCRIPTOR | DESCRIPCIÓN | FRECUENCIA |
|-------|-------------|---|--|
| 5 | Casi seguro | Se espera que el evento ocurra en la mayoría de las circunstancias | Más de 1 vez al año. |
| 4 | Probable | Es viable que el evento ocurra en la mayoría de las circunstancias | Al menos 1 vez en el último año. |
| 3 | Posible | El evento podrá ocurrir en algún momento | Al menos 1 vez en los últimos 2 años. |
| 2 | Improbable | Es poco probable que el evento en algún momento | Al menos 1 vez en los últimos 5 años. |
| 1 | Rara vez | El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales) | No se ha presentado en los últimos 5 años. |

10.4 Valoración de impacto

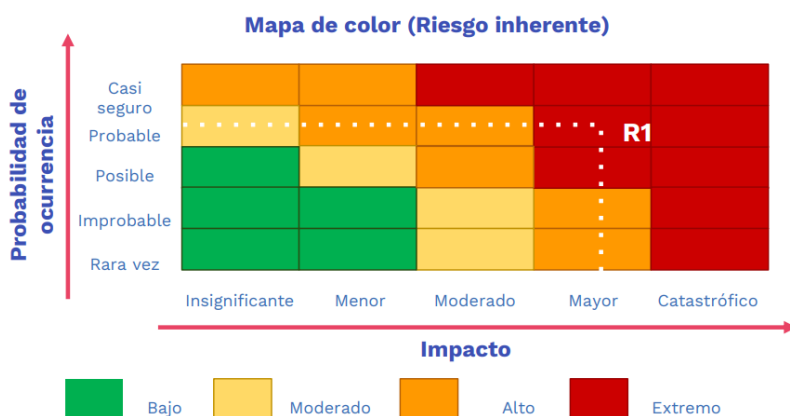
El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

| Nivel | Valor de Impacto | Impacto (consecuencias) cuantitativo | Impacto (consecuencias) cualitativo |
|----------------|------------------|---|---|
| INSIGNIFICANTE | 1 | Afectación \geq X% de la población Afectación \geq X% del presupuesto anual de la entidad. No hay Afectación medioambiental | Sin afectación de la integridad Sin afectación de la disponibilidad Sin afectación de la confidencialidad |
| MENOR | 2 | Afectación \geq X% de la población Afectación \geq X% del presupuesto anual de la entidad Afectación leve del Medio Ambiente requiere de \geq X días de recuperación | Afectación leve de la integridad Afectación leve de la disponibilidad Afectación leve de la confidencialidad |
| MODERADO | 3 | Afectación \geq X% de la población Afectación \geq X% del presupuesto anual Afectación leve del Medio Ambiente requiere de \geq X semanas de recuperación | Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros |
| MAYOR | 4 | Afectación \geq X% de la población Afectación \geq X% del presupuesto anual de la entidad Afectación importante del Medio Ambiente que requiere de \geq X meses de recuperación | Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros |
| CATASTRÓFICO | 5 | Afectación \geq X% de la población Afectación \geq X% del presupuesto anual de la entidad Afectación muy grave del Medio Ambiente que requiere de \geq X años de recuperación | Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Versión: 1 |
| | | Página 29 de 117 |

10.5 Determinación de riesgo inherente

Se identifican los riesgos inherentes o subyacentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso. Se toma la calificación de probabilidad resultante del paso anterior, que para este ejemplo se tomará la probabilidad de ocurrencia en “probable” y la calificación de impacto en “mayor”, se ubica la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel extremo – color rojo (R1), así se podrá determinar el riesgo inherente.



Con base en el proceso antes descrito para la identificación y valoración de riesgos de seguridad digital, la Gobernación del Huila estableció el siguiente formato para generar tanto su procedimiento de identificación y análisis de riesgos en cada uno de los procesos de gestión, como la identificación de consecuencias, probabilidad de ocurrencia, y nivel de impacto para cada riesgo identificado (Ver Anexo 2. Matrices de Identificación y Valoración de Riesgos de Seguridad Digital).

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 30 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | |
|--|--|---|---|----------------------|------------------------------|---|---|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 7 | Gestión de la inspección y vigilancia de los establecimientos educativos | Pérdida de integridad de información pública clasificada y servicios al ciudadano del proceso | seguridad digital | Otros | Directivo y profesional | Cambios de personal directivo docente, generando falta de continuidad de lineamientos directivos y de gobierno en los establecimientos educativos | Incumplimiento en la entrega de informes de gestión a la secretaria de educación y ministerio |
| | | | | | | Cambios normativos frecuentes en todos los procesos, generando desactualización permanente | Retrasos en la generación de actos administrativos |
| | | | | | | Incumplimiento de los plazos establecidos para la implementación de las acciones de mejora continua en los procesos | Posible apertura de proceso disciplinario por incumplimiento en la implementación de las acciones de planes de mejoramiento |
| | | | | | | Incumplimiento de los plazos establecidos para la expedición de actos administrativos | Retrasos en la habilitación de servicios de establecimientos educativos |
| | | | | | | Cambios normativos frecuentes en todos los procesos, generando desactualización permanente | Retrasos en la generación de actos administrativos |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 31 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | |
|--|--|---|---|----------------------|------------------------------|--|---|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| | | | | | | para la elaboración de actos administrativos | |
| | | | | | | Errores en diligenciamiento de actos administrativos en establecimientos educativos para trámites de apostillaje | Retrasos en el servicio de apostillaje de actos administrativos |
| | | | | | | Modificación de firmas, adulteración y expedición ilegal de documentos | Posible apertura de proceso disciplinario por incumplimiento en la implementación de las acciones de planes de mejoramiento |
| | | | | | | Enfermedades de origen laboral | Incumplimiento en la entrega de informes de gestión a la secretaria de educación y ministerio |
| 8 | Gestión de la inspección y vigilancia de los establecimientos educativos | Pérdida de disponibilidad de servicios, herramientas tecnológicas e información pública clasificada del proceso | seguridad digital | Otros | Nivel Directivo | Demora en la aplicación de los cambios de los procesos, documentos y flujos de información | Incumplimiento del plan anual de visitas de inspección y vigilancia |
| | | | | | | Cambio del administrador del portal web | Retrasos en la publicación de actos administrativos |
| | | | | | | Errores en diligenciamiento de actos administrativos en | Retrasos en el servicio de apostillaje de actos administrativos |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 32 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | |
|--|-----------------------|---|---|----------------------------|---------------------------------------|---|--|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| | | | | | | establecimientos educativos para trámites de apostillaje | |
| | | | | | | Modificación de firmas, adulteración y expedición ilegal de documentos | Posible apertura de proceso judicial por falsificación de documento público |
| | | | | | | Enfermedades de origen laboral | Incumplimiento en la entrega de informes de gestión a la secretaria de educación y ministerio |
| | | | | | | Facilidad de editar la herramienta ofimática | Incompletitud de información de visitas a establecimientos educativos |
| | | | | | | Falta de recursos para renovación y actualización de equipos de cómputo | Incumplimiento en la entrega de informes de gestión a la secretaria de educación y ministerio |

| | | |
|---|---|---|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043- PL02</p> |
| | <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | <p>Fecha Aprobación: 31 de Enero de 2020</p> <p>Versión: 1</p> <p>Página 34 de 117</p> |



CODIGO: SGN-C043-PL02

| |
|--|
| Fecha Aprobación: 31 de Enero de 2020 |
|--|

Versión: 1

Página 34 de 117

| | | | | | | | | | | | | | |
|---|---|---------|----|-------------|--------|-------|----|-------|--------------|--------------|---|---|---------|
| 4 | 4 | Extremo | No | Sin control | | | | Débil | No disminuye | No disminuye | 4 | 4 | Extremo |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 35 de 117 |

10.6 Identificación de controles existentes

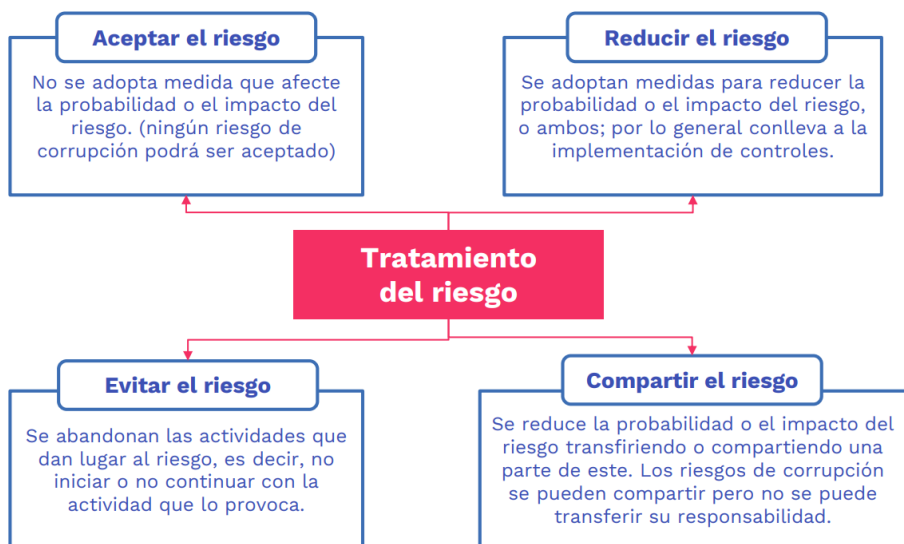
Una vez establecidos y valorados los riesgos inherentes, se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios. Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados, se puede consultar el Anexo A de la Norma ISO/IEC 27001:2013 (Dominios y Objetivos de Control de Seguridad) como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad digital que están enunciados en dicho anexo.

En este caso se utiliza de manera preliminar una matriz de evaluación de controles estandarizada institucionalmente (Ver Matriz de Evaluación de Controles en la página siguiente), a fin de valorar su impacto en la mitigación de riesgos o en las condiciones que contribuyen a la materialización de los riesgos de seguridad digital. Posteriormente se realiza la verificación de controles con base en el Anexo A de la Norma ISO/IEC 27001:2013, para validar alineación de controles existentes con los requerimientos establecidos en dicha norma técnica.



11. TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

Una vez se han identificado los riesgos, la Gobernación del Huila debe definir el tratamiento para cada uno de los riesgos analizados y evaluados. El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la Gobernación del Huila puede tener en cuenta las siguientes opciones planteadas en la Política Institucional de Gestión de Riesgo: Evitar, aceptar, compartir o reducir el riesgo.

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Versión: 1 |
| | | Página 36 de 117 |



| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 37 de 117 |

| <div></div> <div>GOBERNACION DEL HUILA</div> | | | <div></div> <div>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</div> | | | | | | | | | | | CODIGO: SGN-C048-G001-F03 | | | |
|---|---|---|--|---|---|--|---|--|--|---|---|---|---|--|----------------------------|---|--|
| | | | EVALUACIÓN DE CONTROLES PARA RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL | | | | | | | | | | | FECHA DE APROBACIÓN: 04/06/2019 | | | |
| | | | | | | | | | | | | | | VERSIÓN: 1 | | | |
| | | | | | | | | | | | | | | PÁGINA: 1 DE 1 | | | |
| ¿Tiene Control? | Identificación del Riesgo | Causa | ¿Tipo de Control? (Automático o Manual) | ¿Responsable asignado a la ejecución del control? Asignado=15 No asignado=0 | Cargo del responsable de ejecutar el control o nombre del sistema o aplicación automático | Responsable con autoridad y segregación de funciones en la ejecución del control? Adecuado=15 Inadecuado=0 | La periodicidad en la ejecución del control? Oportuna=15 Inoportuna=0 | Tipo de periodicidad del control (diario, semanal, quincenal, trimestral, anual, etc.) | El propósito del control ayuda (causas) a: Prevenir=15 Detectar=10 Corregir = 0 | Describe cuál es el propósito del control | Cómo se utiliza la actividad de control? Confiable=15 No confiable=0 | Cómo se realiza la actividad de control | Se investigan y resuelven oportunamente las observaciones o desviaciones? Si=15 NO =0 | Evidencia de la ejecución del control? Completa=10 Incompleta=5 No existe=0 | PUNTAJE TOTAL DE CONTROLES | Resultado - Peso en la evaluación del diseño del control Fuerte (96-100) Moderado (86-95) Débil (0-85) | |
| No | Pérdida de integridad de información pública clasificada y servicios al ciudadano del proceso | Cambios de personal directivo docente, generando falta de continuidad de lineamientos directivos y de gobierno en los establecimientos educativos | | | | | | | | | | | | | 0 | Sin control | |
| No | | Cambios normativos frecuentes en todos los procesos, generando desactualización permanente | | | | | | | | | | | | | 0 | Sin control | |
| Si | | Incumplimiento de los plazos establecidos para la implementación de las acciones de mejora continua en los procesos | Manual | 15 | Profesional universitario designando | 15 | 15 | Mensual | 15 | Realizar seguimiento permanente según lo establecido en el plan de acción derivado del plan de mejoramiento | 15 | Visitas y acompañamiento para seguimiento y verificación de cumplimiento del plan de mejoramiento | 15 | 5 | 95 | Moderado | |
| No | | Incumplimiento de los plazos establecidos para la expedición de actos administrativos | | | | | | | | | | | | | 0 | Sin control | |
| No | | Cambios normativos frecuentes en todos los procesos, generando desactualización permanente para la elaboración de actos administrativos | | | | | | | | | | | | | 0 | Sin control | |
| No | | Errores en diligenciamiento de actos administrativos en establecimientos educativos para trámites de apostillaje | | | | | | | | | | | | | 0 | Sin control | |
| No | | Modificación de firmas, adulteración y expedición ilegal de documentos | | | | | | | | | | | | | 0 | Sin control | |
| No | | Enfermedades de origen laboral | | | | | | | | | | | | | 0 | Sin control | |
| No | Pérdida de disponibilidad de servicios, herramientas tecnológicas e información pública clasificada del proceso | Demora en la aplicación de los cambios de los procesos, documentos y flujos de información | | | | | | | | | | | | | 0 | Sin control | |
| No | | Cambio del administrador del portal web | | | | | | | | | | | | | 0 | Sin control | |
| No | | Errores en diligenciamiento de actos administrativos en establecimientos educativos para trámites de apostillaje | | | | | | | | | | | | | 0 | Sin control | |
| No | | Modificación de firmas, adulteración y expedición ilegal de documentos | | | | | | | | | | | | | 0 | Sin control | |
| No | | Enfermedades de origen laboral | | | | | | | | | | | | | 0 | Sin control | |
| No | | Facilidad de editar la herramienta ofimática | | | | | | | | | | | | | 0 | Sin control | |
| Si | Falta de recursos para renovación y actualización de equipos de cómputo | Manual | 15 | Profesional universitario designando | 15 | 15 | Anual | 15 | Gestión de recursos mediante oficios y proyectos de POAIV | 15 | Realización de oficios y formulación de proyectos en el POAIV para vigencias siguientes | 0 | 10 | 85 | Débil | | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 38 de 117 |

11.1. Declaración de Aplicabilidad SOA

| | |
|--|---------------------------------|
| Declaración de Aplicabilidad | Vigente hasta el: 31/01/2020 |
| <p>La presente declaración se establece sobre los controles que son relevantes para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Gobernación del Huila y aplicables al mismo. Adicionalmente en ella se encuentran justificada la exclusión de algunos de los controles y se muestra el motivo de selección de los controles aplicables, entre los motivos de selección se pueden encontrar: resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, requisitos legales o reglamentos, obligaciones contractuales y necesidades empresariales de la organización en materia de seguridad de la información:</p> <p>LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos;</p> | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 39 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Controles actuales | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|--|---------|---|--|--|---|----|-------|-----|---|
| Cláusula | Sección | Objetivo de control / control | | | LR | CO | BR/BP | RRA | |
| 5 Políticas de Seguridad | 5,1 | Dirección de la alta gerencia para la seguridad de la información | | | | | | | |
| | 5.1.1 | Políticas de seguridad de la información | Política general de SPI publicada en el SIGC | | X | | X | X | Establecer y documentar políticas de SPI, y posterior inclusión en el SIG |
| | 5.1.2 | Revisión de las políticas de seguridad de la información | Revisión anual de la Política general de SPI | | X | | X | X | Revisión anual periódica de políticas de SPI, y posterior inclusión en el SIG |
| 6 Organización de la Seguridad de la Información | 6,1 | Organización interna | | | | | | | |
| | 6.1.1 | Roles y responsabilidad de seguridad de la información | Política general de SPI publicada en el SIGC | | | | X | X | Se deben añadir las responsabilidades incluidas en las políticas, en los contratos de los funcionarios |
| | 6.1.2 | Segregación de deberes | Asignación de responsabilidad sobre activos de información | | | | X | X | Se debe establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores |
| | 6.1.3 | Contacto con autoridades | Red de emergencias mediante empresa de seguridad | | X | | X | | Establecer y documentar procedimientos |
| | 6.1.4 | Contacto con grupos de interés especial | No existe asignación de responsabilidad para contactar grupos de interés | | | | X | | Establecer y documentar procedimientos |
| | 6.1.5 | Seguridad de la información en la gestión de proyectos | No se han definido aplicación de políticas y/o procedimiento de SPI en los proyectos | | X | X | X | X | Se deben incluir cláusulas referentes a seguridad y confidencialidad de la información interna en los proyectos |
| | 6,2 | Dispositivos móviles y teletrabajo | | | | | | | |
| | 6.2.1 | Política de dispositivos móviles | No existe política para dispositivos móviles, pero existen directrices elevadas por talento humano | | X | X | X | X | Establecer, documentar e implementar |
| | 6.2.2 | Teletrabajo | Se fomenta y aplican lineamientos de la política de teletrabajo pero no existe trazabilidad | | X | | | | Establecer, documentar e implementar procedimientos para acoger dicha estrategia al interior de la entidad |
| | | | | | | | | | |
| 7 Seguridad | 7,1 | Previo al empleo | | | | | | | |

| | | |
|---|---|---|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043-PL02</p> |
| | <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | <p>Fecha Aprobación: 31 de Enero de 2020</p> |
| | | <p>Versión: 1</p> <p>Página 40 de 117</p> |



Página 40 de 117

| ISO 27001:2013 Controles de Seguridad | | | Controles actuales | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---------------------------------------|---------|--|---|---|--|----|-------|-----|---|
| Cláusula | Sección | Objetivo de control / control | | | LR | CO | BR/BP | RRA | |
| | 7.1.1 | Verificación de antecedentes | Solicitud de antecedentes disciplinarios, fiscales, judiciales y profesionales | | X | X | X | | Se deben incluir las responsabilidades incluidas en las políticas, en los contratos de los funcionarios |
| | 7.1.2 | Términos y condiciones del empleo | Explícitamente no se definen obligaciones sobre la información a manejar | | X | X | X | | Se debe establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores |
| | 7.2 | Durante el empleo | | | | | | | |
| | 7.2.1 | Responsabilidades de la Alta Gerencia | No existen procedimientos que garanticen responsabilidades de funcionarios sobre SPI | | X | X | X | X | Seguimiento mediante Control Interno |
| | 7.2.2 | Conciencia, educación y entrenamiento de seguridad de la información | No existe conciencia de SPI | | X | X | X | X | Establecer, documentar e implementar Plan de capacitación y circulares internas |
| | 7.2.3 | Proceso disciplinario | No existen procesos disciplinarios para violaciones de SPI | | X | X | | | Proveer lineamientos jurídicos y establecer procesos de control interno disciplinario |
| | 7.3 | Terminación y cambio de empleo | | | | | | | |
| | 7.3.1 | Termino de responsabilidades o cambio de empleo | No se establecen acuerdos de confidencialidad con funcionarios | | X | X | | | Se deben añadir las responsabilidades incluidas en las políticas, en los contratos de los funcionarios |
| | | | | | | | | | |
| 8 Gestión de Activos | 8.1 | Responsabilidad de los activos | | | | | | | |
| | 8.1.1 | Inventario de activos | Inventario de activos de TI desactualizado, pendiente de revisión, asignación de responsabilidad y aprobación por la alta dirección | | X | X | X | X | Adaptación de aplicativo de inventario, para que incluya perfiles destinados a la gestión de activos TI por parte del Grupo de Tecnología |
| | 8.1.2 | Propiedad de activos | Se aplica proceso de asignación de activos, pero se debe revisar clasificación y asignación final | | X | X | X | X | Establecer y documentar procedimiento de seguimientos a la responsabilidad sobre los activos de TI. |
| | 8.1.3 | Uso aceptable de los activos | Es necesario sensibilización para el uso eficiente de los activos | | | X | X | | Establecer, documentar e implementar política de uso de activos TI (hardware y software) |
| | 8.1.4 | Devolución de activos | Formato de traslado de activos y manual de almacén | | X | X | X | | Verificar su cumplimiento |
| | | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 41 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---------------------------------------|---------|---|---|---|----|-------|-----|--|
| Cláusula | Sección | Objetivo de control / control | | LR | CO | BR/BP | RRA | |
| | 8,2 | Clasificación de la información | | | | | | |
| | 8.2.1 | Clasificación de la información | Procedimientos de clasificación de información por parte de Archivo Departamental | X | X | X | X | Establecer y documentar procedimientos para la clasificación de la información |
| | 8.2.2 | Etiquetado de la información | Procedimiento de etiquetado para activos de información, que no se aplica a cabalidad | X | X | X | | Establecer y documentar procedimientos para la clasificación de la información |
| | 8.2.3 | Manejo de activos | Procedimientos establecidos en Manual de Almacén | | | X | | Establecer y documentar política de uso de activos TI (hardware y software) |
| | 8,3 | Manejo de medios | | | | | | |
| | 8.3.1 | Gestión de medios removibles | Procedimiento inexistente | X | X | X | | Establecer, documentar e implementar política de uso de activos TI (hardware y software) |
| | 8.3.2 | Eliminación de medios | Procedimiento inexistente | X | X | X | | Establecer, documentar e implementar política de uso de activos TI (hardware y software) |
| | 8.3.3 | Transporte de medios físicos | Procedimiento inexistente | X | X | X | X | Establecer, documentar e implementar política de uso de activos TI (hardware y software) |
| 9 Control de Acceso | 9,1 | Requerimientos de negocio para el control de acceso | | | | | | |
| | 9.1.1 | Política de control de acceso | Procedimientos de control de acceso que no se cumplen en su totalidad | X | X | X | X | Establecer, documentar e implementar política de control de acceso |
| | 9.1.2 | Acceso a redes y servicios de red | No existe política de acceso a redes y servicios de red | | X | X | X | Establecer, documentar e implementar política de control de acceso |
| | 9,2 | Gestión de accesos de usuario | | | | | | |
| | 9.2.1 | Registro y baja del usuario | Manual de almacén, no se cumple el procedimiento en su totalidad | X | X | X | X | Establecer, documentar e implementar política de control de acceso |
| | 9.2.2 | Provisión de acceso a usuarios | Formato de solicitud de cuentas de usuario, pero no se realiza trazabilidad al acceso | | | | | Incluir en la política de control de acceso |
| | 9.2.3 | Gestión de derechos de acceso privilegiados | Formato de solicitud de cuentas de usuario, pero no se realiza trazabilidad al acceso | | | | | Incluir en la política de control de acceso |
| | 9.2.4 | Gestión de información de autenticación secreta de usuarios | No existe política de gestión de información de autenticación secreta de usuarios | X | X | X | | Establecer, documentar e implementar política de control de acceso |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 42 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Controles actuales | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---------------------------------------|---|--|---|--|---|----|---|---|--|
| Cláusula | Sección | Objetivo de control / control | | | LR | CO | BR/BP | RRA | |
| | 9.2.5 | Revisión de derechos de acceso de usuarios | No se realizan revisiones periódicas de derechos de acceso a usuarios | | X | X | | Establecer, documentar e implementar política de control de acceso | |
| | 9.2.6 | Eliminación o ajuste de derechos de acceso | Formato de solicitud de cuentas de usuario | | X | X | | Establecer, documentar e implementar política de control de acceso | |
| | 9.3 | Responsabilidades del usuario | | | | | | | |
| | 9.3.1 | Uso de información de autenticación secreta | No existe política de gestión de información de autenticación secreta de usuarios | X | X | X | | Establecer, documentar e implementar política de control de acceso | |
| | 9.4 | Control de acceso de sistemas y aplicaciones | | | | | | | |
| | 9.4.1 | Restricción de acceso a la información | Formato de solicitud de cuentas de usuario, no existe políticas de control de acceso | X | X | X | | Establecer, documentar e implementar política de control de acceso | |
| | 9.4.2 | Procedimientos de inicio de sesión seguro | No existe procedimiento de ingreso seguro a sistemas y aplicaciones | X | X | X | X | Establecer, documentar e implementar política de control de acceso | |
| | 9.4.3 | Sistema de gestión de contraseñas | No existe política de gestión de contraseñas, pero si se gestionan las contraseñas del correo institucional | | | X | X | Establecer, documentar e Implementar política de control de contraseñas | |
| | 9.4.4 | Uso de programas y utilidades privilegiadas | Formato de solicitud de cuentas de usuario para aplicativos de la Gobernación, para otros programas y utilidades no existe procedimiento de control de software | X | X | X | X | Establecer, documentar e implementar política de control de acceso | |
| 9.4.5 | Control de acceso al código fuente del programa | No existe procedimiento de gestión de código fuente de aplicativos | | | | | Establecer, documentar e implementar políticas de seguimiento al control de códigos | | |
| | | | | | | | | | |
| 10 Criptografía | 10.1 | Controles criptográficos | | | | | | | |
| | 10.1.1 | Política en el uso de controles criptográficos | SE EXCLUYE | No se aplican controles criptográfico | X | X | X | X | |
| | 10.1.2 | Gestión de llaves | No existe procedimiento de gestión llaves cifradas de acceso | | X | X | X | X | Establecer, documentar e implementar políticas de gestión de llaves cifradas |
| | | | | | | | | | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 43 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---------------------------------------|---------|--|---|--|----|-------|-----|--|
| Cláusula | Sección | Objetivo de control / control | | LR | CO | BR/BP | RRA | |
| 11 Seguridad Física y del Entorno | 11,1 | Áreas seguras | | | | | | |
| | 11.1.1 | Perímetro de seguridad físico | Restricciones mediante Vigilancia, cámaras y avisos de "Solo personal autorizado", sin definición general en la entidad | X | X | X | X | Definir y aplicar de perímetro de seguridad físico |
| | 11.1.2 | Controles físicos de entrada | No existen controles robustos de ingreso a las instalaciones | X | X | X | X | Establecer, documentar y definir formatos de control de llaves y de control de acceso a oficinas de gestión de información, e incluirlos en políticas de control de acceso |
| | 11.1.3 | Seguridad de oficinas, habitaciones y facilidades | Restricciones mediante Vigilancia, cámaras y avisos de "Solo personal autorizado", sin definición general en la entidad | | X | X | | Establecer, documentar y definir formatos de control de llaves y de control de acceso a oficinas de gestión de información, e incluirlos en políticas de control de acceso |
| | 11.1.4 | Protección contra amenazas externas y del ambiente | Se encuentran definidos riesgos en el SGSST, mas no está implementada en áreas críticas de tecnología | X | X | X | X | Realizar verificación y aplicación de medidas de mitigación de riesgos del SGSST |
| | 11.1.5 | Trabajo en áreas seguras | No existe procedimiento de trabajo en áreas seguras | | X | X | | Establecer, documentar y definir procesos de trabajo en áreas seguras |
| | 11.1.6 | Áreas de entrega y carga | Existen directrices asignadas a personal de vigilancia y bitácora de ingreso en entrada principal de cada sede, pero estas no están consolidadas en toda la entidad | | | X | | Establecer, documentar y definir formatos de control de acceso a oficinas, e incluirlos en políticas de control de acceso |
| | 11,2 | Equipo | | | | | | |
| | 11.2.1 | Instalación y protección de equipo | No existen directrices claras, por tanto no hay cumplimiento de las mismas por parte de funcionarios | | X | X | X | Establecer, documentar e implementar lista de chequeo de mobiliario para uso de activos TI e incluirla en políticas de uso de hardware |
| | 11.2.2 | Servicios de soporte | No se cuenta con los servicios de soporte requeridos para sistemas de respaldo eléctrico | | X | X | | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 44 de117 |

