# PLAN DE TRATAMIENTO DE RIESGOS DE GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA GOBERNACIÓN DEL CESAR

**TABLA DE CONTENIDO**

# INTRODUCCIÓN

La información que genera constantemente la Gobernación del Cesar es crucial para su correcto desempeño y cumplimiento de sus objetivos misionales, es por ello que la seguridad y privacidad de la información se convierten en atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo de los servicios que ofrece la entidad.

En concordancia con lo anterior, dentro del Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, un tema decisivo, es la Gestión de riesgos empleada para la toma de decisiones. Es por ello que la Gobernación del Cesar adopta la metodología “Guía de Riesgos” del Departamento Administrativo de la Función Púbica y como herramienta metodológica la norma internacional ISO 27001 la cual describe cómo gestionar la seguridad de la información en una organización.

En este orden de ideas, la Gobernación del Cesar acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos, aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo.

En el marco del Modelo de Seguridad y Privacidad de la Información el presente plan busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información en la entidad, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

De esta forma se busca mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, que las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja dentro de la entidad.

## 1. OBJETIVO

Definir el plan de tratamiento de riesgos de Seguridad y privacidad de la Información en la Gobernación del Cesar, con el propósito de aplicar los controles necesarios que buscan mitigar su materialización dentro de la entidad.

### 1.1 OBJETIVOS ESPECÍFICOS

- Mediante la utilización del Modelo de Seguridad y Privacidad para las Entidades del Estado, se busca contribuir al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a los diferentes servicios de la Gobernación del Departamento del Cesar en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información. Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.
- Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumpliendo de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del estado colombiano.
- Orientar a las entidades destinatarias en las mejores prácticas para la construcción de una política de tratamiento de datos personales respetuosa de los derechos de los titulares.
- Optimizar la labor de acceso a la información pública al interior de la Gobernación del Departamento del Cesar.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

## 2. ALCANCE

Se define el alcance del presente plan de tratamiento de riesgos, para los procesos misionales y de apoyo de la Gobernación del Cesar.

## 3. TÉRMINOS Y DEFINICIONES

**Riesgo:** Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

**Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

**Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

**Seguridad de la Información:** Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano

**Información Publica Reservada:** Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

**Información Pública Clasificada:** Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.

**No Clasificada:** Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

**Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

**Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

## CONTEXTO DE LA ENTIDAD

La Gobernación del Departamento del Cesar ha establecido las causas externas e internas que pueden afectar al propósito, los objetivos estratégicos y la planificación del Sistema de Gestión de la misma. A lo largo del sistema, la Gobernación se evalúa a sí misma y su contexto. Para ello ha definido las influencias de diversos elementos y cómo se reflejan en el Sistema de Gestión según las normas a saber, la cultura, los objetivos de la organización y las metas, la complejidad y el flujo de los procesos e información, etc. Con todo ello detectamos riesgos y oportunidades en relación con el contexto. Estos aspectos se tienen en cuenta porque pueden intervenir en la capacidad de la organización para conseguir los resultados deseados.

Por tal motivo se determina como contexto externo lo siguiente:

1) La recesión en la economía de la entidad :
   **Amenaza:** un eventual decrecimiento anual de los recursos con los que cuenta la entidad, esto tiene como resultado una disminución significativa de estos para la gobernación del departamento por parte del gobierno nacional.
   **Riesgo:** se puede presentar por la dificultad en el cumplimiento de los programas y las metas establecidas en el plan de desarrollo departamental (la falta de recursos y la no ejecución de los proyectos acordes a esos planes)

2) La estabilidad en la política:
   **Amenaza:** la culminación de un periodo político, el descontinuar los proyectos que se han establecido, ya que el gobierno entrante no contempla seguir con estos proyectos sino con la implementación de los propios.
   **Riesgo:** esta es una situación que esta fuera de control, ya que nada se puede hacer cuando hay cambios en la administración y en la política.

3) Adquisición de recursos tecnológicos: resistencia o no aceptación de los cambios
   **Amenaza:** de manera puntual, hay funcionarios que tienen una resistencia al cambio, ya sea por desconocimiento o porque no quieren cambiar los recursos con los que realizan su trabajo, estos son funcionarios que tienen mucho tiempo en la institución, en cambio hay nuevos funcionarios, entre estos contratistas, que si están prestos y exigen los cambios tecnológicos para así mejorar y agilizar el trabajo.
   **Riesgo:** este factor como tal no es un riesgo representativo.

   Sistemas de comunicación eficientes:
   **Amenaza:** la gobernación del departamento del cesar tiene sistemas de comunicación interna los cuales les ayuda en el cumplimiento de sus funciones (control doc., correo electrónico, etc.), en el caso mencionado se puede presentar una amenaza ya que la conexión puede ser interrumpida o que los recursos tecnológicos sean obsoletos, lo que puede afectar la comunicación.
   **Riesgo:** la situación del riesgo se puede presentar eventualmente por la falta de conexión o la falla tecnológica, esto podría afectar considerablemente la comunicación al interior de la entidad.

Se determina como contexto interno lo siguiente

1) Una adecuada capacidad en la dirección de la institución:
   **Amenaza:** es indispensable y completamente necesario que la gobernación del departamento del cesar mejore y fortalezca la estrategia para dirigir, para lograr esto se puede basar en la normatividad establecida correspondiente al tema a tratar y que según los procesos establecidos, se enfoque en la dirección correcta para que se ejecute de la forma más efectiva posible.
   **Riesgo:** la dirección debe estar alineada según los procesos que se manejan dentro de la entidad, para eso debe haber una política, esta sería la base para la medición de la efectividad y que se pueda implementar un control por parte de MECI, en caso tal la situación de riesgo se puede presentar cuando no se cumpla esta política.

   Una estructura organizacional que sea eficiente en la toma de decisiones
   **Amenaza:** a pesar de que existe una estructura organizacional, varias de las oficinas o secretarias no se amparan a los procesos establecidos dentro de la entidad ya que estos no están documentados, se debe realizar un plan para que estas se ajusten a los procesos para que al momento de direccionar se presente una excelente comunicación y que la toma de decisiones sea la más efectiva y conveniente para la entidad.
   **Riesgo:** el riesgo puede estar determinado en que no se presenta una estructura organizacional dinámica**,** que los procesos los realice o ejecute de manera eficiente y eficaz.

2) Adquisición de tecnología actualizada y la capacidad técnica para ejecutar de la institución para realizar los procesos con eficiencia
   **Amenaza:** la gobernación del departamento del cesar en algunos casos no cuenta con los equipos tecnológicos suficientes y esto hace que se presente fallas en la ejecución de los procesos.
   **Riesgo:** el riesgo estaría materializado en que la gobernación no posee equipos tecnológicos de vanguardia y en algunos casos estos son obsoletos, afectando esto la ejecución eficaz de los procesos, además de las fallas en la cobertura de internet, ya que al presentarse, el tiempo de respuesta a los clientes o grupos de interés se incrementaría.

   Tecnología utilizada que este a nivel de los procesos
   **Amenaza:** los sistemas de información en la gobernación del departamento del cesar son variados, y estos presentan características diferentes dependiendo las necesidades y peticiones que se realizan en cada oficina y sectorial, y pocas veces se presenta un método que los conecte y esto afecta los procesos ya establecidos.

**Riesgo:** el nivel de la tecnología utilizada en la gobernación del cesar representa un riesgo latente, ya que la falta o desactualización de esta impide la interacción adecuada con las demás herramientas, afectando directamente los procesos.

3) La capacidad y preparación del talento humano, o nivel de las competencias adquiridas por el recurso humano de la gobernación del departamento del cesar
   **Amenaza:** en algunos casos los cargos que los funcionarios de planta desempeñan no son acordes a sus capacidades o conocimientos, convirtiéndose en una amenaza, esta se subsanaría si cada cargo está representado por el funcionario idóneo.
   **Riesgo:** El nivel de capacidad del talento humano de la gobernación del cesar está acorde con las necesidades de la institución, el riesgo estaría representado en que ubiquen a un funcionario en un cargo en donde no aplique su preparación.

4) Capacidad en el nivel competitivo: el impacto que genera a la gobernación del cesar los servicios y bienes suministrados por los grupos de contratados
   **Amenaza:** la gobernación del cesar cuenta con muchos proveedores que le prestan sus servicios, además cuenta con un proceso de selección con lo cual implementa un control con el establece puntualmente los requerimientos que se necesitan.
   **Riesgo:** en este caso si la contratación cumple con los parámetros establecidos, no se presentara ningún riesgo.

5) Capacidad financiera de la gobernación del cesar: estructuración de los ingresos que recibe la entidad.
   **Amenaza:** en la gobernación del cesar hay un flujo de ingresos variado o mixto, lo que corresponde a ingresos por impuestos directos, ingresos corrientes, transferencias recibidas por concepto de regalías, la amenaza estaría representada en la intervención de terceros en esos ingresos lo cual podría afectar los objetivos y las metas corporativas dentro de la misión de la gobernación del departamento del cesar.
   **Riesgo:** en la situación actual de la gobernación, el riesgo se refleja en la intervención hecha por demás instituciones de las cuentas de la gobernación, (representado por embargos) lo cual afectaría el logro o el cumplimiento de las metas por parte de la entidad.

## COMPONENTE INFORMATIVO DEL CONTEXTO ACTUAL DE LA GOBERNACION DEL DEPARTAMENTO DEL CESAR

### Contexto externo

***Factores que posiblemente se presentan en el exterior de la entidad y riesgos identificados fuera de la institución***

***Económicos***

- **Presencia de una recesión en la economía de la entidad:** problemas y dificultades en el cumplimiento de la ejecución del plan de desarrollo (planes, programas, proyectos) por la falta de los recursos con los que cuenta la entidad.

***Políticos***

- ***Cambios o modificaciones que se presentan en la entidad correspondiente a las fuentes de ingreso en materia legal:*** un cambio en el aspecto legal a las fuentes de ingreso afectaría directamente a la gobernación del cesar ya que impediría el cumplimiento de los objetivos estratégicos, esto afectaría enormemente la disponibilidad de los recursos con lo que cuenta la gobernación.
- ***La no estabilidad política:*** este es un aspecto que la gobernación del departamento del cesar no pude controlar, ya que esta situación se determina socialmente y está fuera de los controles establecidos dentro de la entidad.

***Tecnológicos***

- ***Resistencia a los cambios en la tecnología utilizada por la entidad:*** esta es una situación en la que se puede presentar riesgos, ya que existe renuencia al cambio, y hay funcionarios que prefieren seguir operando de la misma manera que hace mucho lo hacen.
- ***Eficiencia en los sistemas de comunicación:*** el riesgo estaría representado en una eventual falla en la tecnología, lo cual afectaría la comunicación al interior de la entidad.

***Contexto interno***

***Factores que posiblemente se presentan en el interior de la entidad y riesgos identificados en la institución***

***Capacidad directiva***

- ***Imagen proyectada al interior de la gobernación del cesar de los directivos:*** La capacidad o estilo de la dirección que implementa para la ejecución de los procesos dentro de la entidad, es una base fundamental para la medición del elemento de control que implementa MECI y CALIDAD, los llamados “estilos de dirección” por parte del ente de control, con lo cual el riesgo estaría materializado por el no cumplimiento de las políticas aceptadas dentro de los proceso manejados al interior de la entidad.

- ***Una estructura organizacional eficaz que permita la toma de las decisiones más adecuadas para la ejecución de los procesos:*** el riesgo se podría materializar si dentro de la entidad no existe una estructura directiva eficiente, efectiva y que sea dinámica y que se acople a los procesos que están establecidos.

***Capacidad tecnológica:***

- ***Habilidad técnica dentro de la gobernación del cesar para llevar a cumplimiento los procesos que a esta le competen:*** El riesgo puede estar materializado en que la entidad no posea los equipos tecnológicos acorde a los procesos que debe manejar y la ausencia de una adecuada cobertura de internet, estas fallas podrían afectar la ejecución de los procesos en cuanto a calidad y tiempo de respuesta a los grupos de interés o a sus clientes ya establecidos.
- ***La tecnología debe estar a un nivel acorde a los procesos:*** el nivel de la tecnología que adquiere la gobernación del cesar debe estar acorde a los procesos, para que estos sean ejecutados con eficiencia, si esto no se presenta, el nivel de interacción de las herramientas seria mínimo y esto afectaría la ejecución de los ya mencionados procesos.

***Talento humano:***

- ***Competencias del talento humano de la entidad:*** el nivel de competencias del talento humano debe ser acorde a los procesos que a estos le asignen, de presentarse lo contrario, se podrían presentar fallas en la ejecución de los procesos, porque estos serían asignados a funcionarios que no tienen las competencias requeridas para llevar a buen término cada uno de ellos.

***Capacidad competitiva dentro de la gobernación:***

- ***El impacto dentro de la entidad de los bienes y servicios que le suministra a sus grupos de interés:*** solo se presentaría el riesgo si los bienes y servicios no son suministrados por la entidad.
- ***Que la entidad sea eficiente en el tiempo de respuesta de las quejas y reclamos a sus grupos de interés:*** No se presenta ningún riesgo en esta situación, ya que la capacidad de la gobernación del cesar es eficiente.

***Capacidad financiera de la gobernación del cesar:***

- ***Estructura de los ingresos de la entidad:*** esto no representa un riesgo para la entidad, solo que sus ingresos sean intervenidos y se presenten

"embargos", con lo cual se afectaría estos ingresos y tendría un impacto en la ejecución de los planes y proyectos.

***Contexto del proceso***

- ***Diseño del proceso:*** Este debe tener una claridad en la descripción del alcance y cuál debe ser el objetivo del proceso.
- ***Interacciones con los demás procesos de la entidad:*** se debe tener una relación precisa con los demás procesos en el aspecto de insumos, los proveedores, productos, usuarios y clientes.
- ***Transversalidad:*** Procesos que definen los lineamientos que son netamente necesarios para el desarrollo de todos los procesos de la entidad.
- ***Procedimientos asociados:*** se debe tener pertinencia en los procedimientos que se desarrollan dentro de los procesos.
- ***Responsables de cada uno de los procesos:*** hay que determinar los grados de responsabilidad y la autoridad que se tiene de los funcionarios que están asignados a los procesos.
- ***Comunicación entre los procesos establecidos:*** se debe tener una efectividad en los flujos de información determinados en la interacción de cada uno de los procesos.