| ISO 27001:2013 Controles de Seguridad | | | Controles actuales | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---------------------------------------|---------|---|--|--|--|----|-------|-----|---|
| Cláusula | Sección | Objetivo de control / control | | | LR | CO | BR/BP | RRA | |
| | | | | | | | | | periódico de sistemas de respaldo eléctrico (UPS y Planta Eléctrica) |
| | 11.2.3 | Seguridad en el cableado | No existen medidas de protección y seguridad del cableado eléctrico y de telecomunicaciones, de acuerdo a estándares internacionales | | | X | X | X | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de cableado estructurado |
| | 11.2.4 | Mantenimiento de equipos | No existe plan de mantenimiento de equipos | | | X | X | X | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de equipos |
| | 11.2.5 | Retiro de activos | No existen directrices ni políticas definidas para retiro temporal de activos, aunque se aplica servicio de vigilancia y bitácora de ingreso en entrada principal de cada sede | | | X | X | | Establecer, documentar e implementar formatos de retiro de activos e incluirlos en las políticas y procedimientos de uso y administración de hardware |
| | 11.2.6 | Seguridad del equipo y activos fuera de las instalaciones | No existen medidas de seguridad para activos que se encuentran fuera de las instalaciones | | | X | X | | Establecer, documentar e implementar formatos de retiro de activos e incluirlos en las políticas y procedimientos de uso y administración de hardware |
| | 11.2.7 | Eliminación segura o reuso del equipo | No existen directrices para disposición segura o reuso de equipos | | X | X | X | | Establecer, documentar e implementar procedimientos para la eliminación segura o reuso de activos TI |
| | 11.2.8 | Equipo de usuario desatendido | No existen directrices definidas ni procedimientos establecidos al respecto | | | X | X | X | Establecer, documentar e implementar procedimientos para bloqueo de sesión de usuario en equipos |
| | 11.2.9 | Política de escritorio limpio y pantalla limpia | No existen directrices ni políticas de escritorio y pantalla limpia | | | X | X | X | Adoptar procedimientos para escritorio y pantalla limpios |
| 12 Seguridad en las | | | | | | | | | |
| | 12.1 | Procedimientos Operacionales y Responsabilidades | | | | | | | |
| | 12.1.1 | Documentación de procedimientos operacionales | Manual de funciones. No existen procedimientos de operación detallados. | | X | X | X | | Incluir funciones y obligaciones contractuales de SPI y a su vez incluir en Manual de funciones y Portal de Contratación |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 45 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---------------------------------------|---------|--|--|---|----|-------|-----|---|
| Cláusula | Sección | Objetivo de control / control | | LR | CO | BR/BP | RRA | |
| | 12.1.2 | Gestión de cambios | No existe procedimiento de control de cambios formalizado | | X | X | | Establecer formato de gestión de cambios en los procesos |
| | 12.1.3 | Gestión de la capacidad | No existen procedimientos de gestión de capacidad. | | X | X | | Establecer, documentar e implementar plan periódico de diagnóstico de equipos |
| | 12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación | No existe procedimientos para la separación de ambientes | | | | | Realizar identificación de ambientes y señalar debidamente |
| | 12.2 | Protección de Software Malicioso | | | | | | |
| | 12.2.1 | Controles contra software malicioso | No existen políticas de prohibición de uso de software no autorizado, sin embargo se realizan sensibilizaciones al respecto. | | X | X | | Plan de adquisición y mantenimiento de aplicativo de protección contra software malicioso |
| | 12.3 | Respaldo | | | | | | |
| | 12.3.1 | Respaldo de información | Se realizan backups de algunos sistemas de información, sin un procedimiento establecido para almacenamiento y pruebas de restauración | X | X | X | X | Estandarizar y promover mediante políticas |
| | 12.4 | Bitácoras y monitoreo | | | | | | |
| | 12.4.1 | Bitácoras de eventos | No existe un registro de eventos u actividades de SPI | X | X | X | X | Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad |
| | 12.4.2 | Protección de información en bitácoras | No existe procedimiento de control de la información de bitácoras | X | | X | X | Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad |
| | 12.4.3 | Bitácoras de administrador y operador | No existe registros de actividades de administrador ni de operadores | X | | X | X | Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad |
| | 12.4.4 | Sincronización de relojes | No se cuenta con fuente de referencia de tiempo única | | | X | | Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad |
| | 12.5 | Control de software operacional | | | | | | |
| | 12.5.1 | Instalación de software en sistemas operacionales | No se realizan controles de actualizaciones de software | | X | X | | Establecer, documentar e implementar política de uso de activos TI (hardware y software) y de control de acceso |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 46 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---------------------------------------|---------|---|--|--|----|-------|-----|---|
| Cláusula | Sección | Objetivo de control / control | | LR | CO | BR/BP | RRA | |
| | 12,6 | Gestión de vulnerabilidades técnicas | | | | | | |
| | 12.6.1 | Gestión de vulnerabilidades técnicas | Solo existe el Mapa de Riesgos por Proceso en el SIG para gestión de riesgos, pero no abarca vulnerabilidades técnicas de los mismos | | X | X | X | Establecer y documentar análisis y evaluación de riesgos TI |
| | 12.6.2 | Restricciones en la instalación de software | Se efectúan restricciones para la instalación de software pero no existe proceso documentado | X | X | X | X | Establecer, documentar e implementar política de uso de activos TI (hardware y software) y de control de acceso |
| | 12,7 | Consideraciones de auditoría de sistemas de información | | | | | | |
| | 12.7.1 | Controles de auditoría de sistemas de información | Procedimientos de Auditoría Interna y Planes de Mejora Continua | | X | X | | Establecer, documentar e implementar plan de auditoría de sistemas de información para Control Interno |
| 13 Seguridad en las Comunicaciones | 13,1 | Gestión de seguridad en red | | | | | | |
| | 13.1.1 | Controles de red | Existen restricciones generales para todos los funcionarios, y se habilita acceso de acuerdo a requerimientos a través de mesa de ayuda. | | | | | Efectuar análisis periódicos de tráfico de red, realizar reporte de anomalías detectadas y aplicar medidas preventivas y correctivas cuando sea el caso. Documentar e implementar política de restricciones y controles de red. |
| | 13.1.2 | Seguridad en los servicios en red | No se tienen identificados en todos los servicios de red directrices de seguridad en información | | X | X | X | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de cableado estructurado |
| | 13.1.3 | Segregación en redes | Existen procedimientos básicos no documentados de segregación de redes en la entidad | | | X | X | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de cableado estructurado |
| | 13,2 | Transferencia de información | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 47 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Controles actuales | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|--|---------|---|--|--|--|----|-------|-----|--|
| Cláusula | Sección | Objetivo de control / control | | | LR | CO | BR/BP | RRA | |
| | 13.2.1 | Políticas y procedimientos para la transferencia de información | No existe seguimiento de flujo de comunicaciones en la red | | | X | X | X | Establecer, documentar e implementar políticas de transferencia de información al interior de la Gobernación del Huila |
| | 13.2.2 | Acuerdos en la transferencia de información | No existen directrices u acuerdos de transferencia de información | | X | X | X | X | Establecer, documentar e implementar políticas de transferencia de información al interior de la Gobernación del Huila |
| | 13.2.3 | Mensajería electrónica | No existen directrices u definiciones de protección formal para mensajería electrónica | | | X | X | X | Establecer, documentar e implementar políticas de uso del correo electrónico institucional |
| | 13.2.4 | Acuerdos de confidencialidad o no-revelación | No existen acuerdos ni políticas de confidencialidad de información transmitida | | X | X | X | X | Establecer, documentar e implementar políticas de uso del correo electrónico institucional, y acuerdos de confidencialidad en los procesos contractuales y de gestión de proyectos |
| | | | | | | | | | |
| 14 Adquisición, Desarrollo y Mantenimiento de Sistemas | 14,1 | Requerimientos de seguridad en sistemas de información | | | | | | | |
| | 14.1.1 | Análisis y especificación de requerimientos de seguridad | No existen directrices ni políticas de requerimientos de SPI en Fichas Técnicas y Estudios Previos Contractuales | | X | X | X | X | Incluir en estudios de conveniencia previos y procesos contractuales |
| | 14.1.2 | Aseguramiento de servicios de aplicación en redes públicas | No existen directrices de seguridad formales de servicios en aplicaciones de redes públicas. | | X | X | X | | Incluir encriptación de comunicaciones en características técnicas de aplicaciones que trabajen sobre redes públicas |
| | 14.1.3 | Protección de transacciones en servicios de aplicación | No existen directrices de protección de transacciones en los servicios disponibles en la entidad | | X | X | X | X | Establecer e implementar medidas de protección de transacciones |
| | 14,2 | Seguridad en el proceso de desarrollo y soporte | | | | | | | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 48 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Controles actuales | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---------------------------------------|---------|---|---|--|---|----|-------|-----|---|
| Cláusula | Sección | Objetivo de control / control | | | LR | CO | BR/BP | RRA | |
| | 14.2.1 | Política de desarrollo seguro | No existen políticas de desarrollo seguro de software | | | | | | Establecer, documentar e implementar políticas de desarrollo seguro de software |
| | 14.2.2 | Procedimientos de control de cambios del sistema | No existen directrices en el control de cambio de sistemas | | | X | X | | Establecer, documentar e implementar procedimientos de control de cambios por funcionarios de tecnología. |
| | 14.2.3 | Revisión técnica de aplicaciones después de cambios a la plataforma operativa | No existen directrices de revisión técnica de aplicaciones | | | X | X | | Establecer, documentar e implementar procedimientos de control de cambios por funcionarios de tecnología. |
| | 14.2.4 | Restricción de cambios en paquetes de software | No existen directrices de restricción de cambios en paquetes de software | | | X | X | | Establecer, documentar e implementar políticas de desarrollo seguro de software |
| | 14.2.5 | Principios de seguridad en la ingeniería de sistemas | No existe procedimiento de construcción de sistemas seguros | | | | | | Establecer, documentar e implementar políticas de desarrollo seguro de software |
| | 14.2.6 | Entorno de desarrollo seguro | No existen políticas para ambientes de desarrollo seguro | | | | | | Establecer, documentar e implementar políticas de desarrollo seguro de software |
| | 14.2.7 | Desarrollo tercerizado | No existen directrices para desarrollos contratados externamente | | | X | X | | Establecer, documentar e implementar procedimiento de seguimiento por funcionarios de tecnología. |
| | 14.2.8 | Pruebas de seguridad del sistema | No existen procedimientos de pruebas de seguridad | | | | | | Establecer, documentar e implementar procedimiento de pruebas de seguridad por funcionarios de tecnología. |
| | 14.2.9 | Pruebas de aceptación del sistema | No existen procedimientos de pruebas para aceptación de sistemas | | | X | X | | Establecer, documentar e implementar procedimiento de pruebas de aceptación por funcionarios de tecnología. |
| | 14,3 | Datos de prueba | | | | | | | |
| | 14.3.1 | Protección de datos de prueba | Se realizan backups de sistemas de información, pero no existen procedimientos para protección de datos e información de prueba | | | X | X | | Establecer, documentar e implementar procedimiento para el almacenamiento seguro de datos de prueba |

| | | |
|---|---|---|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043- PL02</p> |
| | <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | <p>Fecha Aprobación: 31 de Enero de 2020</p> |
| | | <p>Versión: 1</p> <p>Página 49 de 117</p> |



CODIGO: SGN-C043-PL02

| |
|--|
| Fecha Aprobación: 31 de Enero de 2020 |
|--|

Página 49 de 117

| ISO 27001:2013 Controles de Seguridad | | | Controles actuales | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---|---------|--|--|--|---|----|-------|---|---|
| Cláusula | Sección | Objetivo de control / control | | | LR | CO | BR/BP | RRA | |
| 15 Relaciones con Proveedores | 15,1 | Seguridad de la información en relaciones con el proveedor | | | | | | | |
| | 15.1.1 | Política de seguridad de la información en las relaciones con el proveedor | No existen políticas de SPI para relaciones con proveedores | | X | X | | Establecer e implementar | |
| | 15.1.2 | Atención de tópicos de seguridad en los acuerdos con el proveedor | No existen políticas de SPI para relaciones con proveedores | | X | X | | Establecer e implementar | |
| | 15.1.3 | Cadena de suministros de tecnologías de la información y comunicaciones | No existen políticas de SPI para relaciones con proveedores | | X | X | | Establecer e implementar | |
| | 15,2 | Gestión de entrega de servicios de proveedor | | | | | | | |
| | 15.2.1 | Monitoreo y revisión de servicios del proveedor | No existen políticas de SPI para relaciones con proveedores | | X | X | X | Establecer e implementar | |
| | 15.2.2 | Gestión de cambios a los servicios del proveedor | No existen políticas de SPI para relaciones con proveedores | | X | X | X | Establecer e implementar Política de seguridad de la información en las relaciones con el proveedor | |
| 16 Gestión de Incidentes de Seguridad de la Información | 16,1 | Gestión de incidentes de seguridad de la información y mejoras | | | | | | | |
| | 16.1.1 | Responsabilidades y procedimientos | No existe asignación de responsabilidades y procedimientos de respuesta rápida a incidentes de seguridad | | | X | X | X | Establecer, documentar e implementar plan de contingencia |
| | 16.1.2 | Reporte de eventos de seguridad de la información | No existen directrices ni procedimientos para aplicar en eventos de SPI | | | X | X | X | Establecer, documentar e implementar plan de contingencia |
| | 16.1.3 | Reporte de debilidades de seguridad de la información | No existe procedimiento de reporte de eventos de SPI | | | X | X | X | Establecer, documentar e implementar plan de contingencia |
| | 16.1.4 | Valoración y decisión de eventos de seguridad de la información | No existe reporte de eventos de SPI | | | X | X | X | Establecer, documentar e implementar plan de contingencia |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 50 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|--|---------|---|---|---|----|-------|-----|---|
| Cláusula | Sección | Objetivo de control / control | | LR | CO | BR/BP | RRA | |
| | 16.1.5 | Respuesta a incidentes de seguridad de la información | No existen procedimientos de respuesta a incidentes de SPI | | X | X | X | Establecer, documentar e implementar plan de contingencia |
| | 16.1.6 | Aprendizaje de incidentes de seguridad de la información | No existen procedimientos de respuesta a incidentes de SPI, ni registro de incidentes | | X | X | X | Establecer, documentar e implementar plan de contingencia |
| | 16.1.7 | Colección de evidencia | Existen procedimientos de custodia de archivos como Tablas de retención documental, más no se aplican procedimientos para la identificación, recolección, adquisición y preservación de información | | X | X | X | Establecer, documentar e implementar plan de contingencia |
| 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio | 17,1 | Continuidad de la seguridad de la información | | | | | | |
| | 17.1.1 | Planeación de la continuidad de la seguridad de la información | No se tiene formalidad del BCP y no se tiene cumplimiento por parte de los funcionarios | X | | X | | Establecer, documentar e implementar plan de continuidad del negocio |
| | 17.1.2 | Implementación de la continuidad de la seguridad de la información | Existen procedimientos para el mantenimiento de la información física de la entidad, pero no se tiene formalidad del BCP | X | | X | | Establecer, documentar e implementar plan de continuidad del negocio |
| | 17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | No se han realizado pruebas de funcionalidad en SPI | X | | X | | Establecer, documentar e implementar plan de continuidad del negocio |
| | 17,2 | Redundancias | | | | | | |
| | 17.2.1 | Disponibilidad de facilidades de procesamiento de información | No cuenta con elementos redundantes | X | | X | X | |
| 18 Cumplimiento | 18,1 | Cumplimiento con Requerimientos Legales y Contractuales | | | | | | |
| | 18.1.1 | Identificación de legislación aplicable y requerimientos contractuales | Existen responsables para el cumplimiento de las leyes y tiene responsables en la identificación | X | X | X | | Incluir dentro de los procedimientos y la declaración de aplicación de políticas de seguridad de la información, la normatividad, reglamentación y legislación respectiva |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 51 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Comentarios (justificación de exclusión) | Controles seleccionados y razones de selección | | | | Comentarios (visión general de la implementación) |
|---------------------------------------|---------|---|--|---|----|-------|-----|---|
| Cláusula | Sección | Objetivo de control / control | | LR | CO | BR/BP | RRA | |
| | 18.1.2 | Derechos de propiedad intelectual (IPR) | No se cuentan con procedimientos documentados y aprobados para tal fin, pero se entregan derechos contractuales de documentos realizados por contratistas | X | X | X | | Establecer, documentar e implementar plan de verificación y seguimiento a licenciamiento de aplicaciones y software |
| | 18.1.3 | Protección de registros | Existen tablas de retención documental que especifican los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción | X | X | X | | Establecer, documentar e implementar plan de verificación y seguimiento a licenciamiento de aplicaciones y software |
| | 18.1.4 | Privacidad y protección de información personal identificable (PIR) | Existen algunas políticas de protección de información por aplicativo | X | X | X | | Establecer, documentar e implementar plan de capacitación, promoción, divulgación y aplicación de Ley 1273 de 2009 |
| | 18.1.5 | Regulación de controles criptográficos | SE EXCLUYE | X | X | X | | |
| | 18.2 | Revisiones de seguridad de la información | | | | | | |
| | 18.2.1 | Revisión independiente de seguridad de la información | Se cuentan con auditorías en SPI | X | X | X | | Establecer, documentar e implementar planes de auditoría interna las políticas de SPI |
| | 18.2.2 | Cumplimiento con políticas y estándares de seguridad | No se realizan procedimientos de SPI | X | X | X | | Establecer, documentar e implementar planes de auditoría interna las políticas de SPI |
| | 18.2.3 | Revisión del cumplimiento técnico | Se realiza revisión en algunos sistemas de información | X | X | X | | Establecer, documentar e implementar planes de auditoría interna las políticas de SPI |
| | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 52 de 117 |

11.2. Plan de Implementación de Controles para Tratamiento de Riesgos

A continuación se presenta el plan de implementación de controles de seguridad de la información para mitigación de riesgos de seguridad y privacidad de la información, basados en la declaración de aplicabilidad establecida anteriormente. Cabe añadir que este plan engloba la implementación de controles para mitigación de riesgos en cada uno de los procesos, teniendo en cuenta que el avance hasta la fecha corresponde a 11 de 37 procesos de gestión con análisis, valoración y tratamiento de riesgos de seguridad digital en la Gobernación del Huila.

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|--|---------|---|--|---|---|---------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| 5 Políticas de Seguridad | 5,1 | Dirección de la alta gerencia para la seguridad de la información | | | | | | |
| | 5.1.1 | Políticas de seguridad de la información | Todos | Inclusión de políticas de SPI en el SIG | Política General de SPI | Grupo de Tecnología | Feb-2020 | Jun-2020 |
| | 5.1.2 | Revisión de las políticas de seguridad de la información | Todos | Revisión anual periódica de políticas de SPI, y posterior inclusión en el SIG | Política General de SPI | Grupo de Tecnología | Sept-2020 | Dic-2020 |
| 6 Organización de la Seguridad de la Información | 6,1 | Organización interna | | | | | | |
| | 6.1.1 | Roles y responsabilidad de seguridad de la información | Coordinador TIC - Usuarios Finales - Usuarios Externos | Se deben añadir las responsabilidades incluidas en las políticas, en los contratos de los funcionarios | Contratos de personal con funciones asociadas | Talento Humano | Sept-2020 | Dic-2020 |
| | 6.1.2 | Segregación de deberes | Coordinador TIC - Usuarios Finales - Usuarios Externos | Se debe establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores | Certificaciones de Disponibilidad de Personal | Talento Humano | Feb-2020 | Dic-2020 |
| | 6.1.3 | Contacto con autoridades | Coordinador TIC - Usuarios Finales - Usuarios Externos | Establecer y documentar procedimientos | Procedimiento de contacto con autoridades | Grupo de Tecnología | Feb-2020 | Dic-2020 |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 53 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|--|---|---|--|--|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 6.1.4 | Contacto con grupos de interés especial | Coordinador TIC | Establecer y documentar procedimientos | Procedimiento de contacto con grupos de interés | Grupo de Tecnología | Feb-2020 | Dic-2020 |
| | 6.1.5 | Seguridad de la información en la gestión de proyectos | Coordinador TIC - Estudios previos y de conveniencia – Contratos y Convenios para ejecución de proyectos – Estudios previos y de conveniencia | Se deben incluir cláusulas referentes a seguridad y confidencialidad de la información interna en los proyectos | Contratos y Convenios para ejecución de proyectos - Estudios previos y de conveniencia | Grupo de Tecnología – Departamento de Contratación | Sept-2020 | Dic-2020 |
| | 6.2 | Dispositivos móviles y teletrabajo | | | | | | |
| | 6.2.1 | Política de dispositivos móviles | Coordinador TIC - Usuarios Finales | Establecer, documentar e implementar | Política de dispositivos móviles | Grupo de Tecnología | Feb-2020 | Dic-2020 |
| | 6.2.2 | Teletrabajo | Coordinador TIC - Usuarios Finales - Equipos de cómputo - Aplicativos de la entidad | Establecer, documentar e implementar procedimientos para acoger dicha estrategia al interior de la entidad | Procedimientos de adopción de Teletrabajo | Grupo de Tecnología | Sept-2020 | Dic-2021 |
| | | | | | | | | |
| 7 Seguridad en los Recursos Humanos | 7.1 | Previo al empleo | | | | | | |
| | 7.1.1 | Verificación de antecedentes | Documentos Contractuales - Estudios previos y de conveniencia | Se deben incluir las responsabilidades incluidas en las políticas en los contratos de los funcionarios. A su vez, verificar autenticidad de documentos presentados por aspirantes a un cargo dentro de la entidad | Contratos y Convenios – Listas de chequeo | Talento Humano | Feb-2020 | Dic-2021 |
| | 7.1.2 | Términos y condiciones del empleo | Estudios previos y de conveniencia - Contratos de Personal - Contrato de Servicios con Terceros | Se debe establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores. | Certificación de Disponibilidad de Personal | Talento Humano | Feb-2020 | Dic-2020 |
| | 7.2 | Durante el empleo | | | | | | |
| | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 54 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|--|---|--|--|--|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 7.2.1 | Responsabilidades de la Alta Gerencia | Manual de SIG | Seguimiento a las responsabilidades de alta gerencia mediante Control Interno | Revisión y actualización del Manual de SIG | Oficina de Control Interno | Feb-2020 | Dic-2023 |
| | 7.2.2 | Conciencia, educación y entrenamiento de seguridad de la información | Plan de Capacitación y Sensibilización en Seguridad de la Información al personal, contratistas y terceros. | Establecer, documentar e implementar Plan de capacitación y circulares internas | Plan de Capacitación y Sensibilización en SPI | Grupo de Tecnología - Talento Humano | Jul-2020 | Dic-2023 |
| | 7.2.3 | Proceso disciplinario | Manual de Funciones | Aplicar lineamientos jurídicos y establecer procesos de control interno disciplinario | Ajustes de lineamientos jurídicos para definir procesos disciplinarios | Oficina de Control Interno Disciplinario | Feb-2021 | Dic-2023 |
| | 7.3 | Terminación y cambio de empleo | | | | | | |
| | 7.3.1 | Termino de responsabilidades o cambio de empleo | Contratos de Personal - Contrato de Servicios con Terceros | Se deben añadir las responsabilidades incluidas en las políticas, en los contratos de los funcionarios | Contratos laborales y prestación de servicios | Talento Humano – Todas las áreas | Sept-2020 | Dic-2020 |
| 8 Gestión de Activos | 8.1 | Responsabilidad de los activos | | | | | | |
| | 8.1.1 | Inventario de activos | Inventario de Activos de Información – Personal y Funcionarios de apoyo | Actualización de inventario de activos de información. Parametrización y/o modificación de aplicativo de inventario, para que incluya perfiles destinados a la gestión de activos TI | Inventario de Activos de Información | Grupo de Tecnología - Archivo | Feb-2020 | Jun-2021 |
| | 8.1.2 | Propiedad de activos | Inventario de Activos de Información - Personal y Funcionarios de apoyo | Establecer y documentar procedimiento de seguimientos a la responsabilidad sobre los activos. | Procedimiento de seguimiento a responsabilidad sobre activos de TI | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 8.1.3 | Uso aceptable de los activos | Aplicaciones y Software - Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Establecer y documentar política de uso de activos TI (hardware y software) | Política de uso de activos TI | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 55 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|---|---|--|---|---------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 8.1.4 | Devolución de activos | Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Establecer y documentar política de uso de activos TI (hardware y software) | Política de uso de activos TI | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 8.2 | Clasificación de la información | | | | | | |
| | 8.2.1 | Clasificación de la información | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer y documentar procedimientos para la clasificación de la información | Procedimiento para la clasificación de la información | Grupo de Tecnología | Feb-2020 | Dic-2020 |
| | 8.2.2 | Etiquetado de la información | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer y documentar procedimientos para la clasificación de la información | Procedimiento para la clasificación de la información | Grupo de Tecnología | Feb-2020 | Dic-2020 |
| | 8.2.3 | Manejo de activos | Aplicaciones y Software - Hardware - Equipos auxiliares - Servicio de Internet - Personal y Funcionarios de apoyo | Establecer y documentar política de uso de activos TI (hardware y software) | Política de uso de activos TI | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 8.3 | Manejo de medios | | | | | | |
| | 8.3.1 | Gestión de medios removibles | Hardware - Personal y Funcionarios de apoyo | Establecer y documentar política de uso de activos TI (hardware y software) | Política de uso de activos TI | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 8.3.2 | Eliminación de medios | Hardware - Personal y Funcionarios de apoyo | Establecer y documentar política de uso de activos TI (hardware y software) | Política de uso de activos TI | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 8.3.3 | Transporte de medios físicos | Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Establecer y documentar política de uso de activos TI (hardware y software) | Política de uso de activos TI | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| 9 Control de Acceso | 9.1 | Requerimientos de negocio para el control de acceso | | | | | | |
| | 9.1.1 | Política de control de acceso | Aplicaciones y Software - Hardware - Equipos auxiliares - Servicio de Internet - Personal y Funcionarios de apoyo | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.1.2 | Acceso a redes y servicios de red | Aplicaciones y Software - Hardware - Equipos auxiliares - Servicio de Internet - Personal y Funcionarios de apoyo | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 56 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|---|---|--|--|---------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 9.2 | Gestión de accesos de usuario | | | | | | |
| | 9.2.1 | Registro y baja del usuario | Aplicaciones y Software – Hardware - Personal y Funcionarios de apoyo | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.2.2 | Provisión de acceso a usuarios | Aplicaciones y Software - Hardware – Servicio de Internet - Personal y Funcionarios de apoyo | Incluir en la política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.2.3 | Gestión de derechos de acceso privilegiados | Aplicaciones y Software - Hardware – Servicio de Internet - Personal y Funcionarios de apoyo | Incluir en la política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.2.4 | Gestión de información de autenticación secreta de usuarios | Aplicaciones y Software - Hardware – Servicio de Internet - Personal y Funcionarios de apoyo | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.2.5 | Revisión de derechos de acceso de usuarios | Aplicaciones y Software - Hardware – Servicio de Internet - Personal y Funcionarios de apoyo | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.2.6 | Eliminación o ajuste de derechos de acceso | Aplicaciones y Software – Hardware – Servicio de Internet - Personal y Funcionarios de apoyo | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.3 | Responsabilidades del usuario | | | | | | |
| | 9.3.1 | Uso de información de autenticación secreta | Aplicaciones y Software - Hardware – Servicio de Internet - Personal y Funcionarios de apoyo | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.4 | Control de acceso de sistemas y aplicaciones | | | | | | |
| | 9.4.1 | Restricción de acceso a la información | Aplicaciones y Software - Hardware - Servicio de Internet | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.4.2 | Procedimientos de inicio de sesión seguro | Aplicaciones y Software - Hardware - Servicio de Internet | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 57 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|---|---|--|---|--|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 9.4.3 | Sistema de gestión de contraseñas | Aplicaciones y Software - Hardware - Servicio de Internet | Establecer, documentar e Implementar política de control de contraseñas | Política de Gestión de Contraseñas | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.4.4 | Uso de programas y utilidades privilegiadas | Aplicaciones y Software - Hardware - Servicio de Internet | Establecer, documentar e implementar política de control de acceso | Política de Control de Acceso a aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 9.4.5 | Control de acceso al código fuente del programa | Aplicaciones y Software - Código Fuente | Establecer, documentar e implementar políticas de seguimiento al control de códigos | Política de control de acceso a código fuente de aplicaciones | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | | | | | | | | |
| 10 Criptografía | 10,1 | Controles criptográficos | | | | | | |
| | 10.1.1 | Política en el uso de controles criptográficos | SE EXCLUYE | SE EXCLUYE | | -- | | -- |
| | 10.1.2 | Gestión de llaves | Aplicaciones y Software - Hardware - Servicio de Internet | Establecer, documentar e implementar políticas de gestión de llaves cifradas | Política de gestión de llaves cifradas | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | | | | | | | | |
| 11 Seguridad Física y del Entorno | 11,1 | Áreas seguras | | | | | | |
| | 11.1.1 | Perímetro de seguridad físico | Aplicaciones y Software - Hardware - Equipos auxiliares | Definir y aplicar de perímetro de seguridad físico | Definición de perímetro de seguridad físico en áreas seguras | Secretaría General - Seguridad y Salud en el Trabajo | Feb-2021 | Dic-2022 |
| | 11.1.2 | Controles físicos de entrada | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer, documentar y definir lineamientos de control de llaves y de control de acceso a oficinas de gestión de información, e incluirlos en políticas de control de acceso | Lineamientos de control de llaves y de control de acceso a oficinas de gestión de información | Grupo de Tecnología - Secretaría General | Feb-2020 | Dic-2021 |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 58 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|--|--|--|---|---|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 11.1.3 | Seguridad de oficinas, habitaciones y facilidades | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer, documentar y definir lineamientos de control de llaves y de control de acceso a oficinas de gestión de información, e incluirlos en políticas de control de acceso | Lineamientos de control de llaves y de control de acceso a oficinas de gestión de información | Grupo de Tecnología - Secretaría General | Feb-2020 | Dic-2021 |
| | 11.1.4 | Protección contra amenazas externas y del ambiente | Aplicaciones y Software - Hardware - Equipos auxiliares - Instalaciones | Realizar verificación y aplicación de medidas de mitigación de riesgos del SGSST | Planes de acción del SGSST | Grupo de Tecnología – Seguridad y Salud en el Trabajo | Feb-2021 | Dic-2022 |
| | 11.1.5 | Trabajo en áreas seguras | Aplicaciones y Software - Hardware - Equipos auxiliares – Instalaciones - Personal y Funcionarios de apoyo | Establecer, documentar y definir procedimientos de trabajo en áreas seguras | Procedimiento de trabajo en áreas seguras | Grupo de Tecnología - Secretaría General | Feb-2020 | Dic-2021 |
| | 11.1.6 | Áreas de entrega y carga | Aplicaciones y Software - Hardware - Equipos auxiliares-Instalaciones | Establecer, documentar y definir lineamientos de control de acceso a oficinas, e incluirlos en políticas de control de acceso | Lineamientos de control de acceso a oficinas en Política de Control de Acceso | Grupo de Tecnología - Secretaría General | Feb-2020 | Dic-2021 |
| | 11.2 | Equipo | | | | | | |
| | 11.2.1 | Instalación y protección de equipo | Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Establecer, documentar e implementar lista de chequeo de mobiliario para uso de activos TI e incluirla en políticas de uso de hardware | lista de chequeo de mobiliario para uso de activos TI | Grupo de Tecnología | Feb-2021 | Dic-2021 |
| | 11.2.2 | Servicios de soporte | Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de sistemas de respaldo eléctrico (UPS y Planta Eléctrica) | Plan de verificación y mantenimiento preventivo periódico de sistemas de respaldo eléctrico | Grupo de Tecnología | Jun-2020 | Dic-2021 |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 59 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|---|--|--|--|-------------------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 11.2.3 | Seguridad en el cableado | Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de cableado estructurado | Plan de verificación y mantenimiento preventivo periódico de cableado estructurado | Grupo de Tecnología | Jun-2020 | Dic-2021 |
| | 11.2.4 | Mantenimiento de equipos | Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de equipos de cómputo | Plan de verificación y mantenimiento preventivo periódico de equipos de cómputo | Grupo de Tecnología | Jun-2020 | Dic-2021 |
| | 11.2.5 | Retiro de activos | Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Establecer, documentar e implementar formatos de retiro de activos e incluirlos en las políticas y procedimientos de uso de activos TI | Formatos de retiro de activos | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 11.2.6 | Seguridad del equipo y activos fuera de las instalaciones | Hardware - Equipos auxiliares - Instalaciones - Personal y Funcionarios de apoyo | Establecer, documentar e implementar formatos de retiro de activos e incluirlos en las políticas y procedimientos de uso de activos TI | Formatos de retiro de activos | Grupo de Tecnología - Almacén | Feb-2020 | Dic-2021 |
| | 11.2.7 | Eliminación segura o reúso del equipo | Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Actualizar procedimientos para la baja, eliminación segura o reúso de activos TI | Procedimiento de baja de equipos y activos | Grupo de Tecnología - Almacén | Jun-2020 | Dic-2021 |
| | 11.2.8 | Equipo de usuario desatendido | Aplicaciones y Software - Hardware - Personal y Funcionarios de apoyo | Establecer, documentar e implementar procedimientos para bloqueo de sesión de usuario en equipos | procedimientos para bloqueo de sesión de usuario | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 11.2.9 | Política de escritorio limpio y pantalla limpia | Aplicaciones y Software - Personal y Funcionarios de apoyo | Establecer, documentar e implementar procedimientos para escritorio y pantalla limpios | procedimientos para escritorio y pantalla limpios | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | | | | | | | | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 60 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|--|--|---|---|--|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| 12 Seguridad en las Operaciones | 12,1 | Procedimientos Operacionales y Responsabilidades | | | | | | |
| | 12.1.1 | Documentación de procedimientos operacionales | Coordinador TIC - Usuarios Finales - Usuarios Externos | Incluir funciones y obligaciones contractuales de SPI y a su vez incluir en Manual de funciones | Manual de funciones | Talento Humano | Feb-2020 | Dic-2021 |
| | 12.1.2 | Gestión de cambios | Soportes de Información | Establecer procedimiento de gestión de cambios en los procesos | Procedimiento de gestión de cambios | Calidad | Feb-2020 | Dic-2021 |
| | 12.1.3 | Gestión de la capacidad | Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo | Establecer, documentar e implementar plan periódico de diagnóstico de equipos | Plan de verificación y mantenimiento preventivo periódico de equipos de cómputo, cableado estructurado y sistemas de respaldo eléctrico | Grupo de Tecnología | Jun-2020 | Dic-2021 |
| | 12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación | Instalaciones | Realizar identificación de ambientes y señalizar debidamente | Señalización de ambientes | Grupo de Tecnología - Secretaría General | Jun-2020 | Dic-2021 |
| | 12,2 | Protección de Software Malicioso | | | | | | |
| | 12.2.1 | Controles contra software malicioso | Aplicaciones y Software | Administración de aplicativo de protección contra software malicioso | Reportes de administración de aplicativo | Grupo de Tecnología | Jun-2020 | Dic-2021 |
| | 12,3 | Respaldo | | | | | | |
| | 12.3.1 | Respaldo de información | Aplicaciones y Software | Estandarizar y promover mediante políticas | Políticas de respaldo de información | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 12,4 | Bitácoras y monitoreo | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 61 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|---|---|---|--|---------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 12.4.1 | Bitácoras de eventos | Aplicaciones y Software | Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad | política de monitoreo de usuarios y eventos de seguridad | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 12.4.2 | Protección de información en bitácoras | Aplicaciones y Software | Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad | política de monitoreo de usuarios y eventos de seguridad | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 12.4.3 | Bitácoras de administrador y operador | Aplicaciones y Software - Personal y Funcionarios de apoyo | Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad | política de monitoreo de usuarios y eventos de seguridad | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 12.4.4 | Sincronización de relojes | Aplicaciones y Software | Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad | política de monitoreo de usuarios y eventos de seguridad | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 12.5 | Control de software operacional | | | | | | |
| | 12.5.1 | Instalación de software en sistemas operacionales | Aplicaciones y Software | Establecer, documentar e implementar política de uso de activos TI (hardware y software) y de control de acceso | política de uso de activos TI y de control de acceso | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 12.6 | Gestión de vulnerabilidades técnicas | | | | | | |
| | 12.6.1 | Gestión de vulnerabilidades técnicas | Aplicaciones y Software - Hardware - Equipos auxiliares – Datos | Establecer y documentar análisis y evaluación de riesgos TI | Plan de Tratamiento de Riesgos de Seguridad Digital | Grupo de Tecnología | Feb-2020 | Dic-2020 |
| | 12.6.2 | Restricciones en la instalación de software | Aplicaciones y Software - Personal y Funcionarios de apoyo | Establecer y documentar política de uso de activos TI (hardware y software) | política de uso de activos TI | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 12.7 | Consideraciones de auditoría de sistemas de información | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 62 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|---|--|--|--|----------------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 12.7.1 | Controles de auditoría de sistemas de información | Aplicaciones y Software | Establecer, documentar e implementar plan de auditoría de sistemas de información para Control Interno de Gestión | plan de auditoría de sistemas de información | Oficina de Control Interno | Feb-2020 | Dic-2022 |
| 13 Seguridad en las Comunicaciones | 13.1 | Gestión de seguridad en red | | | | | | |
| | 13.1.1 | Controles de red | Aplicaciones y Software | Efectuar análisis periódicos de tráfico de red, realizar reporte de anomalías detectadas y aplicar medidas preventivas y correctivas cuando sea el caso. | Reportes de análisis de tráfico y aplicación de medidas preventivas | Grupo de Tecnología | Jun-2020 | Dic-2022 |
| | 13.1.2 | Seguridad en los servicios en red | Aplicaciones y Software | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de cableado estructurado | plan de verificación y mantenimiento preventivo periódico de cableado estructurado | Grupo de Tecnología | Jun-2020 | Dic-2021 |
| | 13.1.3 | Segregación en redes | Aplicaciones y Software | Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de cableado estructurado | plan de verificación y mantenimiento preventivo periódico de cableado estructurado | Grupo de Tecnología | Jun-2020 | Dic-2021 |
| | 13.2 | Transferencia de información | | | | | | |
| | 13.2.1 | Políticas y procedimientos para la transferencia de información | Aplicaciones y Software - Personal y Funcionarios de apoyo | Establecer, documentar e implementar políticas de transferencia de información al interior de la Gobernación del Huila | políticas de transferencia de información | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| | 13.2.2 | Acuerdos en la transferencia de información | Aplicaciones y Software - Personal y Funcionarios de apoyo | Establecer, documentar e implementar políticas de transferencia de información al interior de la Gobernación del Huila | políticas de transferencia de información | Grupo de Tecnología | Feb-2020 | Dic-2021 |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 63 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|--|---------|--|--|--|--|---|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 13.2.3 | Mensajería electrónica | Aplicaciones y Software - Personal y Funcionarios de apoyo | Establecer, documentar e implementar políticas de uso del correo electrónico institucional | políticas de uso del correo electrónico institucional | Grupo de Tecnología | Feb-2020 | Jun-2020 |
| | 13.2.4 | Acuerdos de confidencialidad o no-revelación | Aplicaciones y Software - Personal y Funcionarios de apoyo - Contrato de Servicios con Terceros | Establecer, documentar e implementar políticas de uso del correo electrónico institucional, y acuerdos de confidencialidad en los procesos contractuales y de gestión de proyectos | políticas de uso del correo electrónico institucional - Acuerdos de confidencialidad | Grupo de Tecnología | Feb-2020 | Dic-2021 |
| 14 Adquisición, Desarrollo y Mantenimiento de Sistemas | 14,1 | Requerimientos de seguridad en sistemas de información | | | | | | |
| | 14.1.1 | Análisis y especificación de requerimientos de seguridad | Aplicaciones y Software - Personal y Funcionarios de apoyo - Contrato de Servicios con Terceros - Estudios Previos Contractuales | Incluir en estudios de conveniencia previos y procesos contractuales | estudios de conveniencia previos y procesos contractuales | Secretaría General - Departamento de Contratación - Grupo de Tecnología | Feb-2021 | Dic-2023 |
| | 14.1.2 | Aseguramiento de servicios de aplicación en redes públicas | Aplicaciones y Software | Incluir cifrado de comunicaciones en características técnicas de aplicaciones que trabajen sobre redes públicas | Pruebas de cifrado de comunicaciones en aplicativos | Grupo de Tecnología | Feb-2021 | Dic-2023 |
| | 14.1.3 | Protección de transacciones en servicios de aplicación | Aplicaciones y Software | Establecer e implementar medidas de protección de transacciones | Política de protección de transacciones | Grupo de Tecnología | Feb-2020 | Dic-2023 |
| | 14,2 | Seguridad en el proceso de desarrollo y soporte | | | | | | |
| | 14.2.1 | Política de desarrollo seguro | Aplicaciones y Software – Código Fuente | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| | 14.2.2 | Procedimientos de control de cambios del sistema | Soportes de información | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 64 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|---|---|---|--|---------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 14.2.3 | Revisión técnica de aplicaciones después de cambios a la plataforma operativa | Aplicaciones y Software | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| | 14.2.4 | Restricción de cambios en paquetes de software | Aplicaciones y Software | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| | 14.2.5 | Principios de seguridad en la ingeniería de sistemas | Todos | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| | 14.2.6 | Entorno de desarrollo seguro | Aplicaciones y Software - Instalaciones | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| | 14.2.7 | Desarrollo tercerizado | Aplicaciones y Software | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| | 14.2.8 | Pruebas de seguridad del sistema | Aplicaciones y Software | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| | 14.2.9 | Pruebas de aceptación del sistema | Aplicaciones y Software | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| | 14.3 | Datos de prueba | | | | | | |
| | 14.3.1 | Protección de datos de prueba | Aplicaciones y Software | Establecer, documentar e implementar procedimiento para el almacenamiento seguro de datos de prueba | procedimiento para el almacenamiento seguro de datos de prueba | Grupo de Tecnología | Feb-2020 | Dic-2023 |
| 15 Relaciones | 15.1 | Seguridad de la información en relaciones con el proveedor | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 65 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|------------|--|---|---|---|---------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 15.1.1 | Política de seguridad de la información en las relaciones con el proveedor | Estudios contractuales previos y de conveniencia | Establecer e implementar política de seguridad de la información en relaciones con proveedores | política de seguridad de la información en relaciones con proveedores | Grupo de Tecnología | Feb-2020 | Dic-2023 |
| | 15.1.2 | Atención de tópicos de seguridad en los acuerdos con el proveedor | Estudios contractuales previos y de conveniencia | Establecer e implementar política de seguridad de la información en relaciones con proveedores | política de seguridad de la información en relaciones con proveedores | Grupo de Tecnología | Feb-2020 | Dic-2023 |
| | 15.1.3 | Cadena de suministros de tecnologías de la información y comunicaciones | Estudios contractuales previos y de conveniencia | Establecer e implementar política de seguridad de la información en relaciones con proveedores | política de seguridad de la información en relaciones con proveedores | Grupo de Tecnología | Feb-2020 | Dic-2023 |
| | 15.2 | Gestión de entrega de servicios de proveedor | | | | | | |
| | 15.2.1 | Monitoreo y revisión de servicios del proveedor | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer e implementar Política de seguridad de la información en las relaciones con el proveedor | política de seguridad de la información en relaciones con proveedores | Grupo de Tecnología | Feb-2020 | Dic-2023 |
| | 15.2.2 | Gestión de cambios a los servicios del proveedor | Aplicaciones y Software - Hardware - Equipos auxiliares - Estudios contractuales previos y de conveniencia - Contrato de Servicios con Terceros | Establecer e implementar Política de seguridad de la información en las relaciones con el proveedor | política de seguridad de la información en relaciones con proveedores | Grupo de Tecnología | Feb-2020 | Dic-2023 |
| 16 | Gestión de | 16.1 | Gestión de incidentes de seguridad de la información y mejoras | | | | | |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 66 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|--|---------|--|---|--|---------------------------------|---------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 16.1.1 | Responsabilidades y procedimientos | Coordinador TIC - Usuarios Finales - Usuarios Externos | Establecer, documentar e implementar plan de contingencia | plan de contingencia | Grupo de Tecnología | Feb-2021 | Dic-2022 |
| | 16.1.2 | Reporte de eventos de seguridad de la información | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer, documentar e implementar plan de contingencia | plan de contingencia | Grupo de Tecnología | Feb-2021 | Dic-2022 |
| | 16.1.3 | Reporte de debilidades de seguridad de la información | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer, documentar e implementar plan de contingencia | plan de contingencia | Grupo de Tecnología | Feb-2021 | Dic-2022 |
| | 16.1.4 | Valoración y decisión de eventos de seguridad de la información | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer, documentar e implementar plan de contingencia | plan de contingencia | Grupo de Tecnología | Feb-2021 | Dic-2022 |
| | 16.1.5 | Respuesta a incidentes de seguridad de la información | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer, documentar e implementar plan de contingencia | plan de contingencia | Grupo de Tecnología | Feb-2021 | Dic-2022 |
| | 16.1.6 | Aprendizaje de incidentes de seguridad de la información | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer, documentar e implementar plan de contingencia | plan de contingencia | Grupo de Tecnología | Feb-2021 | Dic-2022 |
| | 16.1.7 | Colección de evidencia | Aplicaciones y Software - Hardware - Equipos auxiliares | Establecer, documentar e implementar plan de contingencia | plan de contingencia | Grupo de Tecnología | Feb-2021 | Dic-2022 |
| 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio | 17,1 | Continuidad de la seguridad de la información | | | | | | |
| | 17.1.1 | Planeación de la continuidad de la seguridad de la información | Coordinador TIC - Usuarios Finales - Usuarios Externos | Establecer, documentar e implementar plan de continuidad del negocio | plan de continuidad del negocio | Grupo de Tecnología | Feb-2021 | Dic-2022 |
| | 17.1.2 | Implementación de la continuidad de la seguridad de la información | Coordinador TIC - Usuarios Finales - Usuarios Externos - Aplicaciones y Software - Hardware - Equipos auxiliares - Estudios previos y de conveniencia - Personal y Funcionarios de apoyo - Contrato de Servicios con Terceros - | Establecer, documentar e implementar plan de continuidad del negocio | plan de continuidad del negocio | Grupo de Tecnología | Feb-2021 | Dic-2022 |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 67 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|---|---|---|--|---------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Coordinador TIC - Usuarios Finales - Usuarios Externos - Aplicaciones y Software - Hardware - Equipos auxiliares - Estudios previos y de conveniencia - Personal y Funcionarios de apoyo - Contrato de Servicios con Terceros | Establecer, documentar e implementar plan de continuidad del negocio | plan de continuidad del negocio | Grupo de Tecnología | Feb-2021 | Dic-2022 |
| | 17.2 | Redundancias | | | | | | |
| | 17.2.1 | Disponibilidad de facilidades de procesamiento de información | Aplicaciones y Software - Instalaciones - Datos e Información - Soportes de información | Establecer, documentar e implementar políticas de desarrollo seguro de software | políticas de desarrollo seguro de software | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| 18 Cumplimiento | 18,1 | Cumplimiento con Requerimientos Legales y Contractuales | | | | | | |
| | 18.1.1 | Identificación de legislación aplicable y requerimientos contractuales | Aplicaciones y Software - Hardware - Equipos auxiliares - Personal y Funcionarios de apoyo - Contrato de Servicios con Terceros | Incluir dentro de los procedimientos y la declaración de aplicación de políticas de seguridad de la información, la normatividad, reglamentación y legislación respectiva | normatividad, reglamentación y legislación en materia de SPI en políticas y procedimientos | Grupo de Tecnología | Feb-2020 | Dic-2022 |
| | 18.1.2 | Derechos de propiedad intelectual (IPR) | Aplicaciones y Software | Establecer, documentar e implementar plan de verificación y seguimiento a licenciamiento de aplicaciones y software | plan de verificación y seguimiento a licenciamiento de aplicaciones y software | Grupo de Tecnología | Feb-2020 | Dic-2023 |
| | 18.1.3 | Protección de registros | Aplicaciones y Software | Establecer, documentar e implementar plan de verificación y seguimiento a licenciamiento de aplicaciones y software | plan de verificación y seguimiento a licenciamiento de aplicaciones y software | Grupo de Tecnología | Feb-2020 | Dic-2023 |
| | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 68 de 117 |