## 5. INVENTARIO DE ACTIVOS DE INFORMACIÓN

### *IDENTIFICACION DE LOS ACTIVOS DE INFORMACION PRESENTES EN LA GOBERNACIÓN DEL DEPARTAMENTO DEL CESAR*

A continuación se presenta un inventario con los principales activos *de Información* que se identificaron dentro de la gobernación del departamento del cesar, después de hacer una visita a cada una de las oficinas y sectoriales de la entidad, se relaciona los que se consideran se presentan en la mayoría de estas y que están ajustados a los procesos que se llevan al interior de la entidad. Se relacionan los siguientes aspectos dentro de los activos con los que cuenta la gobernación del departamento del cesar: "Procesos que se

manejan dentro de la entidad, el nombre y tipo de activo de información, y por ultimo su ubicación, propietario y custodio.

| PROCESOS | | | | Nombre de Activo | Descripción/Observaciones | Tipo de Activo | Ubicación | Propietario | Custodio |
|---|---|---|---|---|---|---|---|---|---|
| ESTRATEGICO | MISIONAL | APOYO | EVALUACIÓN | | | Tipo | | | |
| | | G. JURIDICA | | PROCESOS JUDICIALES | Expediente que compila todas las actuaciones judiciales adelantadas por el Departamento frente a los procesos de demanda que afronta | Información | Archivo de Gestión de la oficina asesora jurídica y Archivo General del Departamento | Oficina Asesora Jurídica | Profesional a cargo de los procesos de Judiciales |
| | | G. TALENTO HUMANO | | PROCESOS DISCPLINARIOS | Expediente que contiene todas las actuaciones relacionadas con investigaciones disciplinarias que se adelantan contra funcionarios de la Administración Departamental | Información | Archivo de Gestión de la Dirección de Control Interno Displinarios y Archivo General del Departamento | Dirección Control Interno Displinario | Profesional Universitario-secretario judicial |
| Mejoramiento Institucional. | | | | INVENTARIO DOCUMENTAL DE PROCESOS DISPLINARIOS | Base de datos que contiene el registro o inventario de todos los procesos displinarios que adelanta la oficina y el estado de cada proceso | Información | Archivo de Gestión de la Dirección de Control Interno Displinarios y Archivo General del Departamento | Dirección Control Interno Displinario | Profesional Universitario-secretario judicial |
| | INSPECCION VIGILANCIA Y CONTROL | | | EXPEDIENTES FISICOS DE CONSEJO DE SEGURIDAD DE ORDEN PÚBLICO | Expediente que contiene las actas de los diferentes consejos de seguridad que se llevan a cabo en el departamento. | Información | Archivo de Gestión de la Secretaria de Gobierno Y Archivo General del Departamento | Secretaria de Gobierno | Profesional Universitario |
| | INSPECCION VIGILANCIA Y CONTROL | | | EXPEDIENTES FISICOS DE COMITÉ PENITENCIARIO | Expediente que contiene las actas de los comité penitenciarios | Información | Archivo de Gestión de la Secretaria de Gobierno Y Archivo General del Departamento | Secretaria de Gobierno | Profesional Universitario |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | INSPECCION VIGILANCIA Y CONTROL | | | EXPEDIENTES FISICOS DE LAS ACTAS DE COMISIÓN DEPARTAMENTAL PARA LA COORDINACIÓN Y SEGUIMIENTO A LOS PROCESOS ELECTORALES | Expediente que contiene las actas de las comisiones electorales. | Información | Archivo de Gestión de la Secretaria de Gobierno Y Archivo General del Departamento | Secretaria de Gobierno | Profesional Universitario |
| | GESTION DE DLLO | | | EXPEDIENTES FISICOS DE LAS PERSONERÍAS JURÍDICAS RECONOCIDAS | Contienen los documentos que se requieren para el reconocimiento de las Personerías Jurídicas que se otorgan a las juntas de acción comunal, ONG, Organizaciones Deportivas, Entidades que tengan fines Sociales como Cuerpo de Bomberos, Damas Grises, Damas Rosadas, Defensa Civil entre otras. | Información | Archivo de Gestión de la Secretaria de Gobierno Y Archivo General del Departamento | Secretaria de Gobierno | Profesional especializado y auxiliar administrativo |
| | GESTION DE DLLO | | | PROGRAMA DE ASISTENCIA A COMUNIDADES INDIGENAS | Se manejan los procesos de indígenas víctimas del conflicto armado, zonas veredales, espacios de capacitación territorial, políticas públicas, medidas cautelares, pueblo wiwa casos de violaciones a niños menores, conforme lo dispuesto en el decreto 1527 del 25 de noviembre de 2004 sobre la estructura de la secretaria de gobierno. | Hardware | Oficina Secretaria de Gobierno | Secretaria de Gobierno | Profesional Especializado |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | GESTION DE DLLO | | | PLANES INTEGRALES ÚNICOS A DESPLAZADOS | Se maneja lo concerniente a desplazados víctimas del conflicto armado, zonas veredales, espacios de capacitación territorial, políticas públicas, medidas cautelares, derechos humanos y paz. | Hardware | Oficina Secretaria de Gobierno | Secretaria de Gobierno | Profesional Especializado |
| | GESTION DE DLLO | | | PROGRAMAS PARA COMUNIDADES AFRODESCENDIENTES | Se manejan los programas de enlace entre la comunidad Afro descendientes y la Gobernación del Cesar, consejo comunitario en los que se interactúa con las políticas públicas a favor de dicha comunidad. | Hardware | Oficina Secretaria de Gobierno | Secretaria de Gobierno | Profesional Especializado |
| | GESTION DE DLLO | | | INVENTARIO DOCUMENTAL DE PROCESOS JUNTAS DE ACCION COMUNAL, VEEDURIAS CIUDADANAS, SINDICATOS. | Se incluye información de Juntas de acción comunal, veedurías ciudadanas entidades sin ánimo de lucro (ESAL) Sindicatos, bomberos, fundaciones entre otras. Se encuentran almacenados en un archivo de gestión de la Secretaría de Gobierno. | Información | Archivo de Gestión de la Secretaria de Gobierno Y Archivo General del Departamento | Secretaria de Gobierno | Técnico operativo |
| | GESTION DE DLLO | | | INVENTARIO DOCUMENTAL DE ALERTAS TEMPRANAS DE AMENAZAS DE VIDA | Información correspondiente a procesos judiciales, pruebas y respuestas a requerimientos | Información | Oficina asesora de paz | Despacho del Gobernador | Asesor de Paz |
| | GESTION DE DLLO | | | DISCO DURO CON LA INFORMACIÓN DEL REGISTRO FILMICO Y FOTOGRPAFICO | En este computador se almacena el registro fílmico y fotográfico histórico de la entidad | Hardware | Oficina de Prensa | Despacho del Gobernador | Asesor de prensa |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | GESTION EN SALUD Y PS | | | ARCHIVO DE EXCEL CON LA INFORMACIÓN DE LAS MUJERES INSCRITAS DE LA CASA TALLER | Contiene los datos de todas las mujeres inscritas en los diferentes programas de la casa taller. | Hardware | Oficina departamental de la mujer | Despacho del Gobernador | Profesional Universitario |
| | | G. JURIDICA | | REGISTRO DE PROCESOS JUDICIALES | Registro de los procesos judiciales del departamento desde el momento de la notificación hasta su terminación y archivo (fallo y sentencia de cualquier instancia). No existe copia de respaldo. El respaldo es a través del drive personal de la funcionaria. | Hardware | Oficina asesora jurídica | Oficina Asesora Jurídica | Jefe oficina asesora jurídica |
| | | G. JURIDICA | | EXPEDIENTE FÍSICO DE LAS ACTUACIONES JURÍDICAS | Contiene los expedientes de defensa judicial y las actuaciones jurídicas adelantadas por la entidad. | Información | Archivo de Gestión de la Oficina Asesora Jurídica Y Archivo General del Departamento | Oficina Asesora Jurídica | Jefe oficina asesora jurídica |
| | | G. DOCUMENTAL | | ARCHIVO DE PROYECTOS APROBADOS Y PRIORIZADOS | Archivo y almacenamiento de carpetas con proyectos aprobados y priorizados en la base de datos del Banco de Proyectos, en la cual se escanean para organizarlos en medio físico y digital en carpetas compartidas con actas de priorización, acuerdos regionales, el tiempo estipulado para transferir al Archivo General Departamental son de 5 años. | Hardware | Archivo de Gestión de la Oficina Asesora de Planeación Y Archivo General del Departamento | Oficina Asesora de Planeación | Profesional Especializado |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Planeación del Desarrollo | | | | ARCHIVO DE EXCEL CON LA INFORMACIÓN DE LA DOCUMENTACION RECIBIDA Y GENERADA EN EL DESPACHO, | Se organizan y digitalizan los documentos que ingresan y se generan desde el despacho del gobernador, facilitando la búsqueda de información necesaria para su gestión | Software | Despacho del Gobernador | Despacho del Gobernador | Auxiliar Administrativo |
| Planeación del Desarrollo | | | | BASE DE DATOS DE GESTIÓN DE PQRS DIRIGIDAS AL SEÑOR GOBERNADO | Base de datos elaborada en Excel donde se almacena la información de la gestión de los derechos de petición dirigidos al señor Gobernador. Contiene la fecha de vencimiento, la oficina responsable y el radicado. | Información | Oficina de Asuntos Internos | Asesor Asuntos Internos | Profesional Universitario |
| | GESTION EDUCATIVA | | | EXPEDIENTE FÍSICO DE LOS CONVENIOS SUSCRITOS CON FEDECESAR, LAS UNIVERSIDADES, EL MINISTERIO DE EDUCACIÓN Y LOS ENTES TERRITORIALES MUNICIPALES | Realizar las supervisiones a los contratos al programa de fedecesar, Convenios, Actas de inicio, liquidación; interventorías. Datos de los convenios con las universidades (UPC, UNAB, UIS, PAMPLONA y MAGDALENA) Datos del contrato de la interventoría. / Componente de infraestructura educativa con el Ministerio de educación o con recurso propios a través de contratos directos o convenios con los municipios | Información | Archivo de Gestión de la Secretaria de Educación Y Archivo General del Departamento | Secretaria de Educación | Profesional Especializado |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | GESTION EDUCATIVA | | | EXPEDIENTE FÍSICO DE LOS PROYECTOS TRANSVERSALES Y PEDAGÓGICOS ADELANTADO CON LOS ESTABLECIMIENTOS EDUCATIVOS | Maneja los proyectos transversales y pedagógicos con sus respectivos soportes. La información se almacena identificado de la siguiente forma: Macro proceso, proceso, subproceso, meta y actividad. | Información | Archivo de Gestión de la Secretaria de Educación Y Archivo General del Departamento | Secretaria de Educación | Supervisor de educación |
| | GESTION EDUCATIVA | | | EXPEDIENTE FÍSICO DE AUDITORIAS DE CALIDAD | Contiene las listas de chequeo aplicadas a cada proceso, el plan de auditoria, informe de auditoría, evaluación de la auditoria, acciones correctivas, acciones preventivas y plan de acción de acuerdo a las auditorias. . | Información | Archivo de Gestión de la Secretaria de Educación Y Archivo General del Departamento | Secretaria de Educación | Profesional Especializado |
| | GESTION EDUCATIVA | | | EXPEDIENTE FÍSICO DE REVISIÓN POR LA DIRECCIÓN | Contiene información de las actas de comité directivo donde se reúne el secretario con los profesionales de las áreas para evaluar los procesos, sus dificultades, donde además se dan las directrices sobre el plan de trabajo durante el mes. Todo el expediente se encuentra clasificado por año y por tema que sirven de insumos para la visita del ICONTEC; | Información | Archivo de Gestión de la Secretaria de Educación Y Archivo General del Departamento | Secretaria de Educación | Profesional Especializado |
| | GESTION EDUCATIVA | | | EXPEDIENTE FÍSICO DE LOS MANUALES DE FUNCIONES | Información de los manuales de funciones de cada empleado de planta de los funcionarios de la dependencia y los colegios | Información | Archivo de Gestión de la Secretaria de Educación Y Archivo General del Departamento | Secretaria de Educación | Profesional Especializado |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | GESTION EDUCATIVA | | | DISCO DURO CON LA INFORMACIÓN DE MANUALES DE PROCEDIMIENTOS Y FUNCIONES | Se almacenan los procedimientos escaneados, formatos y se encuentra el listado maestro de documentos que se actualiza permanentemente. No se elaboran copias de respaldo de esta información. Manuales de funciones de cada empleado de planta de los funcionarios de la dependencia y los colegios | Hardware | OFICINA INSPECCION VIGILANCIA Y CONTROL | Secretaria de Educación | Profesional Especializado |
| | GESTION EDUCATIVA | | | DISCO DURO CON LA INFORMACIÓN DEL LISTADO MAESTRO DE DOCUMENTOS | Se almacena la información de los registro de los procedimientos que se actualizan permanentemente. | Hardware | OFICINA INSPECCION VIGILANCIA Y CONTROL | Secretaria de Educación | Profesional Especializado |
| | GESTION DE DLLO | | | BASE DE DATOS SOBRE EVENTOS NATURALES | Maneja la información histórica de las afectaciones naturales y desastres que se presentan en el dpto. Del cesar, además de alertar y dar pronósticos de alertas hidrometodologicas. | Información | OFICINA DE GESTION DEL RIESGO YCAMBIO CLIMATICO | OFICINA DE GESTION DEL RIESGO YCAMBIO CLIMATICO | Jefe de Oficina |
| | INSPECCION VIGILANCIA Y CONTROL | | | EXPEDIENTE FÍSICO DE MECANISMOS DE PARTICIPACIÓN SOCIAL EN SALUD | Maneja la Información de los diferentes mecanismos de participación social en salud (copacos, SIAU, SAC, consejo territorial, comité de ética hospitalarias, veedurías ciudadanas, comité de discapacidad, asociaciones de usuarios convenios interadministrativos y de cooperación). | Información | Archivo de Gestión de la Secretaria de Salud Y Archivo General del Departamento | Secretaria de Salud | Profesional Universitario área de la salud |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | INSPECCION VIGILANCIA Y CONTROL | | | EXPEDIENTE FÍSICO DE LICENCIAS DE SALUD OCUPACIONAL, EMISORES Y RAYOS X | Expediente que contiene resoluciones de títulos profesionales en salud, licencias de emisores, rayos X, licencias de salud ocupacional, se formulan cargos e investigaciones en contra de IPS, sanciones. Son 3 copias físicas que reposan en la misma oficina, no obstante no se encuentran escaneadas y salvaguardadas en otro lugar distinto a la secretaria de salud. | Información | Archivo Vida saludable y condiciones no trasmisibles y Archivo General del Departamento | Secretaria de Salud | Secretaria ejecutiva |
| | INSPECCION VIGILANCIA Y CONTROL | | | EXPEDIENTE FÍSICO DE DELEGACIONES DE JUNTAS DIRECTIVAS | Expediente que contiene delegaciones de juntas directivas de los Hospitales del Departamento. | Información | Archivo Vida saludable y condiciones no trasmisibles y Archivo General del Departamento | Secretaria de Salud | Secretaria ejecutiva |
| | INSPECCION VIGILANCIA Y CONTROL | | | REGISTRO DE RESOLUCIONES RADICADAS EN LA SECRETARIA DE SALUD | Es un libro donde se lleva un registro de todas las resoluciones que se radican y que firma la Secretaría de Salud, que contiene número, objeto y fecha de expedición | Información | Archivo Vida saludable y condiciones no trasmisibles y Archivo General del Departamento | Secretaria de Salud | Secretaria ejecutiva |
| | INSPECCION VIGILANCIA Y CONTROL | | | EXPEDIENTE FÍSICO DE ASISTENCIA TÉCNICA A LOS MUNICIPIOS SOBRE EL PAMEC DEPARTAMENTAL | Contiene información relacionada con la asistencia técnica a los 24 municipios del departamento sobre el Programa de Auditoria para el Mejoramiento de la Calidad de la Atención en Salud y el Sistema de Información para la Calidad. | Información | Archivo de Gestión de la Secretaria de Salud Y Archivo General del Departamento | Secretaria de Salud | Profesional especializado del área de la salud |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | INSPECCION VIGILANCIA Y CONTROL | | | EXPEDIENTE FÍSICO DE LA DEFENSA JUDICIAL DE LA SECRETARÍA DE SALUD | Contiene la información de las respuestas e impugnación de las acciones de tutela, derechos de petición, seguimiento, control de los incidentes de desacato que se proponen en contra de la secretaría de salud y funcionarios de dicha sectorial por algún incumplimiento de los fallos de tutela. Así mismo, contiene información de la emisión de conceptos dirigidos a la oficina de contratación por solicitud de esta en aquellos casos donde se pretenda demandar al Dpto. del Cesar por la vía administrativa. | Información | Archivo de Gestión de la Secretaria de Salud Y Archivo General del Departamento | Secretaria de Salud | Secretario de salud |
| | INSPECCION VIGILANCIA Y CONTROL | | | RS | Sistema de información que contiene la base de datos de la población BDUA (Base de Datos Única de Afiliados) del Dpto. Dicho software tiene paramen tizado los procedimientos, los contratos, los diagnósticos, medicamentos, las IPS. A través del sistema de información se revisan históricos del usuario. | Software | ATENCION CIUDADANA | Secretaria de Salud | Profesional Especializado |
| | INSPECCION VIGILANCIA Y CONTROL | | | SITIS | A través del aplicativo se radican las cuentas, se realizan procesos de auditorías, módulos de facturación, control y procesos administrativos | Software | Asuntos en salud | Secretaria de Salud | Líder oficina de Aseguramiento |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | hospitalarios del componente de asuntos en salud de la Secretaria de Salud Dptal. | | | | |
| | INSPECCION VIGILANCIA Y CONTROL | | | ARCHIVO FÍSICO DE LAS ACTAS DE DEVOLUCIÓN DE LAS FACTURAS | Contiene información de las actas de devolución a los distintos prestadores de salud de las facturas de los diferentes tipos de atención proporcionados a la población pobre no asegurada del Departamento del Cesar | Información | Validación | Secretaria de Salud | Líder oficina de Aseguramiento |
| | INSPECCION VIGILANCIA Y CONTROL | | | ARCHIVOS PLANOS RIPS | Contiene la información de los registros individuales de prestación de servicios de salud que envían de manera periódica los prestadores. | Hardware | COMPONENTE DE VIGILANCIA EPIDEMIOLOGICA, TBC Y LEPRA | Secretaria de Salud | Profesional Especializado |
| | GESTION DE TRAMITES | | | BASE DE DATOS DE REGISTRO DE TITULOS DE LOS PROFESIONALES DE LA SALUD | Base de datos elaborada en Excel que Contiene la información de los actos administrativos donde se autoriza ejercer la profesión en el territorio Nacional | Software | Salud publica | Secretaria de Salud | Líder de salud pública |
| | GESTION EN SALUD Y PS | | | BASE DE DATOS DE MORVILIDAD DE NIÑOS POR DESNUTRICIÓIN EN DEL DEPARTAMENTO | Base de datos elaborada en Excel que contiene información de los casos de morbilidad de los niños por desnutrición de los 25 municipios del dpto. Del cesar. | Información | Gestión en salud y promoción social | Secretaria de Salud | Jefe de Oficina |
| | GESTION DE DLLO | | | EXPEDIENTE FISICO DE LAS ESTADISTICAS HISTORICAS DEL SECTOR AGROINDUS | ARCHIVO QUE CONTIENE LAS ESTADISTICAS HISTORICAS DEL SECTOR AGROINDSTRIAL | Información | Secretaria de Agricultura | Profesional universitario | Profesional Universitario |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | TRIAL | | | | | |
| | | CONTRATACION E INTERVENTORIA. | | PCT | Administra la información financiera de la entidad. Balance general, registran ingresos, egresos, registros presupuestales, ingresos, conciliaciones, certificado de disponibilidad, informes contables, consultas, elaboración de cuentas, legalización de viáticos, reportes, etc. | Software | Secretaria de Hacienda | Secretaria de Hacienda | Secretaria de Hacienda |
| | | G. FINANCIERA | | DISCO DURO QUE CONTIENE LA INFORMACION DE LAS CONCILIACIONES BANCARIAS | Carpetas con información de las conciliaciones bancarias | Hardware | Oficina de Contabilidad | Secretaria de Hacienda | Líder de Contabilidad |
| | | G. DOCUMENTAL | | Archivos Actos Administrativos Presupuestales | Carpetas físicas (Decretos y resoluciones, Requerimientos presupuestales para los entes de control, datos presupuestales auditorias, derechos de peticiones, entidades bancarias, comunicaciones oficinales internas en su gran mayoría y externas entre otros) | Información | Oficina de Presupuesto | Secretaria de Hacienda | Líder de Presupuesto |
| | | G. FINANCIERA | | Informes Financieros | Archivos de información dentro del computador tales como informes al Ministerio de Hacienda, Ministerio de salud, Supe salud. Trimestralmente se presenta el FUT, SGR | Hardware | Oficina de Presupuesto | Secretaria de Hacienda | Líder de Presupuesto |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | presupuestal y SGR. El equipo no tiene clave de administrador. | | | | |
| | | G. FINANCIERA | | Base de datos Contribuyentes y clasificación de impuestos | Contiene el número del proceso, nombre de identificación del contribuyente, el concepto es decir el tipo de impuesto, las vigencias, la ubicación en el archivo físico, la asignación es decir qué abogado lo tiene, el monto de la deuda, el título ejecutivo, id del número ejecutivo, la clasificación de la cartera (mediano, bajo o alto riesgo) actuación surtida entre otros, tiene una confidencialidad alta integridad y disponibilidad alta. | Software | Rentas | Secretaria de Hacienda | Profesional Universitario |
| | | G. FINANCIERA | | EXPEDIENTE FÍSICO DE LAS ACTUACIONES PROCESALES SOBRE EL PAGO DE LA OBLIGACIÓN TRIBUTARIA | Contiene la información de todas las actuaciones procesales tendientes a obtener el pago de la obligación tributaria. | Información | Oficina de rentas | Secretaria de Hacienda | Profesional Especializado |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | G. FINANCIERA | | SIIAF | Se toma lo no ejecutado del presupuesto, conciliaciones bancarias, legalización de viáticos. Todas las áreas deberían estar integradas al área contable. No están integrados los módulos al módulo financiero por ello hay que estar enviando oficios. Integración de interfaz. Debería existir un archivo plano con toda la información de la entidad que se encuentra dispersa. El jefe tiene que consolidar toda la información en Excel. Se consolida a través de Excel. | Software | Oficina de Contabilidad | Secretaria de Hacienda | Líder de Contabilidad |
| | | G. FINANCIERA | | Archivo de Excel del Registro de Cartera Morosa | Recaudar la cartera morosa por concepto de impuesto vehicular en el departamento del cesar | Hardware | Rentas | Secretaria de Hacienda | Profesional Universitario |
| | | G. FINANCIERA | | Sycstrace | verificar, analizar y procesar la información de recaudos de impuestos de licores, cervezas y cigarrillos importados y nacionales para ejercer control al recaudo | Software | Rentas | Secretaria de Hacienda | Líder de Rentas |
| | | G. FINANCIERA | | LIQUIDACION DE IMPUESTOS | verificar que los impuestos que se deben recaudar en el departamento se deben liquidar y recaudar en el tiempo correcto | Hardware | Rentas | Secretaria de Hacienda | Profesional Universitario |
| | | G. DOCUMENTAL | | EXPEDIENTES FISICOS CONTRACTUALES DE LA SECTORIAL INFRAESTRUCTURA | Contiene la información de los expedientes contractuales de contratos de obras e interventorías de la secretaria de infraestructura. | Información | Archivo de Gestión de la Secretaria de Infraestructura Y Archivo General del Departamento | Secretaria de Infraestructura | Técnico Operativo |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | GESTION DE DLLO | | | EXPEDIENTE FÍSICO DE LOS PROYECTOS DE LA SECRETARIA DE MINAS | Contiene información de los proyectos de gasificación, de apoyo a las pequeñas minerías, y energía eléctrica del departamento | Información | Secretaria de Minas | Secretaria de Minas | Secretario de Minas |
| | | CONTRATACION E INTERVENTORIA. | | EXPEDIENTE FISICO DE LOS PROCESOS CONTRACTUALES | Contiene la información de las diferentes modalidades de contratación que adelanta la entidad (personal, convenios, licitaciones). | Información | Archivo de Gestión de la Secretaria General Y Archivo General del Departamento | Secretaria General | Secretario General |
| | | CONTRATACION E INTERVENTORIA. | | SERVIDOR SECRETARIA GENERAL | Contiene la información digitalizada (escaneada Original) de los expedientes contractuales de la entidad | Hardware | Secretaria General | Secretaria General | Secretario General |
| | | CONTRATACION E INTERVENTORIA. | | HUMANO | Sistema de información que permite generar la nómina de las plantas globales y pensionados del Dpto. del Cesar | Software | Secretaria General | Secretaria General | Técnico Operativo |
| | | ADMON RECURSOS FISICOS | | EXPEDIENTE FISICO DEL INVENTARIO DEL ALMACEN | Contiene la información de entradas y salidas de los inventarios de los recursos físicos de la entidad. | Información | Archivo de Gestión de la Secretaria General (almacén) Y Archivo General del Departamento | Secretaria General | Almacenista General |
| | | ADMON RECURSOS FISICOS | | SERVIDOR PCT | Equipo donde se aloja la base de datos con la información financiera de la entidad | Hardware | Sistemas | Secretaria General | Profesional Especializado |
| | | ADMON RECURSOS FISICOS | | SERVIDOR SIRCC | Equipo donde se aloja la base de datos con la información de Radicación de contratos y convenios, en los cuales se reporta todas las novedades relacionadas con los mismos | Hardware | Sistemas | Secretaria General | Profesional Especializado |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | ADMON RECURSOS FISICOS | | SERVIDOR SIGNUS | Equipo donde se aloja la base de datos con la información del Sistema de gestiones, declaraciones de estampillas, degüellos y registro del Dpto. | Hardware | Sistemas | Secretaria General | Profesional Especializado |
| | | ADMON RECURSOS FISICOS | | SERVIDOR CONTROL DOC | Equipo donde se aloja la base de datos con la información del Sistema de Administración, gestión y trámite de comunicaciones oficiales de la entidad | Hardware | Sistemas | Secretaria General | Profesional Especializado |
| | | ADMON RECURSOS FISICOS | | SERVIDOR HUMANO | Equipo donde se aloja la base de datos con la información de la nómina de las plantas globales y pensionados del Dpto. del Cesar. | Hardware | Sistemas | Secretaria General | Profesional Especializado |
| | | ADMON RECURSOS FISICOS | | SERVIDOR CHIP | Equipo donde se aloja la base de datos con la información de los estados financieros de la entidad e informe del control interno contable de la entidad | Hardware | Sistemas | Secretaria General | Profesional Especializado |
| | | G. DOCUMENTAL | | Base de datos del inventario general de archivo | Es un archivo de Excel que contiene la Base de datos del inventario general de archivo | Hardware | PROGRAMA DE ARCHIVO | Programa Líder de Archivo | Líder de Archivo |
| | | G. DOCUMENTAL | | Depósito de fondos de archivo | Espacio dado para la preservación, conservación, custodia y seguridad de los documentos de archivo de los distintos fondos. | Otros. | PROGRAMA DE ARCHIVO | Programa Líder de Archivo | Líder de Archivo |
| | | G. DOCUMENTAL | | Base de datos del proceso de Disposición final de los archivos | Base de datos donde se almacena la información del proceso de Disposición final de los archivos | Hardware | PROGRAMA DE ARCHIVO | Programa Líder de Archivo | Líder de Archivo |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | G. DOCUMENTAL | | CONTROL DOC | Sistema de Administración, gestión y trámite de comunicaciones oficiales, Comunicaciones internas, externas, circulares, documentos recibidos a través de ventanilla única de correspondencia | Software | PROGRAMA LIDER DE ARCHIVO | Secretaria General | Líder Programa Archivo |
| | | CONTRATACION E INTERVENTORIA. | | SIRCC | Sistema de Radicación de contratos y convenios, en los cuales se reporta todas las modificaciones que se surten a los procesos hasta su liquidación, Informes para los entes de control y diferentes sectoriales, se generan estadísticas, alimenta el SIRECI, oficio de supervisión, solicitud de registros, radicación y control de contratos, certificaciones contractuales, reporte de todos los contratos y convenios suscritos por la entidad en las diferentes vigencias. | Software | Secretaria General | Secretaria general | Sectario General |
| | | G. FINANCIERA | | SIGNUS | Sistema de gestiones, declaraciones de estampillas, degüellos y registro del Dpto.; Es un programa para presentación de declaraciones (estampillas, degüellos, gasolina, lotería foráneas. Informes de pago de las declaraciones, reportes. | Software | Oficina de Rentas | Oficina de Rentas | Jefe Oficina de Rentas |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | G. TALENTO HUMANO | | HUMANOS | Sistema de información que permite generar la nómina de las plantas globales y pensionados del Dpto. del Cesar. | Softw are | Secretaria general | Oficina de Gestión Human a | Jefe Oficina de Gestión Humana |
| | APOYO GESTIO TERRRIT ORIAL. | | | SAGEP | Realizar seguimiento al plan de desarrollo en sus diferentes dimensiones así como la evaluación física y financiera al plan | Softw are | Oficina Asesora de Planeación | Oficina Asesora de Planeac ión | Jefe Oficina Asesora de Planeaci ón |
| | | G. FINANCIE RA | | SISTEMAS Y COMPUTADO RES | Almacena la información del recaudo de las empresas de vinos, licores, cervezas y aperitivos de empresas nacionales e importadas, y de cigarrillos | Softw are | Oficina de Rentas | Oficina de Rentas | Jefe Oficina de Rentas |
| | | G. FINANCIE RA | | Expedientes cobros tributarios | Contiene todas las actuaciones procesales tendientes a obtener el pago de la obligación tributaria. La información no se encuentra organizada en archivadores sin embargo sin ningún tipo de seguridad. La información se puede reconstruir en caso de un incendio. Los entes de control, los contribuyentes pueden acceder a esta información. Cuando llueve se inunda a raíz del ascensor que se colocó se filtra el agua por debajo del cubículo. Los cables de red y eléctricos se encuentran expuestos. Es de aclarar que el espacio laboral es muy pequeño | Inform ación | Rentas | Secreta ria de Haciend a | Profesio nal Universit ario |