| ISO 27001:2013 Controles de Seguridad | | | Activos de Información | Actividad/Descripción | Evidencia o Soporte | Responsable | Fecha de Inicio | Fecha de Término |
|---------------------------------------|---------|---|--|--|---|---------------------------------------|-----------------|------------------|
| Cláusula | Sección | Objetivo de control / control | | | | | | |
| | 18.1.4 | Privacidad y protección de información personal identificable (PIR) | Datos e información – Usuarios finales | Establecer, documentar e implementar plan de capacitación, promoción, divulgación y aplicación de Ley 1273 de 2009 | plan de capacitación, promoción, divulgación y aplicación de Ley 1273 de 2009 | Grupo de Tecnología | Feb-2021 | Dic-2023 |
| | 18.1.5 | Regulación de controles criptográficos | SE EXCLUYE | SE EXCLUYE | | -- | | -- |
| | 18.2 | Revisiones de seguridad de la información | | | | | | |
| | 18.2.1 | Revisión independiente de seguridad de la información | Sistema Integrado de Gestión | Establecer, documentar e implementar planes de auditoría interna las políticas de SI | Cumplimiento de Indicadores de planes establecidos | Oficina de Control Interno de Gestión | Feb-2020 | Dic-2023 |
| | 18.2.2 | Cumplimiento con políticas y estándares de seguridad | Sistema Integrado de Gestión | Establecer, documentar e implementar planes de auditoría interna las políticas de SI | Cumplimiento de Indicadores de planes | Oficina de Control Interno de Gestión | Feb-2020 | Dic-2023 |
| | 18.2.3 | Revisión del cumplimiento técnico | Sistema Integrado de Gestión | Establecer, documentar e implementar planes de auditoría interna las políticas de SI | Cumplimiento de Indicadores de planes | Oficina de Control Interno de Gestión | Feb-2020 | Dic-2023 |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 69 de 117 |

12. CONCLUSIONES

- Se ha realizado hasta la fecha un diagnóstico efectivo a los activos de TI correspondientes a 11 de los 37 procesos de gestión de la Administración Central Departamental de la GOBERNACIÓN DEL HUILA, las amenazas y vulnerabilidades existentes, de modo que en el análisis y evaluación de riesgos, se identifica las deficiencias en infraestructura tecnológica para soportar la prestación de los servicios de TI a todas las áreas de la administración, generando la presentación de incidentes y eventos de indisponibilidad de servicios, entre otras implicaciones relacionadas con la ejecución de actividades y procesos misionales y estratégicos de la entidad.
- Así mismo, se identifica la necesidad apremiante de establecer y documentar lineamientos internos de seguridad y privacidad de la información, que faciliten la implementación de medidas y controles para la gestión de la información y los activos de TI de la entidad, a fin de optimizar los procesos y servicios ofertados a la ciudadanía.
- Respecto al talento humano, La GOBERNACIÓN DEL HUILA no cuenta con personal calificado en buenas prácticas de seguridad de la información, que a su vez permita crear, difundir y establecer una cultura organizacional en esta materia entre los funcionarios y áreas de la entidad. Los planes de capacitación y sensibilización internos dispuestos para el personal del área TIC, no incluyen áreas ni aspectos relacionados con el fortalecimiento de las competencias y habilidades específicas requeridas en materia de TI, de acuerdo a la normatividad, estándares y lineamientos vigentes a nivel nacional e internacional.

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Versión: 1 |
| | | Página 70 de 117 |

13. RECOMENDACIONES

- A través del presente documento, se da inicio a la adopción del Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio TIC, y alineado con la norma técnica ISO 27001, ISO 27005 e ISO 27017.
- A partir de esta adopción, se requiere establecer, documentar y aprobar los diferentes procedimientos, políticas y/o actividades que garanticen la seguridad y privacidad de la información, en los términos legales establecidos por el Gobierno Nacional y los acuerdos determinados con los usuarios y ciudadanos. Posteriormente se debe realizar seguimiento permanente y detallado a la ejecución de los mismos por parte de los funcionarios, contratistas y proveedores en las diferentes áreas y dependencias de la GOBERNACIÓN DEL HUILA.
- Es necesario crear, difundir y establecer una cultura organizacional en materia de seguridad y privacidad de la información, mediante capacitación y sensibilización a los funcionarios en este sentido, de acuerdo a la normatividad, estándares y lineamientos vigentes a nivel nacional e internacional.
- Así mismo, es necesario identificar las necesidades reales para cada área y dependencia, y realizar las adquisiciones o renovaciones que sean convenientes, para el desarrollo eficiente de las funciones de la entidad, evitando exposición a malware y debilidades de seguridad, producto de falta de soporte por parte de marcas fabricante o proveedores.
- En materia de software, se requiere verificar y actualizar si corresponde, el inventario de licenciamiento, tanto de sistemas operativos, sistemas de información, paquetes ofimáticos, etc., a fin de evaluar la capacidad de gestión y soporte de la infraestructura de TI.
- En materia de hardware, se considera importante la renovación del centro de datos y la red de cableado estructurado, de modo que permitan optimizar la prestación de los servicios que alojan, el rendimiento de los gestores de bases de datos, la centralización de los servicios, y el procesamiento de información a través de los aplicativos y sistemas de información correspondientes.
- En el caso del centro de datos, es primordial su renovación acorde a la normatividad y estándares técnicos establecidos en lo relacionado al cableado estructurado, reglamentación de instalaciones eléctricas, y centros de datos, que permita

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Versión: 1 |
| | | Página 71 de 117 |

garantizar disponibilidad de servicios, integridad y confidencialidad de la información, en la gestión de los sistemas de información incorporados. Por esta razón, es indispensable implementar un sistema de control de acceso eficiente y confiable, que restrinja el acceso a estos equipos, y permita realizar seguimiento al personal de soporte y las labores desarrolladas sobre los mismos. A esto se debe añadir que se debe realizar una inspección a todas las áreas y dependencias de la GOBERNACIÓN DEL HUILA, con el fin de evaluar las condiciones de cableado estructurado existente (puntos de red, puntos eléctricos normales y regulados), la capacidad existente y la capacidad necesaria en cuanto a la demanda por asignación de puestos de trabajo, equipos de cómputo, impresoras y escáner, entre otros equipos.

- Igualmente, se requiere ampliar el alcance en la planeación financiera de mantenimientos preventivos y correctivos sobre los activos tecnológicos de la entidad, para cubrir la demanda existente, y disminuir los tiempos de atención de fallas, incidentes y recuperación de incidentes y eventos de seguridad.
- Se recomienda realizar verificación de accesibilidad y auditoría periódica de seguridad web al portal web institucional de la GOBERNACIÓN DEL HUILA, y los diferentes aplicativos y sistemas de información que cuenten con entornos web, para evitar hallazgos y subsanar vulnerabilidades (exposición de datos sensibles, direccionamientos erróneos, entre otras) a través de alguna de las metodologías existentes (OWASP, OSSTMM, ISSAF).
- De igual forma es necesario establecer, difundir y fomentar la apropiación de buenas prácticas relacionadas con la realización de copias de seguridad y respaldo de información procesada por parte de todos los funcionarios de la entidad, para garantizar así la disponibilidad de la información, ante eventos o incidentes.
- Adicionalmente, incluir la gestión de dispositivos externos de almacenamiento de información (CD, DVD, memorias flash –USB-, discos duros externos, etc.), en los controles de seguridad a establecer e implementar, sensibilizando a los funcionarios para evitar acceso a información clasificada por parte de personas no autorizadas.
- Además, se requiere implementar y fortalecer la gestión de contraseñas para los diferentes servicios disponibles en la GOBERNACIÓN DEL HUILA, estableciendo niveles de complejidad, cambios periódicos, y almacenamiento seguro, para evitar incidentes y ataques cibernéticos.
- En los procesos de contratación relacionados con adquisición de software, sistemas de información, y aplicativos, es importante contar con directrices que reconozcan

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTIÓN: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 72 de 117 |

el papel del Grupo de Tecnología de la GOBERNACIÓN DEL HUILA, en la definición de requerimientos y capacidades necesarias y existentes en materia de TI, a fin de definir en las cláusulas que correspondan, aspectos como escalabilidad e interoperabilidad con otros sistemas, el tipo de uso y derechos de autor que contrata la entidad en dichos procesos, para que eventuales modificaciones, actualizaciones o complementos que se requieran, sean tenidas en cuenta en caso de que sea necesaria una asignación presupuestal adicional.

- Se debe verificar la inclusión del centro de datos y de los diferentes espacios destinados para la gestión y administración de activos de TI, en los planes de acción y cronogramas de actividades relacionadas con riesgos laborales (reubicar los diferentes elementos de seguridad y salud en el trabajo: extintores, botiquín, señalización, etc.), con el fin de que estén disponibles en caso de una situación de emergencia o contingencia, y no interfieran con el acceso a los equipos ni reduzcan los espacios de circulación señalados.

14. FUENTES DE INFORMACIÓN

- DAFP (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4
- DAFP (2018). Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018
- Durán Rodríguez, E., & Londoño de Perdomo, A. C. (2009). Resolución 223 de 2009 “Por medio del cual se conforma un grupo interno de trabajo permanente en la Secretaría General y se designa el Coordinador”.
- MINTIC (2009). Ley 1273 de 2009.
- MINTIC (2016). Modelo de Seguridad – Fortalecimiento de TI.
- MINTIC (2016). Guía de Gestión de Riesgos.
- MINTIC (2016). Guía para la Gestión y Clasificación de Activos de Información.
- MINTIC (2016). Modelo de Seguridad y Privacidad de la Información.
- MINTIC (2016). Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información.
- MinTIC. (2018). Gobierno Digital - Estrategia GEL.
- MINTIC (2018). Taller “Más seguridad, mejor región”. Estrategia Gobierno Digital.
- NTC ISO/IEC 27001: 2013. Sistemas de Gestión de la Seguridad de la Información
- NTC ISO/IEC 27005: 2009. Gestión del Riesgo en la Seguridad de la Información

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 73 de 117 |

- Pajarito Sánchez García, L. J. (2008). Gobernación del Huila. Gaceta Departamental. Decreto N° 1338 de 2008 “Por el cual se define la estructura orgánica de la Administración Departamental y se dictan otras disposiciones”.


| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 74 de 117 |

ANEXOS

1. Matrices de Identificación de Activos de Seguridad Digital

- Proceso de Sistemas de Información

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 75 de 117 |


| | | | |
|--|---|--|--|
|  GOBERNACIÓN DEL HUILA | SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | | Código: SGN-C048-G001-F05 |
| | CRITERIOS PARA IDENTIFICAR LA CRITICIDAD DE LOS ACTIVOS DE SEGURIDAD DIGITAL | | Fecha de aprobación: 04/09/2019 |
| | | | Versión 1 |
| | | | Página 1 de 1 |

| | |
|------------------------------|---|
| NOMBRE DEL PROCESO: | PLANEACIÓN - SISTEMAS DE INFORMACIÓN |
| OBJETIVO DEL PROCESO: | |

| PASOS | | | | | | | | | | | | | | | | |
|--|----------------|--|--|------------------------------|------------|----------------|-----------------------|---------------------|--------------|--|--|---|--|------|-------------------------------------|---------------|
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Criticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores y fallas | Ataques intencionados | | | | | |
| Base de datos de calidad de datos | Información | Entidades propietarias del dato | Lider de proceso Sistemas de Información | 3 | 1 | 1 | Alta | N.A | N.A | N.A | Corrupción de datos | Ausencia formal para la supervisión de registro de SGSI | N.A. | N.A | N.A. | N.A. |
| Base de datos de seguridad de datos | Información | Entidades propietarias del dato | Lider de proceso Sistemas de Información | 3 | 1 | 1 | Alta | N.A | N.A | Error de uso | N.A | Uso incorrecto de software y hardware | N.A. | N.A | N.A. | N.A. |
| Portal web Sistema de Información Regional sirhuila.gov.co | Software | Lider de proceso Sistemas de Información | Coordinador TIC | 3 | 3 | 1 | Media | N.A | N.A | Error de uso | N.A | Configuración incorrecta de parámetros | N.A. | N.A. | | |
| Equipos de computo | Hardware | Secretaría General | Lider de proceso Sistemas de Información | 3 | 3 | 1 | Media | N.A. | N.A. | Errores de mantenimiento o actualización de hardware | Hurto de Medios | Almacenamiento sin protección | Mantenimiento insuficiente de equipos de cómputo | N.A | N.A. | N.A. |
| Funcionarios del proceso | Personas | Secretaría General | Lider de proceso Sistemas de Información | 3 | 3 | 1 | Media | N.A. | N.A. | Ausencia de control del personal | Incumplimiento de la disponibilidad del personal | Ausencia del personal | N.A. | N.A | N.A. | N.A. |

| | | |
|--|---|--|
|  GOBERNACIÓN DEL HUILA |  SC4353-1 | CODIGO: SGN-C043-PL02 |
| | SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | Fecha Aprobación: 31 de Enero de 2020 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Versión: 1 |
| | | Página 76 de 117 |


• Proceso de Control y Auditorías

| | | | | | | | | | | | | | | | | | | | |
|--|--|---|---------------------------|------------------------------|------------|----------------|-----------------------|-------------------------------|---------------------------------|--|---|---------------------------------------|----------------------------|------|-------------------------------------|---------------|--|--|--|
|  GOBERNACION DEL HUILA | SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | | | | | | | | | | | Código: SGN-C048-G001-F05 | | | | | | | |
| | CRITERIOS PARA IDENTIFICAR LA CRITICIDAD DE LOS ACTIVOS DE SEGURIDAD DIGITAL | | | | | | | | | | | Fecha de aprobación: 04/09/2019 | | | | | | | |
| | | | | | | | | | | | | Versión 1 | | | | | | | |
| | | | | | | | | | | | | Página 1 de 1 | | | | | | | |
| NOMBRE DEL PROCESO: | CONTROL INTERNO | | | | | | | | | | | | | | | | | | |
| OBJETIVO DEL PROCESO: | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| PASOS | | | | | | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 | | | |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Críticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Critica Cibernética | Observaciones | | | |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores y fallas | Ataques intencionados | | | | | | | | |
| Información generada de la evaluación y seguimiento de los planes de mejoramiento por procesos | Información | Jefe de Oficina de Control Interno de Gestión | Profesional Universitario | 3 | 3 | 1 | Media | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | Modificación deliberada de la información | Uso incorrecto de software y hardware | N.A. | N.A. | N.A. | N.A. | | | |
| Información de evaluación a la gestión de la entidad | Información | Jefe de Oficina de Control Interno de Gestión | Profesional Universitario | 3 | 3 | 1 | Media | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | Modificación deliberada de la información | Uso incorrecto de software y hardware | N.A. | N.A. | N.A. | N.A. | | | |
| Equipos de computo | Hardware | Secretaria de Salud | Secretaria General | 3 | 2 | 1 | Media | Daños por desastres naturales | Daños debido a actividad humana | Errores de mantenimiento o actualización de hardware | Uso no previsto | Uso incorrecto de software y hardware | Mantenimiento insuficiente | N.A | N.A. | N.A. | | | |
| Funcionarios del proceso | Personas | Secretaria de Salud | Secretaria General | 3 | 3 | 1 | Media | N.A. | N.A. | Ausencia de control del personal | N.A | Ausencia del personal | N.A. | N.A | N.A. | N.A. | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 77 de 117 |


- Proceso de Gestión a la Dirección del SGSSS

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 78 de 117 |

|  GOBERNACION DEL HUILA | SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | | | | | | | | | | Código: SGN-C048-G001-F05 | | | | | |
|---|--|---|---|------------------------------|------------|----------------|-----------------------|-------------------------------|---------------------------------|--|--|--|---|--|-------------------------------------|---------------|
| | CRITERIOS PARA IDENTIFICAR LA CRITICIDAD DE LOS ACTIVOS DE SEGURIDAD DIGITAL | | | | | | | | | | Fecha de aprobación: 04/09/2019 | | | | | |
| | | | | | | | | | | | Versión 1 | | | | | |
| | | | | | | | | | | | Página 1 de 1 | | | | | |
| NOMBRE DEL PROCESO: | SALUD - GESTIÓN A LA DIRECCIÓN DEL SGSSS | | | | | | | | | | | | | | | |
| OBJETIVO DEL PROCESO: | | | | | | | | | | | | | | | | |
| PASOS | | | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Críticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores y fallas | Ataques intencionados | | | | | |
| Información presupuestal y financiera de las inversiones en la red pública de prestación de servicios en salud | Información | Secretaría de Salud | Área de Gestión de la Dirección del SGSSS | 2 | 1 | 1 | 1 | N.A. | N.A. | DILIGENCIAMIENTO ERRONEO DE LA INFORMACIÓN | MODIFICACIÓN INTENCIONAL DE LA INFORMACIÓN | Falta de planificación y desconocimiento normativo | Falencia en estudios y diseños | N.A. | | |
| Conceptos técnicos y viabilidades de infraestructura y dotación de la red pública de prestación de servicios en salud | Información | Secretaría de Salud | Área de Gestión de la Dirección del SGSSS | 2 | 1 | 1 | 1 | N.A. | N.A. | FALLAS EN EJECUCIÓN DE LOS PROYECTOS | MODIFICACIÓN INTENCIONAL DE LA INFORMACIÓN | Favorecimiento a terceros en la ejecución de los proyectos | N.A. | N.A. | | |
| Parámetros, requisitos, normatividad y regulaciones tecnicas para la operación del SGSSS | Información | Ministerio de Salud de la Protección Social | Secretaría de Salud | 3 | 1 | 1 | 1 | N.A. | N.A. | N.A. | N.A. | Desconocimiento normativo | Inestabilidad normativa | N.A. | | |
| Evaluación general de las direcciones locales de salud | Información | Secretaría de Salud | Área de Gestión de la Dirección del SGSSS | 2 | 1 | 1 | 1 | N.A. | N.A. | FALLAS EN LA EWALUACIÓN DE LAS DIRECCIONES LOCALES | N.A. | Subjetividad en la evaluación | N.A. | N.A. | | |
| Plataforma 2193 SIHO - Información sobre red publica de prestación de servicios en salud | Software | Ministerio de Salud de la Protección Social | Ministerio de Salud de la Protección Social | 1 | 1 | 1 | 1 | N.A. | N.A. | FALLAS EN EL APLICATIVO / DILIGENCIAMIENTO ERRONEO DE LA INFORMACIÓN | INGRESO DE DATOS CORRUPTOS (MAQUILLADA) | Ausencia de seguimiento permanente | N.A. | N.A. | | |
| Equipos de computo | Hardware | Secretaría de Salud | Secretaría General | 3 | 2 | 1 | 2 | Daños por desastres naturales | Daños debido a actividad humana | Errores de mantenimiento o actualización de hardware | Uso no previsto | Mantenimiento insuficiente | Falta de políticas de seguridad de la información | N.A | | |
| Funcionarios del proceso | Personas | Secretaría de Salud | Secretaría General | 1 | 1 | 1 | 1 | N.A. | N.A. | Ausencia de control del personal | N.A | Ausencia del personal | Falta de compromiso | Falta de actualización del manual de funciones | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 79 de 117 |

• Proceso de Prestación de Servicios de Salud


| | | |
|--|---|--|
|  GOBERNACION DEL HUILA | SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | Código: SGN-C048-G001-F05 |
| | CRITERIOS PARA IDENTIFICAR LA CRITICIDAD DE LOS ACTIVOS DE SEGURIDAD DIGITAL | Fecha de aprobación: 04/09/2019 |
| | | Versión 1 |
| | | Página 1 de 1 |

| PASOS | | | | | | | | | | | | | | | |
|---|----------------|---|---|------------------------------|------------|----------------|-----------------------|---|--|---|---|--|---|---|---------------|
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Criticidad del activo | Amenazas por activo | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores y fallas | | | | | |
| Sistema de Registro Especial de Prestadores de Salud - REPS | Software | Ministerio de Salud y Protección Social | Secretaria de Salud | 1 | 1 | 1 | 1 | N.A. | Avería de origen físico o lógico por colapso | Mal funcionamiento del software en flujos de trabajo específicos | N.A. | Capacidad insuficiente del software para soportar gran cantidad de usuarios cargando simultáneamente información | Error en la configuración del software para carga de información en flujos de trabajo específicos | N.A. | |
| Aplicativo extranet | Software | Lider Atencion al ciudadano | Coordinador TIC | 3 | 1 | 1 | 1 | N.A. | Avería de origen físico o lógico | Alteración accidental de la información | Modificación deliberada de la información | Fallas en servidor de app extranet | Falta de backup de la información | Falta de políticas de seguridad de la información | |
| Información sobre novedades presentadas por prestadores de servicios de salud | Información | Prestadores de Servicios de Salud | Lider del área de Habilitación - Administrador del REPS | 3 | 2 | 1 | 2 | Daños de documentos por lluvias y/o inundaciones | N.A. | N.A. | N.A. | Infraestructura física no adecuada para archivo de documentos | N.A. | N.A. | |
| Actas e informes de visitas de habilitación de servicios en salud. | Información | Secretaria de Salud | Lider del área de Habilitación - Administrador del REPS | 3 | 1 | 1 | 1 | Daños de documentos por lluvias y/o inundaciones | N.A. | Falta o error en el proceso de aval del informe y actas de visita | Acceso no autorizado / Divulgación de información | Infraestructura física no adecuada para archivo de documentos | Verificación deficiente para el aval de las actas e informes de visita por parte del funcionario líder de la visita | N.A. | |
| Equipos de computo | Hardware | Secretaria de Salud | Lider del área de Habilitación | 3 | 2 | 2 | 2 | Daños por desastres naturales | Daños debido a actividad humana | Errores de mantenimiento o actualización de hardware | Uso no previsto | Mantenimiento insuficiente o deficiente | Falta de políticas de seguridad de la información para controlar acceso | N.A. | |
| Funcionarios de apoyo al proceso (Equipo técnico de verificadores) | Personas | Secretaria de Salud | Lider del área de Habilitación | 3 | 1 | 1 | 1 | Enfermedad o muerte de personal a cargo del manejo de herramientas tecnológicas del área (temporal) | N.A. | Personal no idóneo y/o irresponsable frente al manejo de las herramientas tecnológicas del área | Abuso sobre derechos y permisos de acceso a herramientas tecnológicas | No disponibilidad de registro de auditoría y bitácora de usuarios integrados al precontractual | Ausencia de verificación y evaluación de competencias blandas en la fase precontractual | N.A. | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 80 de 117 |

- Proceso de Aseguramiento del SGSSS

| | | |
|--|---|---------------------------------------|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 81 de 117 |

| | | | | | | | | | | | | | | | | |
|--|--|---------------------|--|------------------------------|------------|----------------|-----------------------|----------------------------------|---|---|---|---|--|------|-------------------------------------|---|
|  GOBERNACION DEL HUILA | SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | | | | | | | | | | | Código: SGN-C048-G001-F05 | | | | |
| | CRITERIOS PARA IDENTIFICAR LA CRITICIDAD DE LOS ACTIVOS DE SEGURIDAD DIGITAL | | | | | | | | | | | Fecha de aprobación: 04/09/2019 | | | | |
| | | | | | | | | | | | | Versión 1 | | | | |
| | | | | | | | | | | | | Página 1 de 1 | | | | |
| NOMBRE DEL PROCESO: | SALUD - ASEGURAMIENTO DEL SGSSS | | | | | | | | | | | | | | | |
| OBJETIVO DEL PROCESO: | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| PASOS | | | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Criticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores y fallas | Ataques intencionados | | | | | |
| BDUA - Base de datos única de afiliados | Software | Ministerio de Salud | Profesional Universitario Proceso de Gestión a la Dirección | 3 | 1 | 1 | Alta | N.A. | Incumplimiento en el mantenimiento del software | MAL FUNCIONAMIENTO DEL SOFTWARE | N.A. | AUSENCIA DE CONTROL DE CAMBIOS EFICAZ | Respuesta inadecuada de mantenimiento del servicio | N.A. | SI | Propiedad del Ministerio de Salud. Consultar con MinTIC si ya fue reportado |
| SISHUILA - Plataforma de almacenamiento de bases de datos del SGSSS para todos los municipios | Software | Secretaria de Salud | Profesional Universitario Proceso de Gestión a la Dirección | 2 | 1 | 1 | Alta | N.A. | Averia de origen físico o lógico | Alteración accidental de la información | Modificación deliberada de la información | Fallas en servidor de SISHUILA | Falta de políticas de seguridad de la información | N.A. | N.A. | N.A. |
| Bases de datos de régimen contributivo | Información | Secretaria de Salud | Profesional Universitario Proceso de Gestión a la Dirección | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Errores en ingreso de información | Dstrucción de información | N.A. | N.A. | N.A. |
| Bases de datos de régimen subsidiado | Información | Secretaria de Salud | Profesional Universitario Proceso de Gestión a la Dirección | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Errores en ingreso de información | Dstrucción de información | N.A. | N.A. | N.A. |
| Aplicativo de inspección y vigilancia - SUPERSALUD | Software | SUPERSALUD | Profesional Universitario Proceso de Gestión al Aseguramiento del SGSSS | 2 | 1 | 1 | Alta | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE | N.A. | Software Nuevo o inmaduro | N.A. | N.A. | N.A. | N.A. |
| Población afiliada a régimen contributivo y subsidiado por EPS para todos los municipios del Departamento | Información | Secretaria de Salud | Lider de Gestión de Aseguramiento del SGSSS | 3 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Errores en ingreso de información | Dstrucción de información | N.A. | N.A. | N.A. |
| Matrices de recursos aplicados al régimen subsidiado por fuentes de financiación para todos los 37 municipios del Departamento | Información | Secretaria de Salud | Lider de Gestión de Aseguramiento del SGSSS | 3 | 2 | 1 | Media | Averia de origen físico o lógico | N.A. | Errores de los usuarios | Manipulación de programas | Descarga y uso no controlado del software | N.A. | N.A. | N.A. | N.A. |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 82 de 117 |

| | | | | | | | | | | | | | | | | |
|----------------------------------|----------|---------------------|--|---|---|---|------|-------------------------------|---------------------------------|--|-------------------------------|----------------------------|---|------|------|------|
| Equipos de computo | Hardware | Secretaría de Salud | Profesional Universitario Proceso de Gestión a la Dirección | 3 | 1 | 1 | Alta | Daños por desastres naturales | Daños debido a actividad humana | Errores de mantenimiento o actualización de hardware | Uso no previsto | Mantenimiento insuficiente | Falta de políticas de seguridad de la información | N.A. | N.A. | N.A. |
| Funcionarios de apoyo al proceso | Personas | Secretaría de Salud | Líder de Gestión de Aseguramiento del SGSSS | 3 | 1 | 1 | Alta | N.A. | N.A. | Indisponibilidad del personal | Indisponibilidad del personal | Ausencia del personal | N.A. | N.A. | N.A. | N.A. |

- Proceso de Salud Pública

| | | |
|---|--|---|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043-PL02</p> |
| | | <p>Fecha Aprobación: 31 de Enero de 2020</p> |
| | | <p>Versión: 1</p> |
| | | <p>Página 83 de 117</p> |
| <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | | |

| PASOS | | | | | | | | | | | | | | | | |
|---|----------------|-----------------------------|--|------------------------------|------------|----------------|-----------------------|--|---------------------------------|--|--|---|---|--|-------------------------------------|---------------|
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Críticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores y fallas | Ataques intencionados | | | | | |
| Base de datos de registro de entradas de muestras biológicas para supervisión | Información | Secretaria de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |
| Base de datos de registro de entradas de muestras biológicas para análisis | Información | Secretaria de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |
| Base de datos de registro de entradas de muestras ambientales para análisis | Información | Secretaria de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |
| Base de datos de pacientes y resultados de análisis de toma de muestras biológicas por programa, evento o patología | Información | Secretaria de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |
| SIVICAP- Sistema de Vigilancia de la Calidad del Agua Potable | Software | Instituto Nacional de Salud | Laboratorio de Salud Pública - Salud Ambiental | 2 | 1 | 1 | 1 | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE / DILIGENCIAMIENTO O ERRONEO DE LA INFORMACIÓN | INGRESO DE DATOS CORRUPTOS | Errores en ingreso de información | Destrucción de información | N.A. | | |
| EPIINFO - Software para vigilancia y verificación de alimentos y licores | Software | INVIMA | Laboratorio de Salud Pública | 2 | 1 | 1 | 1 | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE / DILIGENCIAMIENTO O ERRONEO DE LA INFORMACIÓN | INGRESO DE DATOS CORRUPTOS | Errores en ingreso de información | Destrucción de información | N.A. | | |
| PNCQ Internacional - Módulo Control de Calidad | Software | Secretaria de Salud | Laboratorio de Salud Pública | 2 | 1 | 1 | 1 | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE / DILIGENCIAMIENTO O ERRONEO DE LA INFORMACIÓN | INGRESO DE DATOS CORRUPTOS | Software Nuevo o inmaduro | N.A. | N.A. | | |

| | | | |
|---|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 | |
| | | Fecha Aprobación: 31 de Enero de 2020 | |
| | | Versión: 1 | |
| | | Página 84 de 117 | |
| PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | | | |

| | | | | | | | | | | | | | | | | |
|---|-------------|----------------------------------|------------------------------|---|---|---|---|--|----------------------------------|--|--|---|---|--|--|--|
| SISHUILA - Módulo Extranet | Software | Oficina de Atención al Ciudadano | Coordinación TIC | 2 | 1 | 1 | 1 | N.A. | Avería de origen físico o lógico | Alteración accidental de la información | Modificación deliberada de la información | Fallas en servidor de SISHUILA | Falta de políticas de seguridad de la información | N.A. | | |
| SIVILAB 2.0 - Sistema de Vigilancia de Laboratorio - Módulo de Muestras | Software | Instituto Nacional de Salud | Laboratorio de Salud Pública | 2 | 1 | 1 | 1 | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE / DILIGENCIAMIENTO O ERROREO DE LA INFORMACIÓN | INGRESO DE DATOS CORRUPTOS | Errores en ingreso de información | Dstrucción de información | N.A. | | |
| SIVIEN - Sistema de Vigilancia Entomológica | Software | Instituto Nacional de Salud | Laboratorio de Salud Pública | 2 | 1 | 1 | 1 | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE / DILIGENCIAMIENTO O ERROREO DE LA INFORMACIÓN | INGRESO DE DATOS CORRUPTOS | Errores en ingreso de información | Dstrucción de información | N.A. | | |
| Software REAL - Identificación de bacterias (microbiología) | Software | Secretaría de Salud | Laboratorio de Salud Pública | 2 | 1 | 1 | 1 | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE / DILIGENCIAMIENTO O ERROREO DE LA INFORMACIÓN | INGRESO DE DATOS CORRUPTOS | Software Nuevo o inmaduro | N.A. | N.A. | | |
| Software OBSERVA - Identificación de bacterias (microbiología) | Software | Secretaría de Salud | Laboratorio de Salud Pública | 2 | 1 | 1 | 1 | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE / DILIGENCIAMIENTO O ERROREO DE LA INFORMACIÓN | INGRESO DE DATOS CORRUPTOS | Errores en ingreso de información | Dstrucción de información | N.A. | | |
| Reportes a partir de Indices de Riesgo de Calidad del Agua Potable - IRCA | Información | Instituto Nacional de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |
| Reportes e informe de resultados de análisis de muestras a INVIMA | Información | INVIMA | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |
| Resultados y informes de muestras para supervisión | Información | Secretaría de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |
| Informes de evaluación externa de desempeño nacional por cada programa activo para el talento humano y metodologías de atención de eventos de interés en salud pública ESPI | Información | Instituto Nacional de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |
| Informes de evaluación externa de desempeño internacional por cada programa activo para el talento humano y metodologías de atención de eventos de interés en salud pública ESPII | Información | Secretaría de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |
| Informes de desempeño para laboratorios de la Red Pública de Servicios en Salud | Información | Secretaría de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos | | |
| Informe trimestral de programas de ETV - Enfermedades Transmitidas por Vectores - a MinSalud | Información | Secretaría de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 85 de 117 |

| | | | | | | | | | | | | | | | | |
|---|-------------|----------------------------------|------------------------------|---|---|---|---|---|----------------------------------|---|---|--|--|--|--|--|
| Informes anuales de los programas de Laboratorio de Salud Pública a MinSalud | Información | Secretaría de Salud | Laboratorio de Salud Pública | 3 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de bases de datos | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos | | |
| Informe de gestión del subproceso de Laboratorio de Salud Pública | Información | Secretaría de Salud | Laboratorio de Salud Pública | 3 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de antivirus | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos | | |
| Resultados de patologías de mortalidades por eventos de interés en salud publica | Información | Instituto Nacional de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de adquisición y actualización de licencias de gestores de | Falta de backup de la información y de actualización de antivirus | Falta de dotación y renovación de equipos tecnológicos | | |
| Actas de visitas para verificación de estándares a laboratorios de laboratorios de la Red Publica | Información | Secretaría de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de procedimientos para acceso y préstamo | Falta de repositorios adecuados para archivar | N.A. | | |
| Actas de visitas por programa a laboratorios, direcciones locales y ESEs | Información | Secretaría de Salud | Laboratorio de Salud Pública | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de procedimientos para acceso y préstamo | Falta de repositorios adecuados para archivar | N.A. | | |
| Actas de comité por programa de la Secretaría de Salud | Información | Secretaría de Salud | Laboratorio de Salud Pública | 2 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Diligenciamiento erróneo de información de bases de datos | Modificación Intencional de la Información | Falta de procedimientos para acceso y préstamo | Falta de repositorios adecuados para archivar | N.A. | | |
| Sistema de Comunicaciones Oficiales | Software | Oficina de Atención al Ciudadano | Coordinación TIC | 2 | 1 | 1 | 1 | N.A. | Avería de origen físico o lógico | Alteración accidental de la información | Modificación deliberada de la información | Fallas en servidor de app extranet | Falta de backup de la información | Falta de políticas de seguridad de la información | | |
| Protocolos de validación | Información | Secretaría de Salud | Laboratorio Salud Publica | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Daño accidental de documentos | Hurto de documentos | Falta de procedimientos para acceso y préstamo | Falta de repositorios adecuados para archivar | N.A. | | |
| Equipos de computo | Hardware | Secretaría de Salud | Laboratorio Salud Publica | 2 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Errores de mantenimiento o actualización de hardware | Uso no previsto | Instalaciones físicas deficientes | Mantenimiento insuficiente o deficiente | Instalaciones electricas insuficientes | | |
| Equipos de laboratorio | Hardware | Secretaría de Salud | Laboratorio Salud Publica | 1 | 1 | 1 | 1 | Daños por desastres naturales / daños por inundación y lluvias | Daños debido a actividad humana | Errores de mantenimiento o actualización de hardware | Uso no previsto | Falta de mantenimiento y calibracion de equipos de laboratorio | Instalaciones físicas deficientes | Instalaciones electricas insuficientes | | |
| Funcionarios de apoyo al proceso (Equipo técnico) | Personas | Secretaría de Salud | Laboratorio Salud Publica | 2 | 1 | 1 | 1 | Enfermedad o muerte de personal a cargo del manejo de herramientas tecnológicas del área (temporal) | N.A. | Personal no idóneo y/o irresponsable frente al manejo de las herramientas tecnológicas del área | Abuso sobre derechos y permisos de acceso a herramientas tecnológicas | No disponibilidad de registro de auditoría y bitácora de usuarios integrados al software | Ausencia de verificación y evaluación de competencias blandas en la fase precontractual del personal | N.A. | | |

- Proceso de Gestión del Recurso Físico

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 86 de 117 |

| PASOS | | | | | | | | | | | | | | | | |
|--|----------------|---|---------------------------|------------------------------|------------|----------------|-----------------------|-------------------------------|----------------------------------|--|---|---|---|---|-------------------------------------|---------------|
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Críticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores | Ataques | | | | | |
| Inventario general de activos de la Administración Central | Información | Secretaría General | Líder de Recursos Físicos | 2 | 1 | 1 | Alta | N.A. | N.A. | De Configuración / Del Administrador / Alteración accidental de la información | N.A | Error en el diligenciamiento de la información | Falta de backup de la información | Falta de políticas de seguridad de la información | N.A. | N.A. |
| SIFA - Sistema de Información Financiera - Módulo Almacén | Software | Secretaría General - Secretaría de Hacienda | Líder de Recursos Físicos | 2 | 1 | 1 | Alta | N.A. | Avería de origen físico o lógico | Alteración accidental de la información | Modificación deliberada de la información | Fallas en servidor de app SIFA | Falta de backup de la información | Falta de políticas de seguridad de la información | N.A. | N.A. |
| Informes periódicos de saldos y movimientos de activos | Información | Secretaría General | Líder de Recursos Físicos | 2 | 1 | 1 | Alta | N.A. | N.A. | N.A | Acceso no autorizado a la información | Falta de políticas de seguridad de la información | N.A | N.A. | N.A. | N.A. |
| Contratación de compraventa, suministros, o donaciones | Información | Ordenador del gasto | Líder de Recursos Físicos | 2 | 1 | 1 | Alta | N.A. | N.A. | Alteración accidental de la información | N.A | Ausencia de auditorías regulares | Falta de políticas de seguridad de la información | N.A. | N.A. | N.A. |
| Equipos de computo | Hardware | Secretaría General | Líder de Recursos Físicos | 3 | 2 | 2 | Media | Daños por desastres naturales | Daños debido a actividad humana | Errores de mantenimiento o actualización de hardware | Uso no previsto | Mantenimiento insuficiente | Falta de políticas de seguridad de la información | N.A. | | |
| Funcionarios de apoyo al proceso | Personas | Secretaría General | Líder de Recursos Físicos | 3 | 1 | 1 | Alta | N.A. | N.A. | Indisponibilidad del personal | Indisponibilidad del personal | Ausencia del personal | N.A. | N.A. | N.A. | N.A. |

• Proceso de Mejora Continua

| PASOS | | | | | | | | | | | | | | | | |
|--|----------------|-----------------------------|---------------------|------------------------------|------------|----------------|-----------------------|----------------------------------|----------------------------------|--|---|------------------------------------|---|---|-------------------------------------|---------------|
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Críticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores | Ataques | | | | | |
| Informacion del SIG | Información | Gerente SIG | Gerente SIG | 3 | 1 | 1 | Alta | N.A. | N.A. | Destrucción de la información | Destrucción de la información | Fallas en conectividad a internet | Falta de backup de la información | Falta de políticas de seguridad de la información | N.A. | N.A. |
| Aplicativo extranet | Software | Lider Atencion al ciudadano | Coordinador TIC | 3 | 1 | 1 | Alta | N.A. | Averia de origen fisico o lógico | Alteración accidental de la información | Modificación deliberada de la información | Fallas en servidor de app extranet | Falta de backup de la información | Falta de políticas de seguridad de la información | N.A. | N.A. |
| Funcionarios de apoyo al proceso | Personas | Secretaría General | Gerente SIG | 3 | 1 | 1 | Alta | N.A. | N.A. | Indisponibilidad del personal | Indisponibilidad del personal | Ausencia del personal | | | N.A. | N.A. |
| Acompañamiento a la implementación y mejora continua del SIG | Servicios | Secretaría General | Gerente SIG | 3 | 1 | 1 | Alta | N.A. | N.A. | Alteración accidental de la información | Destrucción de la información | Falta de backup de la información | Falta de políticas de seguridad de la información | | N.A. | N.A. |
| Herramientas tecnologicas para seguimiento del SIG | Software | Secretaria General | Gerente SIG | 2 | 1 | 1 | Alta | Averia de origen fisico o lógico | N.A. | Errores de los usuarios | Manipulación de programas | Fallas en conectividad a internet | | | N.A. | N.A. |
| Equipos de computo | Hardware | Secretaría General | Gerente SIG | 3 | 2 | 2 | Media | Daños por desastres naturales | Daños debido a actividad humana | Errores de mantenimiento o actualización de hardware | Uso no previsto | Mantenimiento insuficiente | Falta de políticas de seguridad de la información | | N.A. | N.A. |

• Proceso de Calidad del Servicio Educativo en Educación Preescolar, Básica y Media

| | | |
|---|--|---|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043-PL02</p> |
| | | <p>Fecha Aprobación: 31 de Enero de 2020</p> |
| | | <p>Versión: 1</p> |
| | | <p>Página 87 de 117</p> |
| <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | | |

| PASOS | | | | | | | | | | | | | | | | |
|---|----------------|-------------------------|--|------------------------------|------------|----------------|-----------------------|---------------------|-------------------------------------|--|---|--|--|--|-------------------------------------|---------------|
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Críticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores y fallas | Ataques intenciona- dos | | | | | |
| Portal virtual educativo www.virtual.huila.edu.co | Software | Secretaría de Educación | Profesional Universitario - Lider de Gestion de Uso y Apropiación TIC - Lider de Calidad y Pertinencia Educativa | 3 | 1 | 1 | Alta | N.A. | N.A. | Errores de mantenimiento / actualización de programas (software) | Uso no previsto / Suplantación de la identidad del usuario / Acceso no autorizado | Cambio del administrador del portal web | Tercerización del servicio de administración de centro de datos | Descuido de usuarios en manejo de datos de acceso | N.A. | N.A. |
| MISEDH - Mi Inventario de la Secretaría de Educación Departamental | Software | Secretaría de Educación | Lider de Gestion de Uso y Apropiación TIC | 2 | 1 | 1 | Alta | N.A. | Avería de origen físico o lógico | ALTERACION ACCIDENTAL DE LA INFORMACION | Modificación deliberada de la información | Descuido de usuarios en manejo de datos de acceso | Criterios sujetos a cambios periódicos para la estructuración de la información y bases de datos | N.A. | N.A. | N.A. |
| Reporte de planes de mantenimiento anuales de cada establecimiento educativo oficial de los municipios no certificados en Educación del Departamento | Información | Secretaría de Educación | Lider de Gestion de Uso y Apropiación TIC | 3 | 1 | 2 | Media | N.A. | Avería de origen físico o lógico | Errores de los usuarios / ALTERACION ACCIDENTAL DE LA INFORMACION / Destrucción de la información | Modificación deliberada de la información | Criterios sujetos a cambios periódicos para la estructuración de la información y bases de datos | N.A. | N.A. | N.A. | N.A. |
| Formulario de indicador de gestión del uso y apropiación de tecnologías de la información | Software | Secretaría de Educación | Lider de Gestion de Uso y Apropiación TIC | 2 | 1 | 2 | Media | N.A. | N.A. | Mal FUNCIONAMIENTO DEL SOFTWARE | Suplantación de la identidad del usuario | Ausencia de autenticación de usuarios | Uso no previsto | N.A. | N.A. | N.A. |
| Información sobre novedades, experiencias, y formación del talento humano, para el uso y apropiación de TIC en entornos educativos | Información | Secretaría de Educación | Lider de Gestion de Uso y Apropiación TIC | 2 | 1 | 2 | Media | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | Modificación deliberada de la información | Desconocimiento de la información sobre experiencias | Uso incorrecto del software (registro adicional de participantes) | N.A. | N.A. | N.A. |