### a. CANTIDAD DE ACTIVOS DE INFORMACIÓN

| SECTORIAL | CANTIDAD DE ACTIVOS | PORCENTAJE |
|---|---|---|
| DESPACHO | 34 | 9,52% |
| OFICINA ASESORA DE PLANEACION | 8 | 2,24% |
| SECRETARIA DE AGRICULTURA | 4 | 1,12% |
| SECRETARIA DE AMBIENTE | 4 | 1,12% |
| SECRETARIA DE DEPORTES | 4 | 1,12% |
| SECRETARIA DE EDUCACIÓN | 37 | 10,36% |
| SECRETARIA DE GOBIERNO | 28 | 7,84% |
| SECRETARIA DE HACIENDA | 49 | 13,73% |
| SECRETARIA DE INFRAESTRUCTURA | 3 | 0,84% |
| SECRETARIA DE MINAS | 3 | 0,84% |
| SECRETARIA DE SALUD | 169 | 47,34% |
| SECRETARIA GENERAL | 14 | 3,92% |
| **TOTALES** | **357** | **100%** |

Se evidencia que el 47% de los activos de información se identificaron en la Secretaría de Salud, seguido la secretaría de hacienda con 13,73%. Esta tendencia indica la sentida necesidad de una correcta gestión de los Activos de Información que dan soporte a los diferentes procesos de la Gobernación del Cesar en especial en las sectoriales antes mencionadas. Esta gestión incluye la actualización periódica del inventario de activos de información, responsable o propietario de cada activo, determinar los usos correctos y adecuados de cada uno de ellos, y su recuperación cuando sea necesario para evitar su pérdida o difusión no controlada.