- Proceso de Cobertura del Servicio Educativo

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | |
| | | |
| | | |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 88 de 117 |

| PASOS | | | | | | | | | | | | | | | | |
|--|----------------|--|---|------------------------------|------------|----------------|-----------------------|---------------------|--------------|--|--|--|--|------|-------------------------------------|--|
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Críticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores y fallas | Ataques intencionados | | | | | |
| Sistema de Información de Matrícula (SIMAT) | Software | Ministerio de Educación | Secretario de Educación | 1 | 1 | 1 | Alta | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE | N.A. | AUSENCIA DE CONTROL DE CAMBIOS EFICAZ | N.A. | N.A. | SI | Propiedad del activo del MinEduación. Consultar con el MinTIC si existe el reporte del activo al CSIRT |
| Información obtenida sobre matrícula escolar en la establecimientos educativos oficiales y no oficiales de los municipios no certificados del departamento del Huila | Información | Rectores Instituciones Educativas Oficiales y no Oficiales | Ministerio de Educación - Secretario de Educación Departamental - Secretario de Educación Municipal | 1 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | Modificación deliberada de la información | Uso indebido de permisos de acceso a la información | Ausencia de procedimientos para el manejo de información clasificada | N.A. | SI | Consultar con el MinTIC si el MinEduación reportó el activo |
| Reportes e informes estadísticos generados a partir de la información suministrada por las EEO y NO de municipios no certificados del departamento del Huila | Información | Secretaria de Educación | Lider de proceso de Gestión de Cobertura Educativa - Administrador de SIMAT (Profesional Universitario) | 2 | 1 | 1 | Alta | N.A. | N.A. | ERRORES DE LOS USUARIOS QUE INGRESA INFORMACIÓN AL SIMAT | N.A. | Uso incorrecto de software | N.A. | N.A. | SI | Impactan en la generación de estrategias y toma de decisiones a nivel departamental |
| Directorio Único de Establecimientos Educativos - DUE | Software | Ministerio de Educación | Secretario de Educación | 2 | 1 | 1 | Alta | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE | N.A. | AUSENCIA DE CONTROL DE CAMBIOS EFICAZ | N.A. | N.A. | SI | Consultar con el MinTIC si el MinEduación reportó el activo |
| Información sobre reconocimiento oficial de establecimientos educativos oficiales y no oficiales de municipios no certificados | Información | Secretaria de Educación | Inspección y Vigilancia - Cobertura Educativa | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE INFORMACION | AUSENCIA DE PROCEDIMIENTOS PARA EL MANEJO DE INFORMACION CLASIFICADA | Errores en ingreso de información relacionada en actos administrativos de establecimientos educativos oficiales y no oficiales de los municipios no certificados | N.A. | N.A. | N.A. | N.A. |
| Sistema de Información de Sedes Educativas | Software | DANE | Secretario de Educación | 1 | 1 | 1 | Alta | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE | N.A. | AUSENCIA DE CONTROL DE CAMBIOS EFICAZ | N.A. | N.A. | SI | Consultar con el MinTIC si el DANE reportó el activo |
| Formulario Electrónico C600 | Software | DANE | Secretario de Educación | 2 | 2 | 1 | Media | N.A. | N.A. | Alteración accidental de la información | Modificación deliberada de la información | Facilidad de editar la herramienta | N.A. | N.A. | N.A. | N.A. |
| Información sobre novedades en establecimientos educativos oficiales y no oficiales de municipios no certificados | Información | DANE - Secretario de Educación | Inspección y Vigilancia - Comité de Cobertura Educativa | 2 | 2 | 1 | Media | N.A. | N.A. | ALTERACION ACCIDENTAL DE INFORMACION | N.A. | Errores en ingreso de información relacionada en actos administrativos de establecimientos educativos oficiales y no oficiales de los municipios no certificados | N.A. | N.A. | SI | Consultar con el MinTIC si el DANE reportó el activo |
| SIMPADE - Sistema de Información para el Monitoreo, la Prevención y el Analisis de la Deserción Escolar | Software | Ministerio de Educación | Lider de proceso de Gestión de Cobertura Educativa - Operador de SIMPADE (Profesional de Apoyo Técnico) | 2 | 1 | 1 | Alta | N.A. | N.A. | MAL FUNCIONAMIENTO DEL SOFTWARE | N.A. | AUSENCIA DE CONTROL DE CAMBIOS EFICAZ | N.A. | N.A. | SI | Propiedad del activo del MinEduación. Consultar con el MinTIC si existe el reporte del activo al CSIRT |



CODIGO: SGN-C043-PL02

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

| | |
|-------------------|---------------------|
| Fecha Aprobación: | 31 de Enero de 2020 |
|-------------------|---------------------|

Versión: 1

Página 89 de 117

[illegible]

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 90 de 117 |

| | | | | | | | | | | | | | | | | |
|---|-------------|--|---|---|---|---|-------|------|------|---|---|---|--|------|------|---|
| Informe de hallazgos sobre establecimientos educativos oficiales y no oficiales de municipios no certificados del departamento | Información | Secretaría de Educación | Director de Núcleo Educativo - Gestión de Cobertura Educativa | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | DIVULGACION NO AUTORIZADA DE INFORMACION | Incumplimiento de los plazos establecidos para la implementación de las acciones de mejora continua en los procesos | N.A. | N.A. | N.A. | N.A. |
| Informe final de auditoría al proceso de cobertura educativa en los establecimientos educativos oficiales y no oficiales de municipios no certificados del departamento | Información | Secretaría de Educación | Director de Núcleo Educativo - Gestión de Cobertura Educativa | 3 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Incumplimiento de los plazos establecidos para la implementación de las acciones de mejora continua en los procesos | N.A. | N.A. | N.A. | N.A. |
| Formato de auditoría al proceso de gestión de cobertura a establecimientos educativos - SED-C053-P638-F02 | Software | Secretaría de Educación | Director de Núcleo Educativo - Gestión de Cobertura Educativa | 3 | 2 | 2 | Media | N.A. | N.A. | Alteración accidental de la información | Modificación deliberada de la información | Errores en ingreso de información relacionada | | | | |
| Formato de auditoría a la etapa de matrícula sede educativa diferente a la sede principal - SED-C053-P638-F03 | Software | Secretaría de Educación | Director de Núcleo Educativo - Gestión de Cobertura Educativa | 3 | 2 | 2 | Media | N.A. | N.A. | Alteración accidental de la información | Modificación deliberada de la información | Errores en ingreso de información relacionada | | | | |
| Formato de Seguimiento a Hallazgos "Auditoría de Matrícula" SED-C053-P638-F05 | Software | Secretaría de Educación | Director de Núcleo Educativo - Gestión de Cobertura Educativa | 3 | 2 | 2 | Media | N.A. | N.A. | Alteración accidental de la información | Modificación deliberada de la información | Errores en ingreso de información relacionada | | | | |
| Formato Control de Asistencia SED-C053-F02 | Software | Secretaría de Educación | Director de Núcleo Educativo - Gestión de Cobertura Educativa | 3 | 2 | 2 | Media | N.A. | N.A. | Alteración accidental de la información | Modificación deliberada de la información | Errores en ingreso de información relacionada | | | | |
| Registro de Entrega de documentos u otros elementos en gestión de matrícula SED-C053-P634-F02 | Software | Secretaría de Educación | Director de Núcleo Educativo - Gestión de Cobertura Educativa | 3 | 2 | 2 | Media | N.A. | N.A. | Alteración accidental de la información | Modificación deliberada de la información | Errores en ingreso de información relacionada | | | | |
| Reporte de novedades en la matrícula de la población escolar y ejecución de proyectos etnoeducativos en establecimientos educativos indígenas de municipios no certificados | Información | Rectores Instituciones Educativas Oficiales y no Oficiales | Líder de proceso de Gestión de Cobertura Educativa - Administrador de SIMAT (Profesional Universitario) | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Uso indebido de permisos de acceso a la información | Ausencia de procedimientos para el manejo de información clasificada | | | |
| Formato Único de Contratación - FUC | Software | Ministerio de Educación | Profesional Universitario - Supervisión a Contratación de Servicios Educativos Indígenas Propios | 2 | 2 | 1 | Media | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | Modificación deliberada de la información | Errores en ingreso de información relacionada | | | | Información sobre establecimientos educativos indígenas y normalistas |
| Propuesta de canasta educativa para población escolar de establecimientos educativos indígenas | Información | Representante de comunidad indígena - CRIHU | Profesional Universitario - Supervisión a Contratación de Servicios Educativos Indígenas Propios | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | Modificación deliberada de la información | Uso indebido de permisos de acceso a la información | | | | |


| | | | |
|---|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 | |
| | | Fecha Aprobación: 31 de Enero de 2020 | |
| | | Versión: 1 | |
| | | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Página 91 de 117 | |

| | | | | | | | | | | | | | | | | |
|---|-------------|--|--|---|---|---|-------|-------------------------------|---------------------------------|--|-----------------------------------|---|---|--|------|--|
| Reporte de novedades de la administración del servicio educativo de la congregación de los hermanos de las escuelas cristianas y resultados de implementación estrategias de desarrollo pedagógico en establecimientos educativos oficiales | Información | Secretario de Educación | Profesional Universitario - Supervisión a Contratación de Servicios Educativos | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Uso indebido de permisos de acceso a la información | | | | Administración del servicio educativo realizada por esta persona jurídica, debido a falta de rector. |
| Información sobre apropiación cultural afrocolombiana en los modelos educativos de establecimientos educativos oficiales de los municipios con mayor población educativa afrocolombiana | Información | Secretario de Educación | Profesional Universitario - Supervisión a Contratación de Servicios Educativos | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Errores en ingreso de información relacionada | | | | Objetivo: implementación de cátedra de estudio afrocolombiano en Modelos educativo institucional |
| Información sobre necesidades y solicitudes de acceso educativo | Información | Rectores Instituciones Educativas Oficiales | Profesional Universitario - Supervisión a Contratación de Servicios Educativos | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Errores en ingreso de información relacionada | | | | |
| Actas de comité técnico municipal directivo docente | Información | Comités Técnicos Municipales Directivos Docentes | Profesional Universitario - Supervisión a Contratación de Servicios Educativos | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Uso indebido de permisos de acceso a la información | | | | |
| Proyectos educativos institucionales para atención de necesidades y solicitudes de acceso educativo | Información | Rectores Instituciones Educativas Oficiales | Profesional Universitario - Supervisión a Contratación de Servicios Educativos | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Uso indebido de permisos de acceso a la información | | | | |
| Información sobre visitas técnicas de validación de necesidades y solicitudes de acceso educativo | Información | Secretario de Educación | Profesional Universitario - Supervisión a Contratación de Servicios Educativos | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | N.A. | Errores en ingreso de información relacionada | | | | |
| Actas de comité departamental de cobertura educativa | Información | Comité Departamental de Cobertura Educativa | Profesional Universitario - Supervisión a Contratación de Servicios Educativos | 2 | 1 | 1 | Alta | N.A. | N.A. | ALTERACION ACCIDENTAL DE LA INFORMACION | ERROR EN EL USO DE LA INFORMACIÓN | Ausencia de documentación relacionada | | | | |
| Equipos de computo | Hardware | Secretaria General | Líder de proceso de Gestión de Cobertura Educativa | 3 | 2 | 2 | Media | Daños por desastres naturales | Daños debido a actividad humana | Errores de mantenimiento o actualización de hardware | Uso no previsto | Mantenimiento insuficiente | Falta de políticas de seguridad de la información | | N.A. | N.A. |
| Funcionarios de apoyo al proceso | Personas | Secretaria General | Líder de proceso de Gestión de Cobertura Educativa | 3 | 1 | 1 | Alta | N.A. | N.A. | Indisponibilidad del personal | Indisponibilidad del personal | Ausencia del personal | | | N.A. | N.A. |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 92 de 117 |

- Proceso de Inspección y Vigilancia de los Establecimientos Educativos

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 93 de 117 |

| | | |
|--|---|--|
|  GOBERNACIÓN DEL HUILA | SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | Código: SGN-C048-G001-F05 |
| | CRITERIOS PARA IDENTIFICAR LA CRITICIDAD DE LOS ACTIVOS DE SEGURIDAD DIGITAL | Fecha de aprobación: 04/09/2019 |
| | | Versión 1 |
| | | Página 1 de 1 |

| | |
|------------------------------|--------------------------------------|
| NOMBRE DEL PROCESO: | EDUCACIÓN - CALIDAD EDUCATIVA |
| OBJETIVO DEL PROCESO: | |

| PASOS | | | | | | | | | | | | | | | | |
|--|----------------|-------------------------|--|------------------------------|------------|----------------|-----------------------|---------------------|----------------------------------|---|---|--|--|---|-------------------------------------|---------------|
| 1 | 2 | 3 | 4 | 5 | | | 6 | 7 | | | | 8 | | | 9 | 10 |
| Activos de Seguridad digital asociados al proceso | Tipo de Activo | Dueño del Activo | Custodia del Activo | Clasificación de los activos | | | Criticidad del activo | Amenazas por activo | | | | Causas / Vulnerabilidades | | | Infraestructura Crítica Cibernética | Observaciones |
| | | | | Confidencialidad | Integridad | Disponibilidad | | Naturales | Industriales | Errores y fallas | Ataques intencionados | | | | | |
| Portal virtual educativo www.virtual.huila.edu.co | Software | Secretaría de Educación | Profesional Universitario - Líder de Gestion de Uso y Apropiación TIC - Líder de Calidad y Pertinencia Educativa | 3 | 1 | 1 | Alta | N.A | N.A | Errores de mantenimiento / actualización de programas (software) | Uso no previsto / Suplantación de la identidad del usuario / Acceso no autorizado | Cambio del administrador del portal web | Tercerización del servicio de administración de centro de datos | Descuido de usuarios en manejo de datos de acceso | N.A. | N.A. |
| MISEDH - Mi Inventario de la Secretaría de Educación Departamental | Software | Secretaría de Educación | Líder de Gestion de Uso y Apropiación TIC | 2 | 1 | 1 | Alta | N.A | Avería de origen físico o lógico | ALTERACION ACCIDENTAL DE LA INFORMACION | Modificación deliberada de la información | Descuido de usuarios en manejo de datos de acceso | Criterios sujetos a cambios periódicos para la estructuración de la información y bases de datos | N.A | N.A. | N.A. |
| Reporte de planes de mantenimiento anuales de cada establecimiento educativo oficial de los municipios no certificados en Educación del Departamento | Información | Secretaría de Educación | Líder de Gestion de Uso y Apropiación TIC | 3 | 1 | 2 | Media | N.A | Avería de origen físico o lógico | Errores de los usuarios / ALTERACION ACCIDENTAL DE LA INFORMACION / Destrucción de la información | Modificación deliberada de la información | Criterios sujetos a cambios periódicos para la estructuración de la información y bases de datos | N.A. | N.A | N.A. | N.A. |
| Formulario de indicador de gestión del uso y apropiación de tecnologías de la información | Software | Secretaría de Educación | Líder de Gestion de Uso y Apropiación TIC | 2 | 1 | 2 | Media | N.A | N.A | MAL FUNCIONAMIENTO DEL SOFTWARE | Suplantación de la identidad del usuario | Ausencia de autenticación de usuarios | Uso no previsto | N.A | N.A. | N.A. |
| Información sobre novedades, experiencias, y formación del talento humano, para el uso y apropiación de TIC en entornos educativos | Información | Secretaría de Educación | Líder de Gestion de Uso y Apropiación TIC | 2 | 1 | 2 | Media | N.A | N.A | ALTERACION ACCIDENTAL DE LA INFORMACION | Modificación deliberada de la información | Desconocimiento de la información sobre experiencias | Uso incorrecto del software (registro adicional de participantes) | N.A | N.A. | N.A. |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 94 de 117 |

ANEXOS

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 95 de 117 |

2. Matrices de Identificación y Valoración de Riesgos de Seguridad Digital

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 96 de 117 |

- Proceso de Sistemas de Información

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 97 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|------------------------------------|---|---|---|----------------------|------------------------------|---|--|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 4 | Gestión de Sistemas de Información | | PÉRDIDA DE DISPONIBILIDAD DE SISTEMA DE INFORMACIÓN REGIONAL Y EQUIPOS DE CÓMPUTO | seguridad digital | Otros | Directivo y profesional | Ausencia formal para la supervisión de registro de SGSI | Inhabilitación de sistema de información y reacción a eventos de seguridad y contingencias |
| | | | | | | | Uso incorrecto de software y hardware | Publicación de datos e información erróneos |
| | | | | | | | Configuración incorrecta de parámetros | Inhabilitación de sistema de información |
| | | | | | | | Almacenamiento sin protección | Acceso no autorizado a información clasificada |
| | | | | | | | Mantenimiento insuficiente de equipos de cómputo | Dificultad en labores de administración de sistema de información y bases de datos |
| | | | | | | | Ausencia de personal | Incumplimiento de funciones y obligaciones |
| 5 | Gestión de Sistemas de Información | | PÉRDIDA DE INTEGRIDAD DE DATO | seguridad digital | Otros | Directivo y profesional | Ausencia formal para la supervisión de registro de SGSI | Hallazgos de los entes de control |
| | | | | | | | Uso incorrecto de software y hardware | Deterioro de imagen institucional |



SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG

CODIGO: SGN-C043-PL02

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

| |
|---|
| <p>Fecha Aprobación: 31 de Enero de 2020</p> |
|---|

Versión: 1

Página 98 de117

| FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------------|---------|----------|-------------|--------------|-------|----------|-------|--------------|---|------|----------|------|---|-------------------------------------|--|---------------------------------|--|--|--|---|--------------|------------|---------|---|--|--|-------|----------|----------------------------|--------------|---------|---------|----------|--------------------------------|---|---|
| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO INHERENTE | | | | | PROBABILIDAD (ver hoja 2.1) | | |
| Rara vez | Improbable | Posible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control | Calificación de la ejecución del control | Solidez individual del control: | Peso en la evaluación del diseño del control SI=100 NO=0 | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: Directamente o No disminuye ? | Controles ayudan a disminuir el impacto ? Directamente o Indirectamente o No disminuye ? | Rara vez | Improbable | Posible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | | |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | 1 | 2 | | | | | | 3 | 4 | 5 | Fuerte (96-100) Moderado (86-95) Débil (0-85) | Fuerte: Siempre se ejecuta Moderado: Algunas veces se ejecuta Débil: No se ejecuta | Fuerte = 100 Moderado=50 Débil=0 | 1 | 2 | 3 | 4 | | | | | 5 | 1 |
| 4 | | | | | 5 | | | | | Extremo | | | | | No | Sin control | | | | Moderado | Directamente | No disminuye | 3 | | | | | 5 | | | | | Extremo | | | | |
| | | | | | | | | | | | | | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | | | | | | | | | | | | | |
| 4 | | | | | 3 | | | | | Alto | | | | | No | Sin control | | | | Moderado | Directamente | No disminuye | 3 | | | | | 3 | | | | | Alto | | | | |
| | | | | | | | | | | | | | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | | | | | | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 99 de 117 |

- Proceso de Control y Auditorías

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 100 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|----------------------|---|---|---|----------------------|------------------------------|---|--|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 5 | Control y Auditorías | | PÉRDIDA DE DISPONIBILIDAD | seguridad digital | Otros | Nivel Directivo | Uso incorrecto de software y hardware | Hallazgos de los entes de control |
| | | | | | | | Mantenimiento insuficiente de equipos de cómputo | Deterioro de imagen institucional |
| | | | | | | | Ausencia de personal | Incumplimiento de funciones y obligaciones |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 102 de 117 |

- Proceso de Gestión a la Dirección del SGSSS

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 103 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|----------------------------------|---|--|---|----------------------|------------------------------|---|---|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 3 | Gestión a la Dirección del SGSSS | | PERDIDA DE INTEGRIDAD | seguridad digital | Otros | Nivel Directivo | Falta de planificación y desconocimiento normativo | Posibles hallazgos de entes de control por inversión errónea y/o detrimento patrimonial |
| | | | | | | | Falencia en estudios y diseños | Posibles hallazgos de entes de control por inversión errónea y/o detrimento patrimonial |
| | | | | | | | Favorecimiento a terceros en la ejecución de los proyectos | Posibles hallazgos de entes de control por inversión errónea y/o detrimento patrimonial |
| | | | | | | | Desconocimiento normativo | Viabilidades de servicios en salud erróneas |
| | | | | | | | Inestabilidad normativa | Viabilidades de servicios en salud erróneas |
| | | | | | | | Subjetividad en la evaluación | Viabilidades de servicios en salud erróneas |
| | | | | | | | Ausencia de seguimiento permanente | Hallazgos de entes de control |
| | | | | | | | Ausencia del personal | Incumplimiento de funciones y obligaciones |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 104 de 117 |

| | | | | | | | | |
|---|----------------------------------|--|--------------------------------|-------------------|-------|-----------------|--|---|
| 4 | Gestión a la Dirección del SGSSS | | PERDIDA DE DISPONIBILIDAD | seguridad digital | Otros | Nivel Directivo | Falta de planificación y desconocimiento normativo | Posibles hallazgos de entes de control por inversión errónea y/o detrimento patrimonial |
| | | | | | | | Falencia en estudios y diseños | Posibles hallazgos de entes de control por inversión errónea y/o detrimento patrimonial |
| | | | | | | | Favorecimiento a terceros en la ejecución de los proyectos | Posibles hallazgos de entes de control por inversión errónea y/o detrimento patrimonial |
| | | | | | | | Desconocimiento normativo | Viabilidades de servicios en salud erróneas |
| | | | | | | | Inestabilidad normativa | Viabilidades de servicios en salud erróneas |
| | | | | | | | Subjetividad en la evaluación | Viabilidades de servicios en salud erróneas |
| | | | | | | | Ausencia de seguimiento permanente | Hallazgos de entes de control |
| | | | | | | | Ausencia del personal | Incumplimiento de funciones y obligaciones |
| | | | | | | | Mantenimiento insuficiente | Retrasos en la emisión de viabilidades y conceptos técnicos |
| 5 | Gestión a la Dirección del SGSSS | | PERDIDA DE CONFIDENCIALIDAD | seguridad digital | Otros | Nivel Directivo | Falta de políticas de seguridad de la información | Expedición de viabilidades y conceptos por personal no autorizado |
| | | | | | | | Ausencia de seguimiento permanente | Hallazgos de entes de control |
| | | | | | | | Ausencia del personal | Incumplimiento de funciones y obligaciones |
| | | | | | | | Falta de compromiso | Incumplimiento de funciones y obligaciones |
| | | | | | | | Falta de actualización | Baja capacidad de |



CODIGO: SGN-C043-PL02

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

| |
|---|
| <p>Fecha Aprobación: 31 de Enero de 2020</p> |
|---|

Versión: 1

Página 105 de 117

| FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------------|----------|----------|---------------------------|----------------|-------|----------------------------|---------|--------------|---|----------|----------|--------|---|-------------------------------------|--|---|--|--|--|---|----------|---------------------------|----------|---|--|----------------|-------|----------|-------|--------------|---------|------|----------|------|---|---|
| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | | | |
| PROBABILIDAD (ver hoja 2.1) | | | | IMPACTO (ver hoja 2.1) | | | NIVEL DEL RIESGO INHERENTE | | | | | | | | | | | | | PROBABILIDAD (ver hoja 2.1) | | | IMPACTO (ver hoja 2.1) | | | NIVEL DEL RIESGO RESIDUAL | | | | | | | | | | | |
| Rara vez | Improbable | Possible | Probable | Casi seguro | Insignificante | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control | Calificación de la ejecución del control | Solidez individual del control: Fuerte = 100 Moderado=50 Débil=0 | Peso en la evaluación del diseño del control SI=100 NO=0 | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: Directamente o No disminuye ? | Controles ayudan a disminuir el impacto ? Directamente o Indirectamente o No disminuye ? | Rara vez | Improbable | Possible | Probable | Casi seguro | Insignificante | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | | |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | 1 | 2 | | | | | | 3 | 4 | 5 | Fuerte (96-100) Moderado (86-95) Débil (0-85) | Fuerte: Siempre se ejecuta Moderado: Algunas veces se ejecuta Débil: No se ejecuta | 1 | 2 | 3 | 4 | 5 | | | | | 1 | 2 |
| 4 | | | | 4 | | | | Extremo | | | | Si | Fuerte | Fuerte | Fuerte | No | Moderado | Directamente | Indirectamente | 3 | 3 | Moderado | | | | | | | | | | | | | | | |
| | | | | | | | | Si | Fuerte | Fuerte | Fuerte | No | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | Si | Fuerte | Fuerte | Fuerte | No | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | |
|---|---|--|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043- PL02</p> |
| | <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | <p>Fecha Aprobación: 31 de Enero de 2020</p> <p>Versión: 1</p> <p>Página 106 de 117</p> |



CODIGO: SGN-C043-PL02

| |
|--|
| Fecha Aprobación: 31 de Enero de 2020 |
|--|

Versión: 1

Página 106 de 117

| | | | | | | | | | | | | | |
|---|------------------------|---------|----|-------------|--------|----------|----|----------|--------------|----------------|---|---|----------|
| 4 | <div><div></div></div> | Extremo | Si | Fuerte | Fuerte | Fuerte | No | Moderado | Directamente | Indirectamente | 3 | 3 | Moderado |
| | | | Si | Fuerte | Fuerte | Fuerte | No | | | | | | |
| | | | Si | Fuerte | Fuerte | Fuerte | No | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| 4 | <div><div></div></div> | Extremo | No | Sin control | | | | Débil | No disminuye | No disminuye | 4 | 4 | Extremo |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 107 de 117 |

- Proceso de Prestación de Servicios de Salud

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 108 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|----------------------------------|---|---|---|----------------------|------------------------------|---|--|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 4 | Prestación de Servicios de Salud | | Pérdida de confidencialidad de acceso a sistemas de información y bases de datos | seguridad digital | Otros | Nivel Directivo | Capacidad insuficiente del software para soportar gran cantidad de usuarios cargando simultáneamente información Error en la configuración del software para carga de información en flujos de trabajo específicos | Retrasos en los procesos de validación de requisitos para habilitación de servicios en salud Retrasos en los procesos de validación de requisitos para habilitación de servicios en salud |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 109 de 117 |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 110 de 117 |

| | | | | | | | | |
|---|----------------------------------|--|---|-------------------|-------|-----------------|---|--|
| 5 | Prestación de Servicios de Salud | | Pérdida de integridad de información y bases de datos | seguridad digital | Otros | Nivel Directivo | Capacidad insuficiente del software para soportar gran cantidad de usuarios cargando simultáneamente información | Retrasos en los procesos de validación de requisitos para habilitación de servicios en salud |
| | | | | | | | Error en la configuración del software para carga de información en flujos de trabajo específicos | Retrasos en los procesos de validación de requisitos para habilitación de servicios en salud |
| | | | | | | | Fallas en servidor de app extranet | Canal de comunicación oficial con los prestadores de servicios de salud inhabilitado |
| | | | | | | | Falta de backup de la información | Inhabilidad de atención a eventos de contingencia que afecten los servicios |
| | | | | | | | Falta de políticas de seguridad de la información | Inhabilidad de atención a eventos de contingencia que afecten los servicios |
| | | | | | | | Infraestructura física no adecuada para archivo de documentos | Pérdida de documentación relacionada con las actividades del proceso |
| | | | | | | | Verificación deficiente para el aval de las actas e informes de visita por parte del funcionario líder de la visita | Validación errónea de requisitos y habilitación indebida de servicios de salud |
| | | | | | | | No disponibilidad de registro de auditoría y bitácora de usuarios integrados al software | Inhabilidad de registro de habilitación de servicios en REPS |
| | | | | | | | Ausencia de verificación y evaluación de competencias blandas en la fase precontractual del personal | Personal no idóneo y clima laboral afectado |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 111 de 117 |

| | | | | | | | | |
|---|----------------------------------|--|--|-------------------|-------|-----------------|---|--|
| 6 | Prestación de Servicios de Salud | | Pérdida de disponibilidad de información, sistemas de información y bases de datos | seguridad digital | Otros | Nivel Directivo | Capacidad insuficiente del software para soportar gran cantidad de usuarios cargando simultáneamente información | Retrasos en los procesos de validación de requisitos para habilitación de servicios en salud |
| | | | | | | | Error en la configuración del software para carga de información en flujos de trabajo específicos | Retrasos en los procesos de validación de requisitos para habilitación de servicios en salud |
| | | | | | | | Fallas en servidor de app extranet | Canal de comunicación oficial con los prestadores de servicios de salud inhabilitado |
| | | | | | | | Falta de backup de la información | Inhabilidad de atención a eventos de contingencia que afecten los servicios |
| | | | | | | | Falta de políticas de seguridad de la información | Inhabilidad de atención a eventos de contingencia que afecten los servicios |
| | | | | | | | Infraestructura física no adecuada para archivo de documentos | Pérdida de documentación relacionada con las actividades del proceso |
| | | | | | | | Verificación deficiente para el aval de las actas e informes de visita por parte del funcionario líder de la visita | Validación errónea de requisitos y habilitación indebida de servicios de salud |
| | | | | | | | No disponibilidad de registro de auditoría y bitácora de usuarios integrados al software | Inhabilidad de registro de habilitación de servicios en REPS |
| | | | | | | | Ausencia de verificación y evaluación de competencias blandas en la fase precontractual del personal | Personal no idóneo y clima laboral afectado |



CODIGO: SGN-C043-PL02

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

| | |
|--------------------------|--|
| Fecha Aprobación: | |
|--------------------------|--|

31 de Enero de 2020

Versión: 1

Página 112 de 117

| FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|---|---|---|---|---------------------------|---|---|---|---|---|--|--|--|--|---|---|--|---|---|---|--|---|------------------------|----------|------------------------------|---|---|----------------|----------|----------|---|---------|----------|----------|--|--|--|--|
| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO INHERENTE | | | | | PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO RESIDUAL | | | | | | | | | | | | | |
| Rara vez Improbable | | | | | Insignificante | | | | | Extremo | | | | | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control | Calificación de la ejecución del control | Solidez individual del control: Fuerte = 100 Moderado=50 Débil=0 | Peso en la evaluación del diseño del control SI=100 NO=0 | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: Directamente o No disminuye ? | Controles ayudan a disminuir el impacto ? Directamente o Indirectamente o No disminuye ? | Rara vez Improbable | | | | | Insignificante | | | | Extremo | | | | | | |
| Posible | | | | | Menor | | | | | Alto | | | | | (Fuerte (96-100) Moderado (86-95) Débil (0-85) | | Fuerte: Siempre se ejecuta Moderado: Algunas veces se ejecuta Débil: No se ejecuta | | | | | | 2 | | | | | Menor | | | | Alto | | | | | | |
| Probable | | | | | Moderado | | | | | Moderado | | | | | | | | | | | | | | 3 | | | | | | Moderado | | | Moderado | | | | | |
| Casi seguro | | | | | Mayor | | | | | Bajo | | | | | | | | | | | | | | 4 | | | | | | Mayor | | | Mayor | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | | | | | | | | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | | | | | 4 | | | | | Alto | | | | | No | Sin control | | | | | #¡VALOR! | No disminuye | No disminuye | #¡VALOR! | | | | | #¡VALOR! | | | | | #¡VALOR! | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 115 de 117 |

- Proceso de Aseguramiento del SGSSS

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 116 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|------------------------------------|---|--|---|----------------------|------------------------------|---|--|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 6 | GESTIÓN DEL ASEGURAMIENTO AL SGSSS | | PÉRDIDA DE INTEGRIDAD DE INFORMACIÓN, APLICATIVOS Y SISTEMAS DE INFORMACIÓN DEL PROCESO | seguridad digital | Otros | Nivel Directivo | Ineficacia en el control de cambios de sistemas de información provistos por Ministerio de Salud, proveedores y/o proveedores Respuesta inadecuada de mantenimiento del servicio Fallas en servidor de SISHuila Falta de políticas de seguridad de la información Errores en ingreso de información Destrucción de información Software Nuevo o inmaduro Mantenimiento insuficiente de equipos de cómputo Ausencia del personal | Evaluación inadecuada a las EAPB (Entidades Administradoras de Planes de Beneficios) e Información falsa a la comunidad sobre el desempeño de las EAPB Retrasos en el suministro de información a la comunidad sobre las EAPB Evaluación inadecuada a las EAPB (Entidades Administradoras de Planes de Beneficios) e Información falsa a la comunidad sobre el desempeño de las EAPB Deterioro en la imagen institucional Investigaciones por parte de los entes de control Investigaciones por parte de los entes de control Deterioro en la imagen institucional Retrasos en el suministro de información a la comunidad sobre las EAPB Asesoría y Asistencia Técnica con errores de acuerdo a la normatividad |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 117 de 117 |

| | | | | | | | | |
|---|------------------------------------|--|---|-------------------|-------|-----------------|---|--|
| 7 | GESTIÓN DEL ASEGURAMIENTO AL SGSSS | | PÉRDIDA DE DISPONIBILIDAD DE INFORMACIÓN, APLICATIVOS Y SISTEMAS DE INFORMACIÓN DEL PROCESO | seguridad digital | Otros | Nivel Directivo | Ineficacia en el control de cambios de sistemas de información provistos por Ministerio de Salud, proveedores y/o proveedores | Evaluación inadecuada a las EAPB (Entidades Administradoras de Planes de Beneficios) e Información falsa a la comunidad sobre el desempeño de las EAPB |
| | | | | | | | Respuesta inadecuada de mantenimiento del servicio | Retrasos en el suministro de información a la comunidad sobre las EAPB |
| | | | | | | | Fallas en servidor de SISHuila | Evaluación inadecuada a las EAPB (Entidades Administradoras de Planes de Beneficios) e Información falsa a la comunidad sobre el desempeño de las EAPB |
| | | | | | | | Falta de políticas de seguridad de la información | Deterioro en la imagen institucional |
| | | | | | | | Errores en ingreso de información | Investigaciones por parte de los entes de control |
| | | | | | | | Destrucción de información | Investigaciones por parte de los entes de control |
| | | | | | | | Software Nuevo o inmaduro | Deterioro en la imagen institucional |
| | | | | | | | Mantenimiento insuficiente de equipos de cómputo | Retrasos en el suministro de información a la comunidad sobre las EAPB |
| | | | | | | | Descarga y uso no controlado de información | Investigaciones por parte de los entes de control |
| | | | | | | | Ausencia del personal | Asesoría y Asistencia Técnica con errores de acuerdo a la normalidad |



SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG

CODIGO: SGN-C043-PL02

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

| |
|---|
| <p>Fecha Aprobación: 31 de Enero de 2020</p> |
|---|

Versión: 1

Página 118 de 117

| FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------------|---------|----------|-------------|--------------|-------|----------|-------|--------------|---|------|----------|------|---|--|--|---|--|--|--|---|---|------------|---------------------------|----------|----------------------------|--------------|--------------------------------|----------|---------------------------|--------------|---------------------------|------|----------|------|---|---|---|
| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | PROBABILIDAD (ver hoja 2.1) | | IMPACTO (ver hoja 2.1) | | NIVEL DEL RIESGO INHERENTE | | PROBABILIDAD (ver hoja 2.1) | | IMPACTO (ver hoja 2.1) | | NIVEL DEL RIESGO RESIDUAL | | | | | | |
| Rara vez | Improbable | Posible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control Fuerte (96-100) Moderado (86-95) Débil (0-85) | Calificación de la ejecución del control Fuerte: Siempre se ejecuta Moderado: Algunas veces se ejecuta Débil: No se ejecuta | Solidez individual del control: Fuerte = 100 Moderado=50 Débil=0 | Peso en la evaluación del diseño del control SI=100 NO=0 | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: Directamente o No disminuye ? | Controles ayudan a disminuir el impacto ? Directamente o Indirectamente o No disminuye ? | Rara vez | Improbable | Posible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | | | |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | | | | | | | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | 1 | 2 | 3 |
| 4 | | | | | 4 | | | | | Extremo | | | | No | Sin control | | | | | Débil | No disminuye | Indirectamente | 4 | | | | | 3 | | | | | Alto | | | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | Si | Débil | Moderado | Débil | Si | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | Si | Débil | Moderado | Débil | Si | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | Si | Débil | Moderado | Débil | Si | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | Si | Fuerte | Moderado | Moderado | Si | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | Si | Fuerte | Fuerte | Fuerte | No | | | | | | | | | | | | | | | | | | | | |

| | | |
|---|---|--|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043- PL02</p> |
| | <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | <p>Fecha Aprobación: 31 de Enero de 2020</p> <p>Versión: 1</p> <p>Página 119 de 117</p> |



Página 119 de 117

| | | | | | | | | | | | | | |
|---|---|---------|----|-------------|----------|----------|----|-------|--------------|----------------|---|---|------|
| 4 | 4 | Extremo | No | Sin control | | | | Débil | No disminuye | Indirectamente | 4 | 3 | Alto |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Moderado | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Moderado | Débil | Si | | | | | | |
| | | | Si | Débil | Moderado | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Fuerte | Moderado | Moderado | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Fuerte | Fuerte | Fuerte | No | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 120 de 117 |

- Proceso de Salud Pública

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 121 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|--------------------|---|---|---|-------------------------|------------------------------------|--|--|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 4 | SALUD PÚBLICA | | Pérdida de confidencialidad | seguridad digital | Otros | Nivel Directivo | Falta de adquisición y actualización de licencias de gestores de bases de datos Falta de backup de la información y de actualización de antivirus Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) Falta de procedimientos para acceso y préstamo de documentos Falta de repositorios adecuados para archivar Falta de mantenimiento y calibración de equipos de laboratorio Instalaciones físicas deficientes Instalaciones eléctricas insuficientes | Duplicidad de información y bases de datos de muestras biológicas o ambientales Posibles pérdidas de resultados de análisis de muestras Posibles pérdidas de bases de datos de muestras y de resultados de análisis de muestras Acceso no autorizado a documentos del proceso (protocolos de validación) Daños o pérdida de documentos del proceso (protocolos, manuales, correspondencia, etc.) Resultados de análisis imprecisos o erróneos Malas condiciones de almacenamiento y análisis de muestras y resultados Malas condiciones de almacenamiento y análisis de muestras y resultados |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 122 de 117 |

| | | | | | | | | |
|---|---------------|--|-----------------------|-------------------|-------|-----------------|--|---|
| 5 | SALUD PÚBLICA | | Pérdida de integridad | seguridad digital | Otros | Nivel Directivo | Falta de adquisición y actualización de licencias de gestores de bases de datos | Duplicidad de información y bases de datos de muestras biológicas o ambientales |
| | | | | | | | Falta de backup de la información y de actualización de antivirus | Posibles pérdidas de resultados de análisis de muestras |
| | | | | | | | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | Posibles pérdidas de bases de datos de muestras y de resultados de análisis de muestras |
| | | | | | | | Errores en ingreso de información | Reportes erróneos de análisis de muestras en diferentes sistemas de información |
| | | | | | | | Destrucción de información | Pérdida de análisis de muestras en sistemas de información |
| | | | | | | | Software Nuevo o inmaduro | Inhabilidad de los servicios de los sistemas de información |
| | | | | | | | Fallas en servidor de SISHuila | Interrupción de servicios de sistemas de información y acceso a bases de datos |
| | | | | | | | Falta de políticas de seguridad de la información | Posibles pérdidas de resultados de análisis de muestras |
| | | | | | | | Falta de procedimientos para acceso y préstamo | Acceso no autorizado a documentos del proceso (protocolos de validación) |
| | | | | | | | Falta de repositorios adecuados para archivar | Daños o pérdida de documentos del proceso (protocolos, manuales, correspondencia, etc.) |
| | | | | | | | Fallas en servidor de app extranet | No recepción ni generación de comunicaciones oficiales |
| | | | | | | | Falta de backup de la información | Posibles pérdidas de resultados de análisis de muestras |
| | | | | | | | Instalaciones físicas deficientes | Malas condiciones de almacenamiento y análisis de muestras y resultados |
| | | | | | | | Instalaciones eléctricas insuficientes | Malas condiciones de almacenamiento y análisis de muestras y resultados |
| | | | | | | | Mantenimiento insuficiente o deficiente de equipos de cómputo | Posibles pérdidas de bases de datos de muestras y de resultados de análisis de muestras |
| | | | | | | | Falta de mantenimiento y calibración de equipos de laboratorio | Resultados de análisis imprecisos o erróneos |
| | | | | | | | No disponibilidad de registro de auditoría y bitácora de usuarios integrados al software | Acceso no autorizado a bases de datos de muestras y resultados de análisis realizados |
| | | | | | | | Ausencia de verificación y evaluación de competencias blandas en la fase precontractual del personal | Personal no idóneo y afectación del clima laboral en el área |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 123 de 117 |

| | | | | | | | | |
|---|---------------|--|---------------------------|-------------------|-------|-----------------|--|---|
| 6 | SALUD PÚBLICA | | Pérdida de disponibilidad | seguridad digital | Otros | Nivel Directivo | Falta de adquisición y actualización de licencias de gestores de bases de datos | Duplicidad de información y bases de datos de muestras biológicas o ambientales |
| | | | | | | | Falta de backup de la información y de actualización de antivirus | Posibles pérdidas de resultados de análisis de muestras |
| | | | | | | | Falta de dotación y renovación de equipos tecnológicos (equipos de cómputo e impresoras) | Posibles pérdidas de bases de datos de muestras y de resultados de análisis de muestras |
| | | | | | | | Errores en ingreso de información | Reportes erróneos de análisis de muestras en diferentes sistemas de información |
| | | | | | | | Dstrucción de información | Pérdida de análisis de muestras en sistemas de información |
| | | | | | | | Software Nuevo o inmaduro | Inhabilidad de los servicios de los sistemas de información |
| | | | | | | | Fallas en servidor de SISHuila | Interrupción de servicios de sistemas de información y acceso a bases de datos |
| | | | | | | | Falta de políticas de seguridad de la información | Posibles pérdidas de resultados de análisis de muestras |
| | | | | | | | Falta de procedimientos para acceso y préstamo | Acceso no autorizado a documentos del proceso (protocolos de validación) |
| | | | | | | | Falta de repositorios adecuados para archivar | Daños o pérdida de documentos del proceso (protocolos, manuales, correspondencia, etc.) |
| | | | | | | | Fallas en servidor de app extranet | No recepción ni generación de comunicaciones oficiales |
| | | | | | | | Falta de backup de la información | Posibles pérdidas de resultados de análisis de muestras |
| | | | | | | | Instalaciones físicas deficientes | Malas condiciones de almacenamiento y análisis de muestras y resultados |
| | | | | | | | Instalaciones eléctricas insuficientes | Malas condiciones de almacenamiento y análisis de muestras y resultados |
| | | | | | | | Mantenimiento insuficiente o deficiente de equipos de cómputo | Posibles pérdidas de bases de datos de muestras y de resultados de análisis de muestras |
| | | | | | | | Falta de mantenimiento y calibración de equipos de laboratorio | Resultados de análisis imprecisos o erróneos |
| | | | | | | | No disponibilidad de registro de auditoría y bitácora de usuarios integrados al software | Acceso no autorizado a bases de datos de muestras y resultados de análisis realizados |
| | | | | | | | Ausencia de verificación y evaluación de competencias blandas en la fase precontractual del personal | Personal no idóneo y afectación del clima laboral en el área |



SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG

CODIGO: SGN-C043-PL02

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

| |
|---|
| <p>Fecha Aprobación: 31 de Enero de 2020</p> |
|---|

Versión: 1

Página 124 de 117

| FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------------|----------|----------|-------------|----------------|-------|----------|-------|--------------|---|------|----------|------|---|---|--|--|--|--|--|---|--------------|----------------|----------|---------------------------|-------------|----------------|-------|----------|-------------------------------|--------------|---------|------|----------|--------------------------------|--|--|--|
| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO INHERENTE | | | | | PROBABILIDAD (ver hoja 2.1) | | | |
| Rara vez | Improbable | Possible | Probable | Casi seguro | Insignificante | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control | Calificación de la ejecución del control | Solidez individual del control: | Peso en la evaluación del diseño del control SI=100 NO=0 | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: Directamente o No disminuye ? | Controles ayudan a disminuir el impacto ? Directamente o Indirectamente o No disminuye ? | Rara vez | Improbable | Possible | Probable | Casi seguro | Insignificante | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | | | |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | Fuerte (96-100) Moderado (86-95) Débil (0-85) | Fuerte: Siempre se ejecuta Moderado: Algunas veces se ejecuta Débil: No se ejecuta | Fuerte = 100 Moderado=50 Débil=0 | | | | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | | |
| 4 | | | | | 4 | | | | | Extremo | | | | | No | Sin control | | | | | Débil | No disminuye | Indirectamente | 4 | | | | | 3 | | | | | Alto | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 125 de 117 |



CODIGO: SGN-C043-PL02

| |
|--|
| Fecha Aprobación: 31 de Enero de 2020 |
|--|

Versión: 1

Página 126 de 117

| | | | | | | | | | | | | | |
|---|--------------------------|---------|----|-------------|--------|--------|----|-------|--------------|----------------|---|---|---------|
| 4 | <div><div></div></div> 4 | Extremo | No | Sin control | | | | Débil | No disminuye | Indirectamente | 4 | 4 | Extremo |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | Si | Fuerte | Fuerte | Fuerte | No | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | | | | | | | | | | | |



CODIGO: SGN-C043-PL02

| |
|--|
| Fecha Aprobación: 31 de Enero de 2020 |
|--|

Versión: 1

Página 127 de117

| | | | | | | | | | | | | | |
|---|--------------------------|---------|----|-------------|--------|--------|----|-------|--------------|----------------|---|---|---------|
| 4 | <div><div></div></div> 4 | Extremo | No | Sin control | | | | Débil | No disminuye | Indirectamente | 4 | 4 | Extremo |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | Si | Fuerte | Fuerte | Fuerte | No | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | | | | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 128 de 117 |