## b. TIPOS DE ACTIVOS DE INFORMACIÓN

| SECTORIAL | HARDWARE | LUGAR | ORGANIZACIÓN | RECURSOS HUMANOS | SERVICIOS | SOFTWARE | DATOS E INFORMACIÓN |
|---|---|---|---|---|---|---|---|
| DESPACHO | 8 | | | | 2 | 9 | 15 |
| OFICINA ASESORA DE PLANEACION | 2 | | | | | | 6 |
| SECRETARIA DE AGRICULTURA | 1 | | | 1 | | | 2 |
| SECRETARIA DE AMBIENTE | | | 2 | | 1 | 1 | |
| SECRETARIA DE DEPORTES | 3 | | | | | 1 | |
| SECRETARIA DE EDUCACIÓN | 19 | 1 | | 1 | | | 16 |
| SECRETARIA DE GOBIERNO | 5 | 1 | | 5 | 1 | 6 | 10 |
| SECRETARIA DE HACIENDA | 7 | | | 2 | | 30 | 10 |
| SECRETARIA DE INFRAESTRUCTURA | 1 | 1 | | 1 | | | |
| SECRETARIA DE MINAS | | | | | | | 3 |
| SECRETARIA DE SALUD | 46 | 2 | | 16 | 1 | 24 | 80 |
| SECRETARIA GENERAL | 9 | 2 | | | | | 3 |
| **PORCETNAJES** | **28,29%** | **1,96 %** | **0,56%** | **7,28%** | **1,40%** | **19,89%** | **40,62%** |
| **TOTAL** | **101** | **7** | **2** | **26** | **5** | **71** | **145** |

Respecto a los tipos de activos de información, es interesante analizar que sólo el tipo de activo “datos e información” concentra el 40,62% del total de los activos de información de la Gobernación del Cesar, siendo la Secretaría de Salud, la sectorial con la más alta

proporción de activos de este tipo de activo respecto a las demás sectoriales. Respecto a dicho tipo de activo prevalecen las bases de datos administradas desde Microsoft Excel, documentos en Microsoft Word, archivos en formato con extensión pdf, expedientes físicos, archivos de gestión de vigencias anteriores, que en el caso particular de la secretaría de salud se encuentra ubicado encuarto donde se almacenan todo tipo de unidades de cajas, carpetas y A-Z, el cual no es el adecuado para conservar este tipo de documentos. Así mismo se evidencia que no posee un mobiliario adecuado para el archivo de Gestión, las unidades de almacenamiento se encuentran en el piso una encima de otra sin ningún tipo de seguridad y expuestas a riesgo de humedad, microorganismos, roedores y/o perdida de documentos. El espacio no cuenta con suficiente iluminación ni ventilación, adicionalmente no existe un responsable de custodio de esta documentación. Cada dependencia ubica sus archivos en cajas sin organización.

Por otra parte, en la secretaría de educación fueron identificados 16 de activos donde gran parte de esta información es compartida en distintos formatos a través del correo electrónico institucional. No obstante, se evidenció que debido al limitado espacio de almacenamiento del correo electrónico, los funcionarios se ven en la obligación de borrar periódicamente información y en muchos casos utilizar correos electrónicos personales.

En este orden de ideas, el tipo de activo de información “Hardware” concentra el 28,29% del total de activos de activos de información de la entidad. Al respecto, la secretaría de salud agrupa la mayor cantidad de activos de este tipo, seguido por la secretaría de educación y el despacho.

Dentro de esta categoría se identificaron gabinetes, equipos servidores, computadores de escritorio, computadores portátiles (en su gran mayoría de uso personal) debido a la insuficiente cantidad de estaciones de trabajo, medios de almacenamiento externos tales como memorias USB y discos duros externos en muchos casos de uso personal sin ningún tipo de control. Así misma información almacenada a través de servicio de alojamiento de archivos en la nube tales como Google Drive y DropBox. En este orden de ideas, dentro de la secretaría de salud se evidenciaron múltiples dificultades de conexión debido a la red obsoleta. Así mismo fallas técnicas en un ventilador del equipo servidor donde se administra la base de datos de las autorizaciones de servicio de salud a la población pobre no asegurada del Departamento del Cesar.

No menos importante, el 19,89% de los activos de información de la entidad corresponde a la categoría software, siendo la Secretaría de Hacienda la sectorial que agrupa la mayor cantidad de activos de este tipo, seguido por la secretaría de salud. Es importante aclarar que se identificaron plataformas web del orden nacional que si bien no corresponden a activos de la entidad, se hizo mención de ellos por ser medios donde se ingresa información de la entidad tales como (RRI) MECANISMOS DE IMPLEMETACIÓN Y VERIFICACIÓN POR PARTE DE LAS FARC Y EL GOBIERNO; RIA (Ruta de Atención a la Primera Infancia) del ICBF; Sistema de Información Integrado para la Identificación, Registro y Caracterización del Trabajo Infantil y sus Peores Formas, SIRITI del Ministerio de Trabajo; SPGR (Sistema presupuestal y giro de regalías) del Ministerio de Hacienda; SUIF (sistema unificado de inversión y finanzas públicas) del DNP entre otros. Así mismo aplicativos de desarrollo propio sin ningún tipo de licenciamiento tales como RS Software no licenciado elaborado por el Ingeniero Orlando Enrique Arrieta Rodríguez quien actualmente ya no se encuentra laborando con la entidad.

Dentro de esta categoría algunos de los sistemas de información más utilizados son:

- **SIRCC:** Sistema de información para la administración de la información contractual de la entidad.
- **PCT Enterprise:** es un Sistema de Información local Administrativo y Financiero. Los Módulos son de gran utilidad para Tesorería, Presupuesto y Contabilidad.
- **CONTROLDOC**: Sistema de información para el envío y recibido de comunicaciones internas y externas.
- **SAGEP:** Sistema de información para realizar el seguimiento a las metas del plan de desarrollo.
- **SOFTWARE DE GESTIÓN PQRD**: sistema de información bajo ambiente web de la Gobernación del Cesar para la gestión de Peticiones, Quejas, reclamos y demandas, elaborado por estudiantes de la UPC. Actualmente se encuentra en funcionamiento pero aún no se encuentra integrado como módulo del Control Doc independiente. Este software es sólo de acceso al SAC (Servicio de atención a la comunidad de la Secretaría de Salud Departamental) y las secretaría de salud municipal y las ESEs.
- **SITIS**: Sistema de información bajo ambiente web el cual inicio su implementación a partir del 1 de septiembre para la administración de los procesos de asuntos en salud. Dicho aplicativo presenta errores en tiempo de ejecución entre los cuales se mencionan: no permite generar reporte de radicación de cuentas, No permite anular una factura por error involuntario;.Idem en los prestadores. No permite registrar el flujo de información de la factura, no permite llevar el procedimiento de devolución administrativa, no permite realizar devolución de facturas; no permite generar reportes de radicación por tiempo mes año, prestador; cuando se hace la pre radicación de la factura en una fecha posterior a la radicación sigue tomando la misma fecha de pre radicación. Adicionalmente no permite cambiar contraseña, y el soporte técnico es deficiente.

### c. CONFIDENCIALIDAD DE LA INFORMACIÓN

| SECTORIAL | RESERVADA | CLASIFICADA | PUBLICA | NO CLASIFICADA |
|---|---|---|---|---|
| DESPACHO | 11 | 15 | 6 | 2 |
| OFICINA ASESORA DE PLANEACION | | | 8 | |
| SECRETARIA DE AGRICULTURA | | | 3 | 1 |
| SECRETARIA DE AMBIENTE | 2 | | 2 | |
| SECRETARIA DE DEPORTES | | | 4 | |
| SECRETARIA DE EDUCACIÓN | 7 | 16 | 11 | 3 |
| SECRETARIA DE GOBIERNO | 12 | 9 | 4 | 3 |
| SECRETARIA DE HACIENDA | 14 | 8 | 24 | 3 |
| SECRETARIA DE INFRAESTRUCTURA | | | 3 | |
| SECRETARIA DE MINAS | | 2 | 1 | |
| SECRETARIA DE SALUD | 34 | 92 | 30 | 13 |
| SECRETARIA GENERAL | 5 | 5 | 3 | 1 |
| **PORCENTAJES** | **23,81%** | **41,18%** | **27,73%** | **7,28%** |
| **TOTALES** | **85** | **147** | **99** | **26** |

Respecto a la confidencialidad de la información el 41.18% de los activos de información de la entidad se ubicaron en la categoría clasificada, es decir información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. Dentro de esta categoría se incluyen sistemas de información, expedientes físicos, activos de información relacionados con recurso humano, Bases de datos administradas desde Excel y archivos planos, en mayor proporción en la secretaría de salud seguida de la secretaría de educación.

Así mismo la información reservada se ubicó en un 23.81%, es decir información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de

pérdida de imagen o económica en mayor proporción en la secretaría de salud seguido de la secretaría de hacienda.

## 6. ANALISIS DE RIESGOS

### EVALUACIÓN DE RIESGOS

Esta última etapa es la valoración del riesgo y se realiza de manera tal que permita establecer la probabilidad de su ocurrencia y el impacto sobre la operación de la Gobernación del Departamento del Cesar.

Para facilitar la calificación y evaluación a los riesgos, a continuación, se presenta una matriz que contempla un análisis cualitativo, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad).

| Probabilidad | | | | | |
|---|---|---|---|---|---|
| Casi seguro (5) | | | | | |
| Frecuente (4) | | | | | |
| Ocasional (3) | | | | | |
| Raro (2) | | | | | |
| Remota (1) | | | | | |
| | Insignificante (1) | Menor (2) | Moderado (3) | Alto (4) | Catastrófico (5) |
| Impacto | | | | | |

### Criterios para la evaluación del riesgo

Las categorías relacionadas con el Impacto son: insignificante, menor, moderado, alto y catastrófico. Las categorías relacionadas con la Probabilidad son: remota, raro, ocasional, frecuente, casi seguro.

**TRATAMIENTO DE RIESGOS**

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros. El tratamiento de riesgos implica tomar decisiones basadas en los resultados de la identificación de riesgos y su análisis.

La política de gestión de riesgos está determinada por las siguientes opciones de tratamiento:

| Zonas o niveles de criticidad e intervención del riesgo | | Tratamiento |
|---|---|---|
| Zona de Riesgo Bajo | Dada su baja probabilidad de presentación, es posible asumir el riesgo, pero deben planearse acciones para reducirlo en caso que se presente. | Asumir el riesgo |
| Zona de Riesgo Moderada | Evaluada la probabilidad e impacto es posible asumir el riesgo, pero siempre acompañado de acciones para reducirlo y evitarlo en lo posible. | Asumir el riesgo, Reducir el riesgo |
| Zona de Riesgo Alta | En esta zona de riesgo alta debe siempre evitar, reducir, compartir o transferir el riesgo. | Reducir el riesgo, evitar, compartir o transferir |
| Zona de Riesgo Extrema | En esta zona de riesgo extrema debe siempre y de manera simultánea: evitarse el riesgo, reducirlo y compartir o transferir el riesgo. Los puntos de control deben ser más estrictos | Reducir el riesgo, evitar, compartir o transferir |

La gestión del riesgo está alineada con el modelo de mejoramiento institucional y es una de las fuentes de mejora. Para el tratamiento de los riesgos se implementan planes de mejoramiento, especialmente en los casos que se identifican nuevos riesgos, cuando es necesario rediseñar los controles existentes o definir unos nuevos controles.

A continuación se presenta el mapa de riesgos de la Gobernación del Departamento del Cesar, el cual fue diseñado después de realizar las visitas en cada una de las sectoriales y oficinas de la entidad, esta fase se le conoce como Diagnostico de los riesgos encontrados:



## *IDENTIFICACIÓN DE LOS RIESGOS Y LAS AMENAZAS EXISTENTES EN LA GOBERNACIÓN DEL DEPARTAMENTO DEL CESAR*

| Nombre del Riesgo | Descripción del Riesgo | Tipo de Amenaza | Amenaza | Origen | Fuente de la Amenaza Humana (Motivación) | Motivación | Fuente de la Amenaza (Acciones Amenazantes) | Acciones Amenazantes |
|---|---|---|---|---|---|---|---|---|
| Software fuera de servicio | Atraso en el envío y recibido de la información de interés para la oficina | Pérdida_de_los_servicios_esenciales | Falla en equipo de telecomunicaciones | Ambientales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Inteligencia |
| Hurto o pérdida de expedientes | Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la información. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Venganza | Intrusos_ | Venganza |
| Sistema de información fuera de servicio | Falla en la red | Fallas técnicas | Mal funcionamiento del software | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| Manipulación de la información | Reportar información errada | Compromiso_de_la_información | Datos provenientes de fuentes no confiables | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| Pérdida/hurto de expediente o documentos | Dada la importancia de la información que reposa en los expedientes y su carácter confidencial no se encuentra | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Ego | Intrusos_ | Inteligencia |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | n adecuadamente protegidos. | | | | | | | |
| Extracción ilegal de información del computador | Pese a que el equipo cuenta con una clave de administrador y un código de seguridad asignado por el alto comisionado para la paz existe un riesgo de hakeo del equipo. | Acciones_no_autorizadas | Corrupción de datos | Deliberadas | Intrusos | Inteligencia | Intrusos_ | Inteligencia |
| Fraude | Cuando la conducta no cumple intencionalmente las normas de la entidad, y se caracteriza por desviaciones de material o valores, la divulgación de mentiras, información confidencial etc. Que el funcionario se desvincule de la entidad y no transfiera el conocimiento de buenas prácticas sobre las funciones desempeñadas. | Compromiso_de_la_información | Divulgación | Deliberadas | Intrusos | Ganancia Monetaria | Espionaje industrial_ | Ventaja de Defensa |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Hurto o destrucción de la información | Sólo reposa una sola copia de la información en físico. En caso de hurto o destrucción no existe copia de respaldo. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Ego | Intrusos_ | Inteligencia |
| Fraude | Cuando la conducta no cumple intencionalmente las normas de la entidad, y se caracteriza por desviaciones de material o valores, la divulgación de mentiras, información confidencial etc. Que el funcionario se desvincule de la entidad y no transfiera el conocimiento de buenas prácticas sobre las funciones desempeñadas. | Compromiso_de_la_información | Divulgación | Deliberadas | Intrusos | Ganancia Monetaria | Espionaje industrial_ | Ventaja de Defensa |
| Sistema de información fuera de servicio | Falla en la red | Fallas técnicas | Mal funcionamiento del software | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| Acceso no autorizado al Correo electrónico | No finalizar la sesión del correo electrónico | Acciones_no_autorizadas | Uso no autorizado del equipo | Accidentales | Intrusos | Curiosidad | Intrusos_ | Curiosidad |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Acceso no autorizado a las plataformas | No finalizar la sesión al culminar el reporte de información | Acciones_no_autorizadas | Corrupción de datos | Accidentales | Intrusos | Curiosidad | Intrusos_ | Curiosidad |
| Fraude | Cuando la conducta no cumple intencionalmente las normas de la entidad, y se caracteriza por desviaciones de material o valores, la divulgación de mentiras, información confidencial etc. | Compromiso_de_la_información | Divulgación | Deliberadas | Intrusos | Ganancia Monetaria | Espionaje industrial_ | Ventaja de Defensa |
| Acceso no autorizado al Correo electrónico | No finalizar la sesión del correo electrónico | Acciones_no_autorizadas | Uso no autorizado del equipo | Accidentales | Intrusos | Curiosidad | Intrusos_ | Curiosidad |
| Pérdida/hurto de expediente o documentos | Dada la importancia de la información que reposa en los expedientes y su carácter confidencial no se encuentran adecuadamente protegidos. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Ego | Intrusos_ | Inteligencia |
| Acceso no autorizado al Correo electrónico | No finalizar la sesión del correo electrónico | Acciones_no_autorizadas | Uso no autorizado del equipo | Accidentales | Intrusos | Curiosidad | Intrusos_ | Curiosidad |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Acceso no autorizado al Software | Cuando la funcionaria se ausenta no existe un control por inactividad dentro del aplicativo constituyendo una gran amenaza de extracción no autorizada de información | Acciones_no_autorizadas | Uso no autorizado del equipo | Deliberadas | Intrusos | Ego | Intrusos_ | Curiosidad |
| Hurto o destrucción de la información | Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la información. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Venganza | Intrusos_ | Venganza |
| Daño del computador | Destrucción del disco duro por polvo, corrosión, fuego entre otros | Fallas técnicas | Mal funcionamiento del equipo | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Ego |
| Fallas en servidor | Las fallas en servidor pueden ocasionar retraso en el pago a los contratistas | Fallas técnicas | Mal funcionamiento del software | Accidentales | Intrusos | Ganancia Monetaria | Intrusos_ | Venganza |
| Daño del computador | Destrucción del disco duro por polvo, corrosión, fuego entre otros | Fallas técnicas | Mal funcionamiento del equipo | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Ego |
| Hurto o destrucción de la información | Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Venganza | Intrusos_ | Venganza |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | información. | | | | | | | |
| Fraude | Cuando la conducta no cumple intencionalmente las normas de la entidad, y se caracteriza por desviaciones de material o valores, la divulgación de mentiras, información confidencial etc. | Compromiso_de_la_información | Divulgación | Deliberadas | Intrusos | Ganancia Monetaria | Espionaje industrial_ | Ventaja de Defensa |
| Fallas en servidor | Las fallas en servidor pueden ocasionar retraso en el pago a los contratistas | Fallas técnicas | Mal funcionamiento del software | Accidentales | Intrusos | Ganancia Monetaria | Intrusos_ | Venganza |
| Fraude | Cuando la conducta no cumple intencionalmente las normas de la entidad, y se caracteriza por desviaciones de material o valores, la divulgación de mentiras, información confidencial etc. | Compromiso_de_la_información | Divulgación | Deliberadas | Intrusos | Ganancia Monetaria | Espionaje industrial_ | Ventaja de Defensa |
| Daño del computador | Destrucción del disco duro por polvo, corrosión, fuego entre otros | Fallas técnicas | Mal funcionamiento del equipo | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Ego |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Uso no autorizado al sistema de información | Cuando la funcionaria se ausenta el sistema tiene cierre de sesión automático después de cierto tiempo por inactividad no obstante existe el riesgo que otro funcionario pueda tener la clave de acceso | Acciones_no_autorizadas | Uso no autorizado del equipo | Deliberadas | Intrusos | Ego | Intrusos_ | Curiosidad |
| Pérdida o destrucción de la información | Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la información. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Venganza | Intrusos_ | Venganza |
| Daño del computador | Destrucción del disco duro por polvo, corrosión, fuego entre otros | Fallas técnicas | Mal funcionamiento del equipo | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Ego |
| Daño del computador | Destrucción del disco duro por polvo, corrosión, fuego entre otros | Fallas técnicas | Mal funcionamiento del equipo | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Ego |
| Hurto o destrucción de la información | Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la información. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Venganza | Intrusos_ | Venganza |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Acceso no autorizado al sistema de información | Cuando la funcionaria se ausenta el sistema tiene cierre de sesión automático después de cierto tiempo por inactividad no obstante existe el riesgo que otro funcionario pueda tener la clave de acceso | Acciones_no_autorizadas | Uso no autorizado del equipo | Deliberadas | Intrusos | Ego | Intrusos_ | Curiosidad |
| Hurto o destrucción de la información | Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la información. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Venganza | Intrusos_ | Venganza |
| Fallas en servidor | Las fallas en servidor pueden ocasionar retraso en el pago a los contratistas | Fallas técnicas | Mal funcionamiento del software | Accidentales | Intrusos | Ganancia Monetaria | Intrusos_ | Venganza |
| Daño del computador | Destrucción del disco duro por polvo, corrosión, fuego entre otros | Fallas técnicas | Mal funcionamiento del equipo | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Ego |
| Pérdida o destrucción de la información | Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la información. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Venganza | Intrusos_ | Venganza |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Acceso no autorizado al sistema de información | Cuando la funcionaria se ausenta el sistema tiene cierre de sesión automático después de cierto tiempo por inactividad no obstante existe el riesgo que otro funcionario pueda tener la clave de acceso | Acciones_no_autorizadas | Uso no autorizado del equipo | Deliberadas | Intrusos | Ego | Intrusos_ | Curiosidad |
| Daño del computador | Destrucción del disco duro por polvo, corrosión, fuego entre otros | Fallas técnicas | Mal funcionamiento del equipo | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Ego |
| Fraude | Cuando la conducta no cumple intencionalmente las normas de la entidad, y se caracteriza por desviaciones de material o valores, la divulgación de mentiras, información confidencial etc. | Compromiso_de_la_información | Divulgación | Deliberadas | Intrusos | Ganancia Monetaria | Espionaje industrial_ | Ventaja de Defensa |
| Hurto o destrucción de la información | Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la información. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Venganza | Intrusos_ | Venganza |
| Pérdida de Conocimiento | Falta de existencia de una segunda | Compromiso_de_las_funciones | Error en uso | Accidentales | Intrusos | Errores y omisiones no | Intrusos_ | Errores y emociones no |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | persona con ese conocimiento | | | | | intencionales | | intencionales |
| DETERIORO | PERDIDA DE SUS CARACTERISTICAS PARA EL OBJETIVO DE SU MISION | Eventos naturales | Fenómenos climáticos | Ambientales | Terrorismo | Destrucción | Terrorismo_ | Bomba/terrorismo |
| ataque informático | se han recibido ataques de virus | Dano_Físico | Destrucción del equipo o medios | Accidentales | Pirata_informático_intruso_ilegal | Ganancia monetaria | Pirata_informático_intruso_ilegal_ | Intrusión en el sistema |
| manipulación de la información | que los datos sean alterados | Acciones_no_autorizadas | Destrucción del equipo o medios | Deliberadas | Intrusos | Destrucción de la información | Intrusos_ | Intrusión en el sistema |
| error de manejo por actualización, error humano | es vulnerable a la manipulación de terceros | Acciones_no_autorizadas | Polvo, corrosión, congelamiento | Accidentales | Intrusos | Destrucción de la información | Intrusos_ | Intrusión en el sistema |
| fallas que se presentan en el servidor | el riesgo se traslada a sistema ya que depende del servidor central | Fallas técnicas | Destrucción del equipo o medios | Accidentales | Intrusos | Destrucción de la información | Criminal_de_la_computación_ | Soborno de la información |
| atraso en la operación | el riesgo se puede presentar en los servidores de la oficina de sistemas, y como los pagos se realizan en un solo computador se puede presentar atrasos en los procesos | Dano_Físico | Destrucción del equipo o medios | Accidentales | Intrusos | Destrucción de la información | Intrusos_ | Intrusión en el sistema |
| atraso en las operaciones | daño del equipo y que sistemas no tenga copia de la información | Fallas técnicas | Destrucción del equipo o medios | Accidentales | Pirata_informático_intruso_ilegal | Ganancia monetaria | Criminal_de_la_computación_ | Intrusión en el sistema |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| no brindar oportunamente la información y la armonización de la parte de presupuesto y contabilidad | daño del equipo y que sistemas no tenga copia de la información | Fallas técnicas | Destrucción del equipo o medios | Accidentales | Pirata_informático_intruso_ilegal | Destrucción de la información | Criminal_de_la_computación_ | |
| intruso de la información | que intrusos tengan acceso a la información y manipulen la misma | Acciones_no_autorizadas | Destrucción del equipo o medios | Accidentales | Intrusos | Ganancia monetaria | Intrusos_ | Soborno de la información |
| perdida de la información relevante para continuar con el proceso de las cesiones de crédito | la información es guardada en el pc y por las diversas fallas eléctricas queda el equipo vulnerable a cualquier daño | Fallas técnicas | Destrucción del equipo o medios | Accidentales | Intrusos | Destrucción de la información | Intrusos_ | Intrusión en el sistema |
| que intrusos tengan acceso a la información y manipulen la misma | todos están en capacidad de realizar los egresos y lo pueden hacer desde cualquier equipo | Acciones_no_autorizadas | Destrucción del equipo o medios | Accidentales | Intrusos | Alteración no autorizada de los datos | Intrusos_ | Intrusión en el sistema |
| Manejo manual de archivos plano de pagos de los impuestos de vehículo, registro etc. | Falta de un web service entre el banco y el proveedor del software para que los pagos estén en línea. Falta de plataforma tecnológica. | Acciones_no_autorizadas | Accidente Importante | la amenaza es con el software | Intrusos | Ganancia monetaria | Intrusos_ | Acto fraudulento |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Manejo manual de archivos plano de pagos de los impuestos de vehículo, registro etc. | perdida de la información tanto física como sistemática | Dano_Físico | Destrucción del equipo o medios | Accidentales | Intrusos | Destrucción de la información | Intrusos_ | Acto fraudulento |
| manipulación de terceros en la información | por ser un software externo no hay control de la información y esta puede ser manipulada | Acciones_no_autorizadas | Destrucción del equipo o medios | Accidentales | Pirata_informático_intruso_ilegal | Ganancia monetaria | Pirata_informático_intruso_ilegal_ | Acto fraudulento |
| perdida de la información relevante para continuar con el proceso de sanciones a deudores morosos | falta de software para realizar los procesos de manera más eficiente y seguro | Dano_Físico | Agua | Accidentales | Intrusos | Destrucción de la información | Intrusos_ | Intrusión en el sistema |
| los riesgos se trasladan a la empresa contratante | no se registran riesgos | Dano_Físico | Destrucción del equipo o medios | Accidentales | Pirata_informático_intruso_ilegal | Destrucción de la información | Intrusos_ | sin acciones amenazantes |
| destrucción o perdida de la información | perdida de la información por no tener un espacio físico idóneo y por qué se maneja en físico es muy factible que esta información sufra algún tipo de destrucción | Dano_Físico | Destrucción del equipo o medios | Accidentales | Pirata_informático_intruso_ilegal | Destrucción de la información | Criminal_de_la_computación_ | Intrusión en el sistema |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| perdida de la información/desconocimiento de normas | otorgar conceptos erróneos favoreciendo a entidades deportivas para su reconocimiento deportivos, posibilidades de avería en los equipos no se hacen copias de seguridad / error humano | Acciones_no_autorizadas | Destrucción del equipo o medios | Accidentales | Intrusos | Alteración no autorizada de los datos | Intrusos_ | sobornos |
| Daño físico de expedientes por causas climáticas y libre exposición de los documentos. Daños físicos a los equipos de cómputo perdiendo la información almacenada | No hay un espacio idóneo para la conservación documental física, está expuesta al agua, polvo y al manipuleo humano, no un personal capacitado para. Administrar los archivos generados en esta oficina. Equipos de cómputos deficientes que no cuentan con protección eléctrica lo que pone en riesgo la información por daños ya sea por equipos muy viejos o por cambios eléctricos drásticos. | Dano_Físico | Destrucción del equipo o medios | Accidentales | Intrusos | Destrucción de la información | Intrusos_ | espacio físico |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | los expedientes no se están escaneando por falta de un equipo solo se están conservando de manera física | | | | | | | |
| perdida de la información por cancelación de programa utilizado sin licencias | no se cuenta con un proveedor legalizado del software y en cualquier momento puede cancelar su operatividad y funcionamiento causando un gran daño a la información que contenga el software | Fallas técnicas | Destrucción del equipo o medios | Accidentales | Pirata_informático_intruso_ilegal | Ganancia monetaria | Intrusos_ | cancelación de licencias de software |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| perdida de la información, fallas en el sistema operativo | esta información puede ser afectada por las fallas presentadas en el software, esto hace que se pueda perder y además el sistema falla y así no se generan archivos e informes donde está la opción para solicitarlos | Fallas técnicas | Destrucción del equipo o medios | Ambientales | Pirata_informático_intruso_ilegal | Ganancia monetaria | Pirata_informático_intruso_ilegal_ | Intrusión en el sistema |
| perdida de la información por daños en el hardware | esta información no puede ser afectada por intrusos ya que no se encuentra en software ni en línea | Dano_Físico | Destrucción del equipo o medios | Accidentales | Pirata_informático_intruso_ilegal | Ganancia monetaria | Criminal_de_la_computación_ | Intrusión en el sistema |
| alteración de los datos | la base de datos puede ser manipulada | Fallas técnicas | Destrucción del equipo o medios | Accidentales | Pirata_informático_intruso_ilegal | Ganancia monetaria | Criminal_de_la_computación_ | Intrusión en el sistema |
| perdida de la información por fallas técnicas | se han presentado perdida de la información por fallas y a esta información no se le hacía copias de seguridad | Fallas técnicas | Destrucción del equipo o medios | Accidentales | Espionaje industrial | Ganancia monetaria | Criminal_de_la_computación_ | Intrusión en el sistema |
| perdida de la información por fallas técnicas | se han presentado virus que han afectado la operatividad de los procesos pero la información no se | Dano_Físico | Destrucción del equipo o medios | Ambientales | Pirata_informático_intruso_ilegal | Ganancia monetaria | Criminal_de_la_computación_ | Intrusión en el sistema |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | ha perdido | | | | | | | |
| seguridad de la información contenida en el software | no se dispone de una infraestructura de servidores adecuada e institucionalizada para el alojamiento del software | Fallas técnicas | Destrucción del equipo o medios | Accidentales | | Alteración no autorizada de los datos | | Intrusión en el sistema |
| perdida del archivo | se puede perder porque el expediente se archiva en lugares donde no se debe | Dano_Físico | Agua | Ambientales | | Destrucción de la información | | |
| Hurto o destrucción de la información | Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la información. | Compromiso_de_la_información | Hurto de medios o documentos | Deliberadas | Intrusos | Venganza | Intrusos_ | Venganza |
| Acceso no autorizado al Correo electrónico | No finalizar la sesión del correo electrónico | Acciones_no_autorizadas | Uso no autorizado del equipo | Accidentales | Intrusos | Curiosidad | Intrusos_ | Curiosidad |
| Acceso no autorizado al sistema de información | Cuando la funcionaria se ausenta el sistema tiene cierre de sesión automático después de cierto tiempo por inactividad no obstante existe el riesgo que otro | Acciones_no_autorizadas | Uso no autorizado del equipo | Deliberadas | Intrusos | Ego | Intrusos_ | Curiosidad |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | funcionario pueda tener la clave de acceso | | | | | | | |
| Sistema de información fuera de servicio | Falla en la red | Fallas técnicas | Mal funcionamiento del software | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| Software fuera de servicio | Atraso en el envío y recibido de la información de interés para la oficina | Pérdida_de_los_servicios_esenciales | Falla en equipo de telecomunicaciones | Ambientales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Inteligencia |
| Colapso del sistema de información (Pérdida de información) | Sistema de información con múltiples fallas en su operación | Pérdida_de_los_servicios_esenciales | Saturación en el sistema de información | Deliberadas | Pirata_informático_intruso_ilegal | Ego | Intrusos_ | Curiosidad |
| Sistema de información fuera de servicio | Falla en la red | Pérdida_de_los_servicios_esenciales | Mal funcionamiento del software | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| Alteración de la información malintencionada o accidental | Al alimentar el instrumento se altere accidentalmente la información de otras filas | Acciones_no_autorizadas | Corrupción de datos | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Venganza |
| Acceso no autorizado al Correo electrónico | No finalizar la sesión del correo electrónico | Acciones_no_autorizadas | Uso no autorizado del equipo | Accidentales | Intrusos | Curiosidad | Intrusos_ | Curiosidad |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| bloqueo del sistema | el software en línea tuvo un percance en la disposición de la información, ya que la información que estaba en un servidor y al tratar de migrarla a otro no se podía tener acceso a esta alrededor de 15 días | Fallas técnicas | Destrucción del equipo o medios | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| daños al computador | se ha presentado virus en los procesos pero la información fue recuperada | Fallas técnicas | Agua | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| posible virus | el riesgo está establecido para el hardware ya que pueden afectarse por virus y por bajones de luz | Fallas técnicas | Destrucción del equipo o medios | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| perdida de la información física | las actas de notificación, de glosas y devoluciones, se encuentran almacenadas en medio físico, permanecen a la vista volviéndose muy vulnerables a la manipulación, extravío y daños por causas ambientales, las actas de conciliación y depuración de cartera se encuentran en medio físico y medio magnético teniendo en cuenta que corren riesgos de pérdidas de igual manera por causas externas ambientales | Fallas técnicas | Destrucción del equipo o medios | | intrusos | | | no cuenta con equipos idóneos para digitalizar la información y salguardarla de una manera más segura |
| perdida de la información tanto física como sistemática | esta información solo se almacenan en medio físico y el riesgo de avería, perdida o daños es latente por su mal ambiente de conservación | Fallas técnicas | Destrucción del equipo o medios | | intrusos | | | no cuenta con equipos idóneos para digitalizar la información y salguardarla de una manera más segura |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| perdida de la información tanto física como digital | la información física está muy vulnerable puesto que no se tienen controles para su almacenamiento, no se escanean, y están expuestas de manera abierta a la manipulación de terceros o al ambiente como humedad, polvo roedores y la información informática también se encuentra expuesta por que está en un computador, no se hacen copias de seguridad, tampoco se almacenan en la nube o correo electrónico | Fallas técnicas | Destrucción del equipo o medios | Accidentales | causas externas y manipulación humana | involuntario | causas ajenas al uso | involuntario |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| fallas en la red y conexión en internet | En este punto de vista la entidad no asume ningún riesgo en cuanto a la información procesada, pero por acceder a la plataforma por medio del internet podemos presentar fallas en el evento de que este servicio no sea el idóneo o se preste de manera deficiente perturbando el eficiente servicio | Fallas técnicas | fallas en la conectividad | Accidentales | fallas en cableado a capacidad de conexión a internet | negligencia administrativa | mala administración | mal servicio de la conexión |
| Daño del Software | Pérdida de la información por daño interno de dispositivo (SOFTWARE). | Fallas técnicas | Mal funcionamiento del software | Accidentales | Criminal_de_la_computación | Destrucción de la información | Criminal_de_la_computación_ | Crimen por computador |
| Pérdida de la información | Pérdida de la información por daño interno de dispositivo (disco duro). | Fallas técnicas | Manipulación con software | Deliberadas | Pirata_informático_intruso_ilegal | Rebelión | Pirata_informático_intruso_ilegal_ | Intrusión, accesos forzados al sistema |
| Sustracción del documento | Pérdida de la información por daño interno de dispositivo (disco duro) debido a la humedad en la ubicación | Fallas técnicas | Agua | Ambientales | Pirata_informático_intruso_ilegal | Dinero | Pirata_informático_intruso_ilegal_ | Suplantación de identidad |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | del activo | | | | | | | |
| Sustracción del documento | Pérdida de la información por daño interno de dispositivo (disco duro) debido a la humedad en la ubicación del activo | Acciones_no_autorizadas | Hurto de medios o documentos | Deliberada | Pirata_informático_intruso_ilegal | Dinero | Pirata_informático_intruso_ilegal_ | Soborno de la información |
| Daño del Software | Pérdida de la información por daño interno de dispositivo (SOFTWARE). | Pérdida_de_los_servicios_esenciales | Mal funcionamiento del software | Accidentales | Criminal_de_la_computación | Destrucción de la información | Criminal_de_la_computación_ | Crimen por computador |
| Daño el equipo donde se encuentra instalado el software | Daño del equipo | Fallas técnicas | Mal funcionamiento del software | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| Perdida de los informes | Perdida de los informes o deterioro por agentes ambientales. | Acciones_no_autorizadas | Hurto de medios o documentos | Deliberadas | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| Perdida de las actas | Perdida de las actas o deterioro por agentes ambientales. | Fallas técnicas | Accidente Importante | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |
| Pérdida de la información | Pérdida de la información por daño interno de dispositivo (disco duro) o por hito del equipo. | Fallas técnicas | Fallas del equipo | Accidentales | Intrusos | Errores y omisiones no intencionales | Intrusos_ | Errores y emociones no intencionales |

**a. AMENAZAS**

| SECTORIAL | EVENTOS NATURALES | PÉRDIDA DE LOSE SEVICIOS ESENCIALES | COMPROMISO DE LA INFORMACIÓN | FALLAS TÉCNICAS | ACCIONES NO AUTORIZADAS | DAÑO FISICO | COMPRIMISO DE LAS FUNCIONES |
|---|---|---|---|---|---|---|---|
| DESPACHO | | 2 | 6 | 9 | 4 | 11 | 2 |
| OFICINA ASESORA DE PLANEACION | | | | 3 | 1 | 4 | |
| SECRETARIA DE AGRICULTURA | | 1 | 1 | 1 | | 1 | |
| SECRETARIA DE AMBIENTE | | | | 2 | | 2 | |
| SECRETARIA DE DEPORTES | | | | | 1 | 3 | |
| SECRETARIA DE EDUCACIÓN | 5 | 4 | | 10 | 9 | 8 | 1 |
| SECRETARIA DE GOBIERNO | | 1 | 13 | 4 | 5 | 4 | 1 |
| SECRETARIA DE HACIENDA | | 2 | 6 | 21 | 9 | 11 | |
| SECRETARIA DE INFRAESTRUCTURA | | | | | 2 | | 1 |
| SECRETARIA DE MINAS | | | | 2 | | 1 | |
| SECRETARIA DE SALUD | 9 | 12 | 34 | 58 | 13 | 28 | 15 |
| SECRETARIA GENERAL | 3 | | 2 | 4 | 1 | 3 | 1 |
| **PORCENTAJES** | **4,76%** | **6,16%** | **17,37%** | **31,93 %** | **12,61%** | **21,29%** | **5,88%** |
| **TOTALES** | **17** | **22** | **62** | **114** | **45** | **76** | **21** |

En cuanto a las amenazas un 31.93% de los activos de información se ubicaron en la categoría fallas técnicas que están asociadas con mal funcionamiento de los equipos de cómputo, incluido el servidor de la secretaría de salud, saturación en el sistema de información y pérdida de su información en su gran mayoría. Estas fallas técnicas se presentan en mayor proporción en la secretaría de salud seguidamente en la secretaría de hacienda.

**b. TIPO DE RIESGOS**

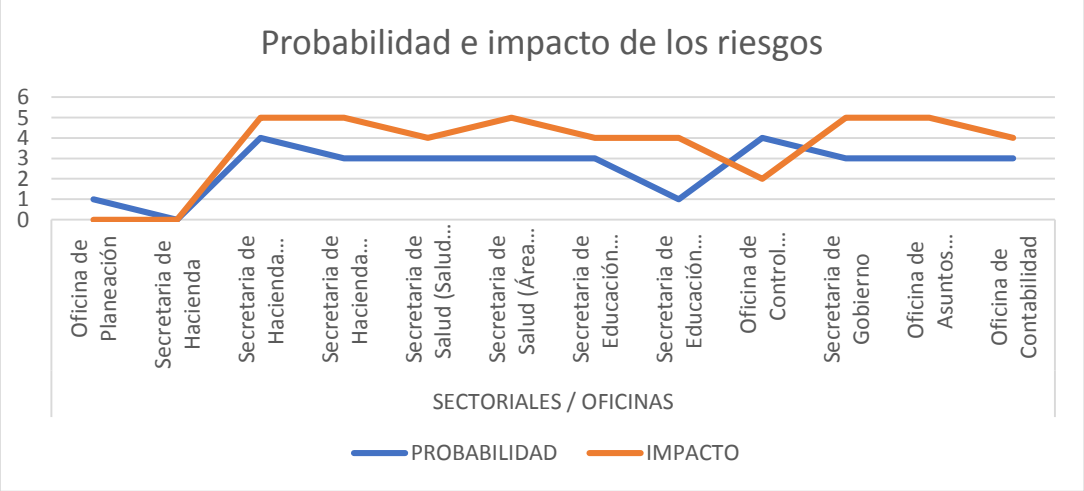
| SECTORIAL | IMAGEN | TECNOLOGICO | OPERATIVO | CUMPLIMIENTO | ESTRATEGICO | FINANCIERO | VARIOS |
|---|---|---|---|---|---|---|---|
| DESPACHO | 5 | 4 | 8 | 7 | | | 10 |
| OFICINA ASESORA DE PLANEACION | | | 4 | | | | 4 |
| SECRETARIA DE AGRICULTURA | | | 3 | | | | 1 |
| SECRETARIA DE AMBIENTE | | 2 | | 2 | | | |
| SECRETARIA DE DEPORTES | | | 4 | | | | |
| SECRETARIA DE EDUCACIÓN | | | 19 | 1 | | 2 | 15 |
| SECRETARIA DE GOBIERNO | 3 | 1 | 3 | 4 | | | 17 |
| SECRETARIA DE HACIENDA | 1 | | 15 | 1 | 1 | 4 | 27 |
| SECRETARIA DE INFRAESTRUCTURA | | | | | | | 3 |
| SECRETARIA DE MINAS | | | 1 | 2 | | | |
| SECRETARIA DE SALUD | 4 | 4 | 68 | 34 | | 1 | 58 |
| SECRETARIA GENERAL | 1 | 1 | 6 | | | | 6 |
| **PORCENTAJES** | **3,92 %** | **3,36%** | **36,69%** | **14,29%** | **0,28%** | **1,96%** | **39,50%** |
| **TOTALES** | **14** | **12** | **131** | **51** | **1** | **7** | **141** |

### c. CLASIFICACIÓN DEL RIESGO

| SECTORIAL | RIESGO EXTREMO | RIESGO ALTO | RIESGO MODERADO | RIESGO BAJO |
|---|---|---|---|---|
| DESPACHO | 10 | 7 | 15 | 2 |
| OFICINA ASESORA DE PLANEACION | | | 3 | 5 |
| SECRETARIA DE AGRICULTURA | 1 | 1 | 1 | 1 |
| SECRETARIA DE AMBIENTE | 1 | 3 | | |
| SECRETARIA DE DEPORTES | | | | |
| SECRETARIA DE EDUCACIÓN | | 15 | 14 | 8 |
| SECRETARIA DE GOBIERNO | 11 | 8 | 6 | 3 |
| SECRETARIA DE HACIENDA | 8 | 15 | 20 | 6 |
| SECRETARIA DE INFRAESTRUCTURA | 1 | 2 | | |
| SECRETARIA DE MINAS | | 3 | | |
| SECRETARIA DE SALUD | 58 | 48 | 45 | 17 |
| SECRETARIA GENERAL | 9 | 4 | | 1 |
| **PORCENTAJES** | **99** | **106** | **104** | **43** |
| **TOTALES** | **27,73%** | **29,69%** | **29,13%** | **12,04%** |

Dentro de los tipos de riesgos la mayor proporción después de la variable Varios se concentró en los operativos en la secretaría de salud que están asociados con pérdida de información, atraso en las operaciones, daños en computador y errores operativos de los sistemas de información.

### ANÁLISIS DEL IMPACTO Y PROBABILIDAD DE RIESGO



Una vez identificados los riesgos, se debe hacer un análisis de estos, deben separarse los menores o aceptables, de los más riesgosos y por supuesto dar información para que ayude en la evaluación y tratamiento de estos. La función principal del análisis de riesgo es la de identificar las posibles fuentes de riesgos, sus consecuencias y la probabilidad de que estos ocurran. El riesgo, es analizado y se le da un valor en escala según las políticas de la Gobernación del Departamento del Cesar.

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, este último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. El análisis del riesgo depende de la información obtenida en la fase de identificación de riesgos.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados:

**Probabilidad e Impacto.**

**Por Probabilidad**

Se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

**Por Consecuencia o Impacto**

Se entienden las derivaciones que puede ocasionar a la organización la materialización del riesgo. Estas a su vez modificaran el alcance de objetivos y el nivel en que lo hagan será proporcional a su impacto.

**IDENTIFICACIÓN Y CLASIFICACIÓN DEL NIVEL DE RIESGO**

**MEDICIÓN DE LA PROBABILIDAD DE RIESGO**

1) Remoto: representa una probabilidad muy baja en la ocurrencia de un fenómeno.

2) Inusual: representa una “Probabilidad Baja de la ocurrencia de un fenómeno”

3) Posible: representa una “probabilidad media en la aparición de un fenómeno” lo que significa que el porcentaje de aparición es de 50%, las decisiones relacionadas con este nivel de riesgo deben ser consensuadas para evitar daños importantes bajo la visión de que existe el mismo “chance” de ocurrencia de que el fenómeno ocurra como de que no.

4) Probable: representa una probabilidad “alta de ocurrencia de un fenómeno”, la toma de decisiones debe estar orientada a la prevención de consecuentes y estrategias de estabilización de la situación ante una crisis, la posición hacia la toma de decisiones debe manifestar de patente la idea de que el fenómeno #va a ocurrir” y el que no ocurra es un escenario más “improbable” del que sí.

5) Probabilidad “Muy Alta de Ocurrencia”, la toma de decisiones está colocada en la estrategia de restauración del daño y máximos niveles de control que eviten la presencia del fenómeno, ambas presentadas en ese orden.

## MEDICIÓN DEL IMPACTO DE RIESGO

Se evalúa en función de la magnitud de los efectos identificados y registrados sobre el programa de trabajo o proyecto.

El impacto que los riesgos identificados pueden tener consecuencias a corto mediano y largo plazo que derivaran en el incumplimiento de las metas institucionales. Para ello la medición del impacto es importante en particular para la toma de decisiones al respecto de las acciones a tomar en torno al riesgo, ya sea para su aceptación, declinación, atenuación o derivación.