- Proceso de Gestión del Recurso Físico

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 129 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|--------------------|---|---|---|----------------------|------------------------------|---|--|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 4 | RECURSOS FISICOS | | Pérdida de disponibilidad de información y sistemas de información | seguridad digital | Otros | Directivo y profesional | Falta de backup de la información relacionada | Inhabilidad ante contingencias y eventos de seguridad |
| | | | | | | | Error en el diligenciamiento de la información | Registro de activos erróneos |
| | | | | | | | Falta de políticas de seguridad de la información | Inhabilidad ante contingencias y eventos de seguridad |
| | | | | | | | Fallas en servidor de app SIFA | Retrasos en la actualización del inventario general y registros de activos |
| | | | | | | | Ausencia de auditorías regulares | Hallazgos de entes de control |
| | | | | | | | Ausencia del personal | Retrasos en la actualización del inventario general y registros de activos |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 130 de 117 |

| | | | | | | | | |
|---|------------------|--|---|-------------------|-------|-------------------------|---|--|
| 5 | RECURSOS FISICOS | | Pérdida de integridad de la información y sistemas de información | seguridad digital | Otros | Directivo y profesional | Falta de backup de la información relacionada | Inhabilidad ante contingencias y eventos de seguridad |
| | | | | | | | Error en el diligenciamiento de la información | Registro de activos erróneos |
| | | | | | | | Falta de políticas de seguridad de la información | Inhabilidad ante contingencias y eventos de seguridad |
| | | | | | | | Fallas en servidor de app SIFA | Retrasos en la actualización del inventario general y registros de activos |
| | | | | | | | Ausencia de auditorías regulares | Hallazgos de entes de control |
| | | | | | | | Ausencia del personal | Retrasos en la actualización del inventario general y registros de activos |



SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG

CODIGO: SGN-C043-PL02

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

| |
|--|
| Fecha Aprobación: 31 de Enero de 2020 |
|--|

Versión: 1

Página 131 de 117

| FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------------|---------|----------|-------------|--------------|-------|----------|-------|--------------|---|------|----------|------|---|---|--|--|--|--|--|---|----------|------------|---------|---------------------------|-------------|--------------|-------|----------|-------------------------------|--------------|---------|--------------------------------|----------|------|
| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO INHERENTE | | | PROBABILIDAD (ver hoja 2.1) | | |
| Rara vez | Improbable | Posible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control | Calificación de la ejecución del control | Solidez individual del control: | Peso en la evaluación del diseño del control SI=100 NO=0 | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: Directamente o No disminuye ? | Controles ayudan a disminuir el impacto ? Directamente o Indirectamente o No disminuye ? | Rara vez | Improbable | Posible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | Fuerte (96-100) Moderado (86-95) Débil (0-85) | Fuerte: Siempre se ejecuta Moderado: Algunas veces se ejecuta Débil: No se ejecuta | Fuerte = 100 Moderado=50 Débil=0 | | | | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | |
| 4 | | | | | 3 | | | | | Alto | | | | Si | Débil | Moderado | Débil | Si | Débil | No disminuye | No disminuye | 4 | | | | | 3 | | | | | Alto | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | |
| 4 | | | | | 3 | | | | | Alto | | | | Si | Débil | Fuerte | Débil | Si | Débil | No disminuye | No disminuye | 4 | | | | | 3 | | | | | Alto | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 132 de 117 |

- Proceso de Mejora Continua

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 133 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|--------------------|---|---|---|----------------------|------------------------------|---|---|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 4 | MEJORA CONTINUA | Herramienta tecnológica-extranet para divulgar información | Pérdida de disponibilidad de información del SIG en el aplicativo extranet | seguridad digital | Otros | Directivo y profesional | Falta de backup de la información relacionada | Hallazgos de entes de control |
| | | | | | | | Ausencia del personal | Bajas calificaciones de transparencia y desempeño institucional |
| | | | | | | | Fallas en servidor de aplicativo extranet | Reprocesos de publicación de información |
| | | | | | | | Fallas en el servicio de conectividad a internet | Herramientas tecnológicas de divulgación de información del SIG, sin acceso para usuarios internos y externos |
| | | | | | | | Mantenimiento insuficiente de equipos de computo | No disponibilidad de equipos para acceso a información relacionada |
| 5 | MEJORA CONTINUA | Formación, capacitación, competencia y retroalimentación del equipo de trabajo de mejora continua | Pérdida de integridad de la información del sistema de Gestión | seguridad digital | Otros | Directivo y profesional | Falta de políticas de seguridad de la información | Reprocesos de publicación de información |
| | | | | | | | Falta de backup de la información relacionada | Hallazgos de entes de control |
| | | | | | | | Fallas en servidor de aplicativo extranet | Bajas calificaciones de transparencia y desempeño institucional |



SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG

CODIGO: SGN-C043-PL02

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

| | |
|-------------------|---------------------|
| Fecha Aprobación: | 31 de Enero de 2020 |
|-------------------|---------------------|

Versión: 1

Página 134 de 117

| FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------------|---------|----------|-------------|--------------|-------|----------|-------|--------------|---|------|----------|------|---|-------------------------------------|--|---|--|--|--|---|---|------------|---------------------------|----------|-------------------------------|--------------|--------------------------------|----------|---------------------------|--------------|------------------------------|---------|----------|------|---|----|
| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | PROBABILIDAD (ver hoja 2.1) | | IMPACTO (ver hoja 2.1) | | NIVEL DEL RIESGO INHERENTE | | PROBABILIDAD (ver hoja 2.1) | | IMPACTO (ver hoja 2.1) | | NIVEL DEL RIESGO RESIDUAL | | | | | |
| Rara vez | Improbable | Posible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control | Calificación de la ejecución del control | Solidez individual del control: Fuerte = 100 Moderado=50 Débil=0 | Peso en la evaluación del diseño del control SI=100 NO=0 | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: Directamente o No disminuye ? | Controles ayudan a disminuir el impacto ? Directamente o Indirectamente o No disminuye ? | Rara vez | Improbable | Posible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | | |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | 1 | 2 | | | | | | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | | | | | 3 | 4 |
| 4 | | | | | 3 | | | | | Alto | | | | | Si | Débil | Moderado | Débil | Si | Débil | No disminuye | Indirectamente | 5 | | | | | 4 | | | | | Extremo | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | |
| 4 | | | | | 3 | | | | | Alto | | | | | No | Sin control | | | Débil | No disminuye | Directamente | 5 | | | | | 4 | | | | | Extremo | | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Moderado | Débil | | | | | | | | | | | | | | | | | | | Si |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | | | | | | | | | | | | | | | | | | | Si |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 135 de 117 |

- Proceso de Calidad del Servicio Educativo en Educación Preescolar, Básica y Media

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 136 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|--------------------------------|---|---|---|----------------------|------------------------------|--|--|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 5 | CALIDAD DEL SERVICIO EDUCATIVO | | PERDIDA DE INTEGRIDAD | seguridad digital | Otros | Nivel Directivo | Cambio del administrador del portal web Tercerización del servicio de administración de centro de datos Descuido de usuarios en manejo de datos de acceso Criterios sujetos a cambios periódicos para la estructuración de la información y bases de datos Ausencia de autenticación de usuarios Uso no previsto Desconocimiento de la información sobre experiencias Uso incorrecto del software (registro adicional de participantes) | Acceso no autorizado al portal web Fallas y/o inhabilitación del portal web Acceso no autorizado al portal web Información imprecisa publicada en el portal web Acceso no autorizado al portal web Fallas y/o inhabilitación del portal web Información imprecisa publicada en el portal web Información imprecisa publicada en el portal web |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 137 de 117 |

| | | | | | | | | |
|---|-----------------------------------|--|------------------------------|-------------------|-------|-----------------|--|---|
| 6 | CALIDAD DEL SERVICIO EDUCATIVO | | PERDIDA DE DISPONIBILIDAD | seguridad digital | Otros | Nivel Directivo | Cambio del administrador del portal web | Acceso no autorizado al portal web |
| | | | | | | | Tercerización del servicio de administración de centro de datos | Fallas y/o inhabilitación del portal web |
| | | | | | | | Descuido de usuarios en manejo de datos de acceso | Acceso no autorizado al portal web |
| | | | | | | | Criterios sujetos a cambios periódicos para la estructuración de la información y bases de datos | Información imprecisa publicada en el portal web |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 138 de 117 |

| FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------------|----------|----------|-------------|--------------|-------|----------|-------|--------------|---|------|----------|------|---|--|--|---|--|--|--|---|--------------|------------|----------|---------------------------|-------------|--------------|-------|----------|----------------------------|--------------|---------|------|----------|--------------------------------|---|---|
| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO INHERENTE | | | | | PROBABILIDAD (ver hoja 2.1) | | |
| Rara vez | Improbable | Possible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control Fuerte (96-100) Moderado (86-95) Débil (0-85) | Calificación de la ejecución del control Fuerte: Siempre se ejecuta Moderado: Algunas veces se ejecuta Débil: No se ejecuta | Solidez individual del control: Fuerte = 100 Moderado=50 Débil=0 | Peso en la evaluación del diseño del control SI=100 NO=0 | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: Directamente o No disminuye ? | Controles ayudan a disminuir el impacto ? Directamente o Indirectamente o No disminuye ? | Rara vez | Improbable | Possible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | | |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | | | | | | | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | 1 | 2 |
| 4 | | | | | 4 | | | | | Extremo | | | | | Si | Fuerte | Fuerte | Fuerte | Si | Moderado | Directamente | No disminuye | 3 | | | | | 4 | | | | | Alto | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | | | | | | | | | | | | | |
| 4 | | | | | 4 | | | | | Extremo | | | | | Si | Fuerte | Fuerte | Fuerte | Si | Moderado | Directamente | No disminuye | 3 | | | | | 4 | | | | | Alto | | | | |
| | | | | | | | | | | | | | | | Si | Débil | Fuerte | Débil | Si | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 Página 139 de 117 |

- Proceso de Cobertura del Servicio Educativo

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043-PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 140 de 117 |

| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|----------------------------------|---|---|---|----------------------|------------------------------|---|---|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 4 | COBERTURA DEL SERVICIO EDUCATIVO | | Pérdida de confidencialidad | seguridad digital | Otros | Nivel Directivo | Ineficacia de control de cambios de software | Retrasos en los reportes de matrícula escolar |
| | | | | | | | Uso indebido de permisos de acceso a la información | Información sobre matrícula escolar imprecisa o alterada |
| | | | | | | | Ausencia de procedimientos para el manejo de información clasificada | Hallazgos e investigaciones por parte de entes de control |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 141 de 117 |

| | | | | | | | | |
|---|-------------------------------------|--|-----------------------|-------------------|-------|-----------------|---|--|
| 5 | COBERTURA DEL SERVICIO EDUCATIVO | | Pérdida de integridad | seguridad digital | Otros | Nivel Directivo | Ineficacia de control de cambios de software | Retrasos en los reportes de matrícula escolar |
| | | | | | | | Uso indebido de permisos de acceso a la información | Información sobre matrícula escolar imprecisa o alterada |
| | | | | | | | Ausencia de procedimientos para el manejo de información clasificada | Hallazgos e investigaciones por parte de entes de control |
| | | | | | | | Uso incorrecto de software | Información sobre matrícula escolar imprecisa o alterada |
| | | | | | | | Errores en ingreso de información relacionada en actos administrativos, apropiación cultural, necesidades y solicitudes de acceso, entre otros. | Asignación presupuestal diferente a la indicada según matrícula escolar registrada, y/o necesidades establecidas |
| | | | | | | | Incumplimiento de los plazos establecidos para la implementación de las acciones de mejora continua en los procesos | Hallazgos e investigaciones por parte de entes de control |
| | | | | | | | Ausencia de documentación relacionada con actas de comité dptal de cobertura educativa | Falta de atención a solicitudes y necesidades de cobertura educativa |
| | | | | | | | Ausencia de personal | Incumplimiento en planes de acción y seguimiento |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 142 de 117 |

| | | | | | | | | |
|---|----------------------------------|--|---------------------------|-------------------|-------|-----------------|---|--|
| 6 | COBERTURA DEL SERVICIO EDUCATIVO | | Pérdida de disponibilidad | seguridad digital | Otros | Nivel Directivo | Ineficacia de control de cambios de software | Retrasos en los reportes de matrícula escolar |
| | | | | | | | Uso indebido de permisos de acceso a la información | Información sobre matrícula escolar imprecisa o alterada |
| | | | | | | | Ausencia de procedimientos para el manejo de información clasificada | Hallazgos e investigaciones por parte de entes de control |
| | | | | | | | Uso incorrecto de software | Información sobre matrícula escolar imprecisa o alterada |
| | | | | | | | Errores en ingreso de información relacionada en actos administrativos, apropiación cultural, necesidades y solicitudes de acceso, entre otros. | Asignación presupuestal diferente a la indicada según matrícula escolar registrada, y/o necesidades establecidas |
| | | | | | | | Facilidad para edición de formatos y herramientas tecnológicas | Incumplimiento en planes de acción y seguimiento |
| | | | | | | | Incumplimiento de los plazos establecidos para la implementación de las acciones de mejora continua en los procesos | Hallazgos e investigaciones por parte de entes de control |
| | | | | | | | Ausencia de documentación relacionada | Falta de atención a solicitudes y necesidades de cobertura educativa |
| | | | | | | | Ausencia de personal | Incumplimiento en planes de acción y seguimiento |

| | | |
|---|---|--|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043- PL02</p> |
| | <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | <p>Fecha Aprobación: 31 de Enero de 2020</p> <p>Versión: 1</p> <p>Página 143 de 117</p> |



CODIGO: SGN-C043-PL02

| |
|--------------------------|
| Fecha Aprobación: |
|--------------------------|

Versión: 1

Página 143 de 117

| FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------------|----------|----------|-------------|---------------------------|-------|----------|-------|--------------|---|------|----------|------|---|-------------------------------------|--|---|--|--|--|---|----------|------------|----------|---------------------------|-------------|--------------|-------|----------|-------|--------------|---------|------|----------|------|---|
| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO INHERENTE | | | | | PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO RESIDUAL | | | | | | | | | | | |
| Rara vez | Improbable | Possible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control | Calificación de la ejecución del control | Solidez individual del control: Fuerte = 100 Moderado=50 Débil=0 | Peso en la evaluación del diseño del control SI=100 NO=0 | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: Directamente o No disminuye ? | Controles ayudan a disminuir el impacto ? Directamente o Indirectamente o No disminuye ? | Rara vez | Improbable | Possible | Probable | Casi seguro | Insuficiente | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | | | | | | | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | 1 |
| 4 | | | | | 4 | | | | | Extremo | | | | | No | Sin control | | | #¡VALOR! | No disminuye | No disminuye | 4 | | | | | 4 | | | | | Extremo | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | |

| | | |
|---|---|--|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043- PL02</p> |
| | <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | <p>Fecha Aprobación: 31 de Enero de 2020</p> <p>Versión: 1</p> <p>Página 144 de 117</p> |

**GOBERNACIÓN
DEL HUILA**



SC4353-1

SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG

CODIGO: SGN-C043-PL02

Fecha Aprobación:
31 de Enero de 2020

Versión: 1

Página 144 de 117

| | | | | | | | | | | | | | |
|---|---------------------------|---------|----|-------------|----------|----------|--|-------|--------------|----------------|---|---|---------|
| 4 | <div>▼</div> <div>4</div> | Extremo | No | Sin control | | | | Débil | Directamente | Indirectamente | 4 | 4 | Extremo |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Moderado | Débil | | | | | | | |
| | | | Si | Moderado | Fuerte | Moderado | | | | | | | |
| | | | Si | Débil | Moderado | Débil | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | | | | | | | |

| | | |
|---|---|--|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043- PL02</p> |
| | <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | <p>Fecha Aprobación: 31 de Enero de 2020</p> <p>Versión: 1</p> <p>Página 145 de 117</p> |



CODIGO: SGN-C043-PL02

| |
|--|
| Fecha Aprobación: 31 de Enero de 2020 |
|--|

Versión: 1

Página 145 de 117

| | | | | | | | | | | | | | |
|---|---|---------|----|-------------|----------|----------|----|-------|--------------|----------------|---|---|---------|
| 4 | 4 | Extremo | No | Sin control | | | | Débil | Directamente | Indirectamente | 4 | 4 | Extremo |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Débil | Moderado | Débil | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | |
| | | | Si | Débil | Moderado | Débil | | | | | | | |
| | | | Si | Débil | Fuerte | Débil | Si | | | | | | |

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 146 de 117 |

- Proceso de Inspección y Vigilancia de los Establecimientos Educativos

| | | |
|---|---|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 147 de 117 |

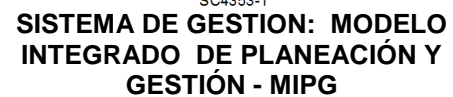
| FASE 1: IDENTIFICACIÓN DE RIESGOS | | | | | | | | |
|--|--|---|---|---|----------------------|------------------------------|--|---|
| ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos) | | | IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 / 1.4) | | | | ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1) | |
| No. De Riesgo | NOMBRE DEL PROCESO | FACTORES CLAVES DE ÉXITO EN EL PROCESO (que permita identificar riesgos asociados) | IDENTIFICACIÓN DEL RIESGO (Implica Incertidumbre y pérdida) | CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción Seguridad Digital) | TIPOLOGÍA DEL RIESGO | NIVEL DE DECISIÓN DEL RIESGO | CAUSA GENERADORA DEL RIESGO | CONSECUENCIAS DEL RIESGO |
| 7 | Gestión de la inspección y vigilancia de los establecimientos educativos | | Pérdida de integridad de información pública clasificada y servicios al ciudadano del proceso | seguridad digital | Otros | Directivo y profesional | <p>Cambios de personal directivo docente, generando falta de continuidad de lineamientos directivos y de gobierno en los establecimientos educativos.</p> <p>Cambios normativos frecuentes en todos los procesos, generando desactualización permanente</p> <p>Incumplimiento de los plazos establecidos para la implementación de las acciones de mejora continua en los procesos</p> <p>Incumplimiento de los plazos establecidos para la expedición de actos administrativos</p> <p>Cambios normativos frecuentes en todos los procesos, generando desactualización permanente para la elaboración de actos administrativos</p> <p>Errores en diligenciamiento de actos administrativos en establecimientos educativos para trámites de apostillaje</p> <p>Modificación de firmas, adulteración y expedición ilegal de documentos</p> <p>Enfermedades de origen laboral</p> | <p>Incumplimiento en la entrega de informes de gestión a la secretaría de educación y ministerio</p> <p>Retrasos en la generación de actos administrativos</p> <p>Posible apertura de proceso disciplinario por incumplimiento en la implementación de las acciones de planes de mejoramiento</p> <p>Retrasos en la habilitación de servicios de establecimientos educativos</p> <p>Retrasos en la generación de actos administrativos</p> <p>Retrasos en el servicio de apostillaje de actos administrativos</p> <p>Posible apertura de proceso disciplinario por incumplimiento en la implementación de las acciones de planes de mejoramiento</p> <p>Incumplimiento en la entrega de informes de gestión a la secretaría de educación y ministerio</p> |

| | | |
|---|--|--|
|  GOBERNACIÓN DEL HUILA |  SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG | CODIGO: SGN-C043- PL02 |
| | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | Fecha Aprobación: 31 de Enero de 2020 |
| | | Versión: 1 |
| | | Página 148 de 117 |

| | | | | | | | | |
|---|--|--|---|-------------------|-------|-----------------|--|---|
| 8 | Gestión de la inspección y vigilancia de los establecimientos educativos | | Pérdida de disponibilidad de servicios, herramientas tecnológicas e información pública clasificada del proceso | seguridad digital | Otros | Nivel Directivo | Demora en la aplicación de los cambios de los procesos, documentos y flujos de información | Incumplimiento del plan anual de visitas de inspección y vigilancia |
| | | | | | | | Cambio del administrador del portal web | Retrasos en la publicación de actos administrativos |
| | | | | | | | Errores en diligenciamiento de actos administrativos en establecimientos educativos para trámites de apostillaje | Retrasos en el servicio de apostillaje de actos administrativos |
| | | | | | | | Modificación de firmas, adulteración y expedición ilegal de documentos | Posible apertura de proceso judicial por falsificación de documento público |
| | | | | | | | Enfermedades de origen laboral | Incumplimiento en la entrega de informes de gestión a la secretaria de educación y ministerio |
| | | | | | | | Facilidad de editar la herramienta ofimática | Incompletitud de información de visitas a establecimientos educativos |
| | | | | | | | Falta de recursos para renovación y actualización de equipos de cómputo | Incumplimiento en la entrega de informes de gestión a la secretaria de educación y ministerio |

| | | |
|---|--|---|
|  <p>GOBERNACIÓN DEL HUILA</p> |  <p>SISTEMA DE GESTION: MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG</p> | <p>CODIGO: SGN-C043-PL02</p> |
| | <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL</p> | <p>Fecha Aprobación: 31 de Enero de 2020</p> |
| | | <p>Versión: 1</p> |
| | | <p>Página 149 de 117</p> |

| ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente) | | | | | | | | | | FASE 2: VALORACIÓN DE RIESGOS | | | | | | | | | | EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual) | | | | | | | | | | | | | | | | | | | |
|--|------------|---------|----------|-------------|---------------------------|-------|----------|-------|--------------|-------------------------------|------|----------|------|--|--|--|---------------------------------|--|--|---|--|--------------|----------------|---------|--------------------------------|-------------|----------------|-------|----------|---------------------------|--------------|---------|------|----------|---------------------------|--|--|--|--|
| PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO INHERENTE | | | | | VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles) | | | | | | | | | | PROBABILIDAD (ver hoja 2.1) | | | | | IMPACTO (ver hoja 2.1) | | | | | NIVEL DEL RIESGO RESIDUAL | | | | |
| Rara vez | Improbable | Pesible | Probable | Casi seguro | Insignificante | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | ¿Tiene Control? (Ver Hoja 3. Evaluación de controles) | Calificación del diseño del control | Calificación de la ejecución del control | Solidez individual del control: | Peso en la evaluación del diseño del control | CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES | Controles ayudan a disminuir la probabilidad: | Controles ayudan a disminuir el impacto ? | Rara vez | Improbable | Pesible | Probable | Casi seguro | Insignificante | Menor | Moderado | Mayor | Catastrófico | Extremo | Alto | Moderado | Bajo | | | | |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | Fuerte (96-100) Moderado (86-95) Débil (0-85) | Fuerte: Siempre se ejecuta Moderado: Algunas veces se ejecuta Débil: No se ejecuta | Fuerte = 100 Moderado=50 Débil=0 | Si=100 NO=0 | | | Directamente o No disminuye ? | Directamente o Indirectamente o No disminuye ? | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | | | |
| 5 | | | | | 4 | | | | | Extremo | | | | | No | Sin control | | | | | Moderado | Directamente | Indirectamente | 3 | | | | | 2 | | | | | Moderado | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | Si | Moderado | Fuerte | Moderado | Si | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | No | Sin control | | | | | | | | | | | | | | | | | | | | | | | |



CODIGO: SGN-C043-PL02

| |
|---|
| <p>Fecha Aprobación: 31 de Enero de 2020</p> |
|---|

Versión: 1

Página 150 de 117

| | | | | | | | | | | | | | |
|---|--------------|---------|-------|-------------|-------|----|--|-------|--------------|--------------|---|---|---------|
| 4 | <div>▼</div> | Extremo | No | Sin control | | | | Débil | No disminuye | No disminuye | 4 | 4 | Extremo |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | | No | Sin control | | | | | | | | | |
| | | Si | Débil | Fuerte | Débil | Si | | | | | | | |