## TABLA DE IMPACTO Y PROBABILIDAD

| Niveles para calificar el Impacto | Impacto (consecuencias) Cuantitativo | Impacto (consecuencias) Cualitativo |
|---|---|---|
| **Catastrófico** | Impacto que afecte la ejecución presupuestal mayor o igual al 50% | Interrupción de las operaciones de la Entidad por más de cinco (5) días |
| | | Intervención por parte de un ente de control u otro ente regulador. |
| | Pérdida de cobertura en la prestación de los servicios de la entidad mayor o igual al 50% | Pérdida de Información crítica para la entidad que no se puede recuperar |
| | Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual 50% | Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. |
| | Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan el presupuesto general de la entidad con un valor mayor o igual al 50% | Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados. |
| **Mayor** | Impacto que afecte la ejecución presupuestal mayor o igual al 20% | Interrupción de las operaciones de la Entidad por más de dos (2) días |
| | | Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta |
| | Pérdida de cobertura en la prestación de los servicios de la entidad mayor o igual al 20% | Sanción por parte ente de control u otro ente regulador. |
| | Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual 20% | Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. |
| | Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan el presupuesto general de la entidad con un valor mayor o igual al 20% | Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos. |

| | | |
|---|---|---|
| **Moderado** | Impacto que afecte la ejecución presupuestal mayor o igual al 5% | Interrupción de las operaciones de la Entidad por un (1) día. |
| | | Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. |
| | Pérdida de cobertura en la prestación de los servicios de la entidad mayor o igual al 10% | Inoportunidad en la información ocasionando retrasos en la atención a los usuarios |
| | | Reproceso de actividades y aumento de carga operativa |
| | Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual 5% | Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos |
| | Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan el presupuesto general de la entidad con un valor mayor o igual al 5% | Investigaciones penales, fiscales o disciplinarias |
| **Menor** | Impacto que afecte la ejecución presupuestal menor o igual al 1% | Interrupción de las operaciones de la Entidad por algunas horas |
| | Pérdida de cobertura en la prestación de los servicios de la entidad menor o igual al 5% | |
| | Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor o igual 1% | Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. |
| | Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan el presupuesto general de la entidad con un valor menor o igual al 1% | Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos |
| **Insignificante** | Impacto que afecte la ejecución presupuestal menor o igual al 0,5% | No hay interrupción de las operaciones de la entidad |
| | Pérdida de cobertura en la prestación de los servicios de la entidad menor o igual al 1% | |
| | Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor o igual 0,5% | No se generan sanciones económicas o administrativas |
| | Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan el presupuesto general de la entidad con un valor menor o igual al 0,5% | No se afecta la imagen institucional de forma significativa |

## RELACIONES CAUSALES DE LOS RIESGOS

## EVALUACIÓN MATRIZ Y MAPA DE RIESGO

La Evaluación de Riesgo permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

## VERIFICACIÓN DE CONTROLES

Antes de conocer los 5 pasos debemos recordar que un control efectivo o funcional, ofrece soluciones adecuadas para controlar los problemas.

1) Comprobar la existencia o no de controles para los factores de riesgo y, en su caso, para sus efectos; es necesario determinar la presencia o ausencia de mecanismos de control que monitoreen los factores de riesgo. Deben identificarse por lo menos 5 Controles.

2) Describir los controles existentes para administrar los factores de riesgo y, en su caso, para sus efectos;

Especificidad

## EXISTENCIA DE CONTROLES

3) Determinar el tipo de control: Para cada uno de los controles que se tengan implementados para administrar riesgos identificados debe generarse un tipo de control específico, estos son:

**Tipo de Control**

Características

4) Identificar en los controles lo siguiente:

a. Deficiencia: cuando no reúna alguna de las siguientes condiciones: que esté documentado, autorizado, operando con evidencias de cumplimiento y es efectivo, y

b. Suficiencia: cuando esté documentado, autorizado, operando con evidencias de cumplimiento y es efectivo, y finalmente

**Parámetros de control**

5) Determinar si el riesgo está controlado suficientemente, cuando al menos todos sus factores cuentan con controles suficientes de acuerdo a los siguientes parámetros:

Los controles internos son la piedra angular de un sistema eficaz de administración de riesgos ya que el personal de cualquier órgano de control, representa la primera barrera contra las pérdidas operativas potenciales.

Un control interno, también conocido como control, simplemente, es un conjunto de instrucciones que la alta dirección establece para prevenir o eliminar el riesgo de las pérdidas causadas por errores humanos, mal funcionamiento tecnológico, negligencia de los empleados o fraude.

**EVALUACIÓN DE CONTROLES.**

• **QUE ESTE DOCUMENTADO:** Debe estar por escrito.

• **QUE ESTE FORMALIZADO:** Lo respalda comunicación oficial.

**• QUE SE APLICA CONSISTENTEMENTE:** De manera permanente sin interrupción.

• **QUE ES EFECTIVO:** Cuando se incide en el para disminuir la probabilidad de ocurrencia o nivel de impacto.

Los controles pueden ser:

a. Preventivo: El mecanismo específico que tiene el propósito de anticiparse a la posibilidad de que ocurran situaciones no deseadas e inesperadas que pudieran afectar el logro de los objetivos y metas.

b. Correctivo: El mecanismo específico que opera en la etapa final de un proceso, el cual permite identificar corregir o subsanar en algún grado, omisiones o desviaciones.

**Escala de Nivel de Riesgo**

Se evalúa en función de la frecuencia con la que un factor potencialmente de riesgo ocurre en un área, servicio o producto determinado, se califica dependiendo de su incidencia.

Se evalúa del Nivel 1 al 10 y se clasifica en un nivel cada 2 ponderaciones:

Para definir el nivel de riesgo es necesario tipificar de acuerdo a la siguiente escala el tipo de probabilidad de ocurrencia para que el evento ocurra al igual que el nivel de impacto que el riesgo tendría sobre el plan de trabajo o el desarrollo del proyecto. A esta valoración se le conoce como “INICIAL” y se realiza sin considerar los controles ya existentes para su monitoreo, que son una serie de instrumentos que se han elaborado para medir los avances y retrocesos de los objetivos de la organización.

Todas las escalas consideran una puntuación del 1 al 10 en donde diez es el número de puntuación mayor, es decir, esta calificación identificara un nivel de ocurrencia mayor y un impacto mayor también.

1) **Nivel Estratégico:**

Es aquel en el que la toma de decisiones se centra en el plan directivo, en el desarrollo de estrategias y el seguimiento de acuerdos interinstitucionales, sus objetivos son estratégicos para el desarrollo de proyectos.

2) **Nivel Directivo:**

Es aquel en el que las estrategias están enfocadas a la manutención de los recursos materiales y humanos que sostienen al proyecto a través de la directriz y la supervisión de lineamientos que aseguren el cumplimiento de metas.

3) **Nivel Operativo:**

Es aquel en el que el desarrollo de proyectos posee una importancia pragmática al estar enfocado a la supervisión de tareas y actividades que aseguren el cumplimiento de las metas y objetivos institucionales.

Consideraremos al Mapa de Riesgos como una representación gráfica de uno o más riesgos que permite vincular la probabilidad de ocurrencia y su impacto en forma clara y objetiva.

Los riesgos se ubicarán por cuadrantes en la Matriz de Administración de Riesgos Institucional y se graficarán en el Mapa de Riesgos, en función de la valoración final del impacto en el eje horizontal y la probabilidad de ocurrencia en el eje vertical.

**CUADRANTES**

• Cuadrante I. Riesgos de Atención Inmediata.- Son críticos por su alta probabilidad de ocurrencia y grado de impacto, se ubican en la escala de valor mayor a 5 y hasta 10 de ambos ejes;

• Cuadrante II. Riesgos de Atención Periódica.- Tienen alta probabilidad de ocurrencia ubicada en la escala de valor mayor a 5 y hasta 10 y bajo grado de impacto de 0 y hasta 5;

• Cuadrante III. Riesgos Controlados.- Son de baja probabilidad de ocurrencia y grado de impacto, se ubican en la escala de valor de 0 y hasta 5 de ambos ejes, y

• Cuadrante IV. Riesgos de Seguimiento.- Tienen baja probabilidad de ocurrencia con valor de 0 y hasta 5 y alto grado de impacto mayor a 5 y hasta 10.

Se puede analizar después de la identificación de los riesgos a los que están expuestos los activos de información en la gobernación del departamento del cesar que en las sectoriales y/o oficinas hay unos riesgos determinados acorde con el formato en que este contenida la información, identificando entre ellos estos riesgos como los que más se presentan o se materializan son:

- Perdida de la información
- Daños en el equipo

- Fallas técnicas del equipo
- Fallas en el sistema operativo
- Daños al hardware
- Virus informático
- Software fuera de servicio
- Pérdida/hurto de expediente o documentos
- Extracción ilegal de información del computador
- Fallas en servidor
- Hurto o destrucción de la información

Se evidencio que los controles que están implementados actualmente no son suficientes y que en realidad no están dentro de los parámetros que se requiere dada la importancia de la información que estos activos contienen.

Se hace necesario implementar un plan estratégico para conocer y comprobar que controles son efectivos, para así mejorar o cambiar los ya existentes y que la información se encuentre de verdad segura y libre de exposición a los riesgos antes mencionados.

Pero la mejora o cambio debe estar acompañado de un periodo de prueba, para verificar si esto es efectivo y que lo que se implementó aporte la seguridad necesaria que la clase de información requiera.

## *TABLA DE CONTROLES A IMPLEMENTAR*

| | |
|---|---|
| Controles de Gestión | Políticas claras aplicadas |
| | Seguimiento al plan estratégico y operativo |
| | Indicadores de gestión |
| | Tableros de control |
| | Seguimiento a cronograma |
| | Informes de gestión |
| Controles Operativos | Conciliaciones |
| | Consecutivos |
| | Verificación de firmas |
| | Listas de chequeo |
| | Registro controlado |
| | Segregación de funciones |
| | Niveles de autorización |
| | Custodia apropiada |
| | Procedimientos formales aplicados |
| | Pólizas |
| | Seguridad física |
| | Contingencias y respaldo |
| | Personal capacitado |
| | Aseguramiento y calidad |
| Controles Legales | Normas claras y aplicadas |
| | Control de términos |

## *IDENTIFICACION DE LOS RIESGOS QUE SE PUEDEN PRESENTAR EN LOS ACTIVOS DE INFORMACION, SUS CAUSAS, CONSECUENCIAS, Y CONTROLES A IMPLEMENTAR*

| ACTIVO | RIESGO | CAUSA | CONSECUENCIA | EVITAR | CONTROLES | TIPO DE CONTROL | ACCIONES |
|---|---|---|---|---|---|---|---|
| RECURSO HUMANO | Indisponibilidad del servicio | alteración o eliminación del proceso | perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos, afectación a toda la entidad | EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado. | Irregularidades encontradas en el proceso deben ser reportadas a control interno disciplinario o a quien corresponda antes de generar una sanción o amonestación. | Preventivo | Reporte a Control Interno |
| | | Robo de información sensible del proceso | | | Acceso a la información y a las funciones de los sistemas de las aplicaciones, se debe restringir su acceso. | Preventivo | Elaboración de reportes de acceso a los datos |
| | | demora en el envío de la información al usuario | | | Procedimientos establecidos y documentados para detectar o corregir las fallas en el proceso rápidamente | Correctivo | Reporte de fallas |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | perdida en la recolección de la información dentro del proceso | | | Desarrollo de campañas de concienciación en temas de seguridad de la información en los procesos | Preventivo | Reuniones, campañas, Talleres y foros |
| | falta de personal autorizado y capacitado para la realización de las actividades del proceso | el encargado del proceso no se encuentra disponible | fallas en los procesos de la seguridad de la información, pérdida o robo de la información de la entidad, daños a los bienes o propiedad del cliente | EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado. | Concientización del personal respecto a la seguridad de la información en procedimientos concernientes a cada proceso | Preventivo y Correctivo | Reuniones, campañas, Talleres y foros |
| | | ausencia de la transferencia de los conocimientos por falta de capacitación | | | Establecer con MECI un mecanismo de suplencia de personal de los encargados de los procesos | Preventivo | Capacitaciones |
| | | inadecuada manipulación de los instrumentos utilizados por parte del personal ajeno al área encargada | | | Capacitaciones, procedimientos establecidos para la manipulación de instrumentos utilizados en cada proceso y acompañamiento por parte del responsable del proceso. | Preventivo | Reuniones, campañas, Talleres y foros |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | no seguir el protocolo adecuado para el manejo de las herramientas utilizadas en el proceso | | | Capacitaciones, procedimientos establecido para la manipulación de equipos. | Preventivo | Reuniones, campañas, Talleres y foros |
| SERVICIOS | daños en los servicios tecnológicos y perdida de la información | eventos catastróficos: inundaciones, terremotos, incendios | interrupción completa de los servicios ofrecidos | REDUCIR EL RIESGO por medio de acciones de control correctivas y preventivas que permita evitar la ocurrencia del riesgo | Centro de datos alterno en donde se espera reconstituir y reanudar a la operación normal de los procesos vitales de la entidad | Preventivo | Elaborar el plan de continuidad de Negocio |
| | mal prestación del servicio, o servicio inexistente | ofrecer servicios que no cuentan con un diseño previo | pérdida de imagen ante los usuarios de la entidad, incumplimiento de las condiciones del servicio | EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado. | Procedimientos, Diseño y desarrollo productos y servicios nuevos". | Preventivo | Diseño y/o prototipo de servicios nuevos, de acuerdo con el procedimiento |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| DATOS / INFORMACION | afectación de la integridad de los datos | incumplimiento de las condiciones del servicio para el cliente | perdida de la información y posibles ataques a la integridad de los datos | EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado. | Aseguramiento y respaldo de los archivos de control de acceso a los usuarios | Preventivo | Realizar un monitoreo al Aseguramiento |
| | | perdida o corrupción de los datos sistematizados del proceso | | | Copias de seguridad, para tener respaldos y evitar daños, redundancia cíclica. | Preventivo | Copias de seguridad en servidores de alta afluencia de datos |
| | | insuficiencia en el aseguramiento de la base de datos | | | Crear procesos de mantenimiento mensual de las BD y depuración de índices. Monitoreo de posibles intrusiones indebidas a las BD | Preventivo | Monitoreo de Bases de Datos |
| | | niveles de seguridad de la información inadecuados | | | Fortalecimiento de la seguridad en perfiles, y acceso a aplicaciones | Preventivo | Documentar la seguridad en perfiles de los funcionarios |
| | afectación de la disponibilidad del respaldo de la información en los procesos | fallas en el software utilizado | afectación a la disponibilidad de acceso al servicio o recurso del proceso | EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado. | Realización del Mantenimiento adecuado | Correctivo | Realizar el contrato de mantenimiento de software |
| | | corrupción de los datos en el momento de realizar copias | | | Restauración de pruebas de información / Transporte, custodia y almacenamiento técnico para salvaguardar la información contenida. | Correctivo | Realizar el contrato de transporte y custodia de cintas de servidores |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SOFWARE / APLICACIONES | funcionamiento inadecuado de las aplicaciones de los software utilizados que afectan el proceso | bloqueo a nivel de servicios de la aplicación | mal funcionamiento del software, retraso en los procesos asociados a la aplicación | REDUCIR EL RIESGO por medio de acciones de control correctivas y preventivas que permita evitar la ocurrencia del riesgo | Monitoreo preventivo diario para determinar anormalidades en los diferentes servicios de la aplicación y los servidores. | Preventivo | Monitoreo de Logs |
| | | bloqueos, congelamiento o intrusión en el sistema | | | Realizar monitoreo diario del espacio en disco para evitar que el tamaño de los logs desborde el espacio | Preventivo | Monitoreo de Logs |
| HARDWARE | indisponibilidad del servidor o de los equipos de computo | obsolescencia tecnológica | perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos, afectación a toda la entidad | REDUCIR EL RIESGO por medio de acciones de control correctivas y preventivas que permita evitar la ocurrencia del riesgo | Se debe contar con el correspondiente plan de cambio y actualización de equipos para evitar rezagos tecnológicos no programados | Preventivo | Elaboración del plan de cambio de los equipos |
| | | falta de espacio por alto consumo de recursos | | | Monitoreo diario con la herramienta disponible para tal fin. | Preventivo | Reporte Mensual de análisis del monitoreo |
| | | puertos abiertos y servicios asociados que pueden causar la caída o falla de los servidores | | | Monitoreo diario con la herramienta disponible para tal fin. | Preventivo | Reporte Mensual de análisis del monitoreo |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | funcionamiento inadecuado del almacenamiento | saturación de la capacidad de almacenamiento | perdida de la información | EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado. | Realizar los correspondientes procedimientos para liberar espacio. Tareas programadas y monitoreadas | Preventivo | Reporte Semanal de Backus de servidores |
| | | reportes y alarmas | | | Contactar al proveedor para que atienda el servicio en discos de servidores | Preventivo | Reporte Semanal de la ocupación de Discos de Servidores |
| REDES DE COMUNICACIONES | ausencia de la integridad de la información en las comunicaciones para el desarrollo de los procesos | ataques informáticos frente a la seguridad de la información | Perdida, robo o mala utilización de la información | REDUCIR EL RIESGO por medio de acciones de control correctivas y preventivas que permita evitar la ocurrencia del riesgo | Monitoreo preventivo para determinar anormalidades, fortaleciendo la seguridad activa de la red. | Preventivo | Reporte Diario del Trafico de la Red. |

## *VALORACION DE LOS RIESGOS ANTES Y DESPUES DE LA IMPLEMENTACIÓN DE LOS CONTROLES*

| ACTIVO | RIESGO | VALOR ANTES DE LA IMPLEMENTACIÓN DE CONTROLES | VALORACIÓN DESPUES DEL CONTROL |
|---|---|---|---|
| RECURSO HUMANO | Indisponibilidad del servicio | RIESGO EXTREMO | RIESGO ALTO |
| | falta de personal autorizado y capacitado para la realización de las actividades del proceso | RIESGO EXTREMO | RIESGO ALTO |
| SERVICIOS | daños en los servicios tecnológicos y perdida de la información | RIESGO EXTREMO | RIESGO EXTREMO |
| | mal prestación del servicio, o servicio inexistente | RIESGO ALTO | RIESGO ALTO |
| DATOS / INFORMACION | afectación de la integridad de los datos | RIESGO EXTREMO | RIESGO ALTO |
| | afectación de la disponibilidad del respaldo de la información en los procesos | RIESGO EXTREMO | RIESGO EXTREMO |
| SOFTWARE / APLICACIONES | funcionamiento inadecuado de las aplicaciones de los software utilizados que afectan el proceso | RIESGO ALTO | RIESGO BAJO |
| HARDWARE | indisponibilidad del servidor o de los equipos de computo | RIESGO EXTREMO | RIESGO ALTO |
| | funcionamiento inadecuado del almacenamiento | RIESGO ALTO | RIESGO MODERADO |

| | | | |
|---|---|---|---|
| REDES DE COMUNICACIONES | ausencia de la integridad de la información en las comunicaciones para el desarrollo de los procesos | RIESGO EXTREMO | RIESGO EXTREMO |

### d. CALIFICACIÓN DE CONTROLES EXISTENTES

| SECTORIAL | EFICAZ | INSUFICIENTE | INEFICAZ | NO EXISTE |
|---|---|---|---|---|
| DESPACHO | 14 | 9 | | 11 |
| OFICINA ASESORA DE PLANEACION | 1 | 3 | | 4 |
| SECRETARIA DE AGRICULTURA | | | | 4 |
| SECRETARIA DE AMBIENTE | | 2 | | 2 |
| SECRETARIA DE DEPORTES | 2 | | | 2 |
| SECRETARIA DE EDUCACIÓN | 9 | 6 | | 22 |
| SECRETARIA DE GOBIERNO | 4 | 8 | | 16 |
| SECRETARIA DE HACIENDA | 16 | 20 | 6 | 7 |
| SECRETARIA DE INFRAESTRUCTURA | | 1 | | 2 |
| SECRETARIA DE MINAS | 1 | 2 | | |
| SECRETARIA DE SALUD | 30 | 55 | 22 | 62 |
| SECRETARIA GENERAL | | 6 | | 8 |
| **PORCENTAJES** | **21,57%** | **31,37%** | **7,84%** | **39,22%** |
| **TOTALES** | **77** | **112** | **28** | **140** |

En cuanto a los controles existentes para proteger los activos de información se identificó que en su gran mayoría no existen controles para mitigar los riesgos. El 31.37% de los controles son insuficientes en especial en la secretaría de salud y la secretaria de hacienda. Al respecto se identifican dentro de los controles existentes colocar contraseña a los equipos, cerrar la sesión de Windows al ausentarse del puesto de trabajo, generar copias de respaldo de la información en medios de almacenamiento externo y en la nube, apagar en forma apropiada en el equipo al culminar la jornada laboral y asegurarse de dejar las oficinas con llave al culminar la jornada de trabajo.

### e. VULNERABILIDADES

| SECTORIAL | HARDWARE | LUGAR | ORGANIZACIÓN | RR.HH. | SERVICIOS | SOFTWARE |
|---|---|---|---|---|---|---|
| DESPACHO | 9 | 1 | 18 | | | 6 |
| OFICINA ASESORA DE PLANEACION | 6 | | 1 | | | 1 |
| SECRETARIA DE AGRICULTURA | 2 | 1 | | 1 | | |
| SECRETARIA DE AMBIENTE | 2 | 2 | | | | |
| SECRETARIA DE DEPORTES | 4 | | | | | |
| SECRETARIA DE EDUCACIÓN | 18 | 5 | 7 | 1 | 4 | 2 |
| SECRETARIA DE GOBIERNO | 9 | 4 | 4 | 4 | 3 | 4 |
| SECRETARIA DE HACIENDA | 18 | 1 | 8 | 2 | 2 | 18 |
| SECRETARIA DE INFRAESTRUCTURA | 3 | | | | | |
| SECRETARIA DE MINAS | | | 3 | | | |
| SECRETARIA DE SALUD | 61 | 11 | 66 | 19 | 5 | 7 |
| SECRETARIA GENERAL | 8 | 5 | 1 | | | |
| **PORCENTAJE** | **39,22%** | **8,40%** | **30,25%** | **7,56 %** | **3,92%** | **10,64%** |
| **TOTALES** | **140** | **30** | **108** | **27** | **14** | **38** |

En cuento a las vulnerabilidades se identificó que un alto porcentaje se concentra en los equipos hardware asociados a la ausencia de procedimiento formal para el registro y retiro de los usuarios, ausencia de autorización de los recursos de procesamiento de información, respuesta inadecuada del mantenimiento del servicio, defectos bien conocidos del software, susceptibilidad a las variaciones de voltaje, suceptibidad al polvo, la humedad y la suciedad así como el uso incorrecto del hardware y el software.

## DIAGNOSTICO DE LOS MAPAS DE RIESGO DE LOS ACTIVOS DE INFORMACIÓN EN LA GOBERNACIÓN DEL CESAR

En la visita que se realizó por cada una de las sectoriales de la Gobernación del Cesar recolectando la información para elaborar un diagnóstico claro y conciso de la situación actual de la entidad, se evidencio en términos generales que los activos de información contenidos en medio físico, en forma digital o electrónica se encuentra en altos grados de probabilidades que ocurran riesgos de pérdida o hurto de la información y/o corrupción de datos de la misma, estos riesgo son altos debido a que son afectados por diferentes tipos de amenazas como son los daños físicos de la información contenidas en carpetas o cajas que son archivadas en sitios sin ningún tipo de control ni protección de la misma, para evitar que personal ajeno a sus custodio puedan tener acceso a ellas, tal como ocurre en la secretaria de Ambiente que carecen de archivadores para guardar sus carpetas de contrataciones, proyectos y comunicaciones internas y externas, al igual sucede en el Laboratorio de la secretaria de salud, en donde cada dependencia archiva la información que evalúan en cada proceso, en cajas que son puestas en estantes que están en las mismas oficinas que comparten entre varias personas y que no tienen ningún tipo de seguridad para evitar la pérdida de la información.

Además los activos de información contenida en forma digital en los discos duros de los computadores de las distintas sectoriales, mantienen amenazas constantes por fallas técnicas, susceptibilidades en cambios en los voltajes, como ocurrió en la oficina del componente de registro de títulos de la secretaria de salud, que por daños en el equipo se perdió información importante.

Además también por falta de controles de acceso, debido a que no utilizan contraseñas de ingreso, los equipos no son bloqueados cuando el titular no está en el puesto de trabajo, lo que conllevan a usos no autorizados de los equipos y exponen la información a errores y omisiones no intencionales de personas que no deben utilizar los equipos donde se guarda información, como ocurre en la oficina de la casa de la mujer, en donde las pasantes utilizan equipos que contienen información vital para esa oficina.

La información contenida en los diferentes correos electrónicos de la Gobernación del Cesar también mantiene unos riesgos altos de pérdida de información ya que no existe una política clara del uso de estos canales de contacto de la entidad con la ciudadanía, tal como ocurre en el despacho del señor gobernador, que no hay claridad sobre la privacidad y seguridad de la clave de acceso al correo institucional cuando la persona titular está de vacaciones, permiso o licencias, además que están expuesta a intrusos informáticos que mediantes virus pueden sustraer información importante para la Gobernación.

Todos estos riesgo tienen una alta probabilidad de ocurrencia por no existir en la mayoría de los procesos de la entidad procedimientos claros, documentados y aprobados por la oficina de Meci calidad, en donde se establezcan las hojas de rutas a seguir, los responsables y los controles necesarios para evitar que haya a lugar de permitir que la Gobernación del Cesar sea vulnerable a todos estos tipos de amenazas y se pueda perder o adulterar información importante para los diferentes procesos de cada una de las dependencias de la entidad.

Además se evidenciaron situaciones que involucran el compromiso de la información vital de la institución, las cuales mediante una muestra evidenciada en un mapa de riesgo levantara un análisis del mismo.

Se pudo observar que una de las fuentes criticas correspondiente a la perdida de la información vital o activo de información en las secretarias, siendo un factor común presentado en las diferente secretarías, pero se tomará de ejemplo para éste ejercicio como es la de infraestructura, se evidencia la vulnerabilidad clara que dicha información correspondiente a los obras de infraestructura contratada, e inspecciones/supervisiones de las obras de la institución reposa en los computadores personales de contratistas, pero también se pudo evidenciar que a dichos computadores o dicho contratista al finalizar su contrato es poca o nula la información suministrada por el correspondiente a cada una de sus actividades. Correspondiente a activos de información física como lo son los Archivos, se evidenció en la Secretaría de Agricultura la existencia de unos documentos de origen privado del funcionario dueño del proceso de estadísticas, los cuales son fuente exacta de información para la generación de documentos e informes que necesitan las áreas como planeación, despacho y la misma Secretaria de Agricultura; alarmante es el riesgo de deterioro que está expuesta dicha información, sin mencionar la posibilidad de pérdida de ella correspondiente al retiro o eliminación por parte propietario, y la cantidad de información que se encuentra organizada de una manera que únicamente el propietario es capaz de traducir. En la Secretaria General se pudo evidenciar la existencia o metodología de recolección de información bajo la utilización de un Disco duro externo como respaldo de un computador que es utilizado como servidor correspondiente a los procesos de sus contrataciones. Pero dicho respaldo no cuenta con un acervo de respaldo de dicha información en los servidores oficiales de la institución, donde la pérdida o daño físico de éste puede ser causal de la pérdida total de toda esa información.

Cada uno de estos procesos de activos de información que se encuentran alojados en los recursos informáticos debería de contar con una red institucional, la cual genere copias de seguridad en una carpeta específica alojada en un servidor para tal fin.

Mediante el levantamiento de información que se realizó en cada una de las secretarias y dependencias de la Gobernación del Cesar, se evidenciaron situaciones que involucran el compromiso de la información vital de la institución, las cuales mediante una muestra evidenciada en un mapa de riesgo levantara un análisis del mismo.

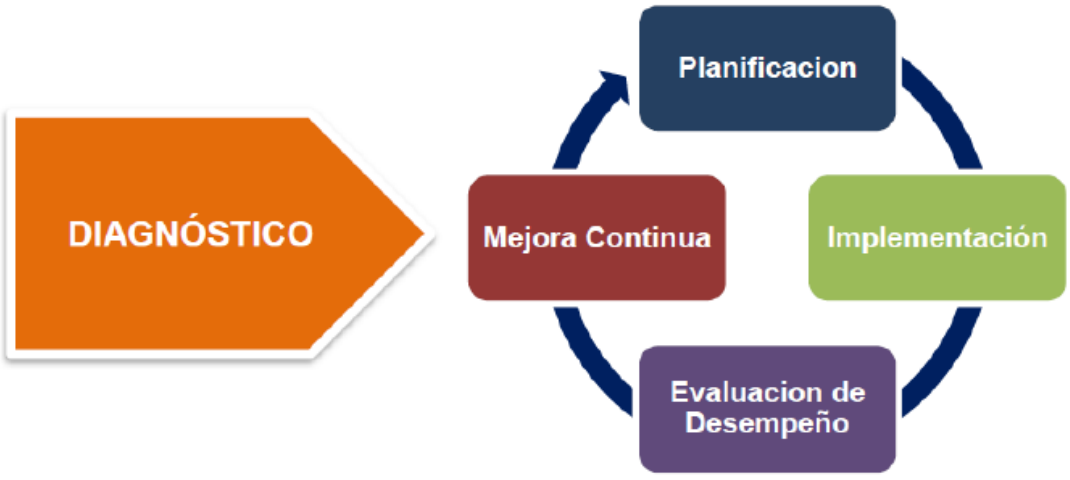
Se pudo observar que una de las fuentes criticas correspondiente a la perdida de la información vital o activo de información en las secretarias, siendo un factor común presentado en las diferente secretarías, pero se tomará de ejemplo para éste ejercicio como es la de infraestructura, se evidencia la vulnerabilidad clara que dicha información

correspondiente a los obras de infraestructura contratada, e inspecciones/supervisiones de las obras de la institución reposa en los computadores personales de contratistas, pero también se pudo evidenciar que a dichos computadores o dicho contratista al finalizar su contrato es poca o nula la información suministrada por el correspondiente a cada una de sus actividades. Correspondiente a activos de información física como lo son los Archivos, se evidenció en la Secretaría de Agricultura la existencia de unos documentos de origen privado del funcionario dueño del proceso de estadísticas, los cuales son fuente exacta de información para la generación de documentos e informes que necesitan las áreas como planeación, despacho y la misma Secretaria de Agricultura; alarmante es el riesgo de deterioro que está expuesta dicha información, sin mencionar la posibilidad de pérdida de ella correspondiente al retiro o eliminación por parte propietario, y la cantidad de información que se encuentra organizada de una manera que únicamente el propietario es capaz de traducir. En la Secretaria General se pudo evidenciar la existencia o metodología de recolección de información bajo la utilización de un Disco duro externo como respaldo de un computador que es utilizado como servidor correspondiente a los procesos de sus contrataciones. Pero dicho respaldo no cuenta con un acervo de respaldo de dicha información en los servidores oficiales de la institución, donde la pérdida o daño físico de éste puede ser causal de la pérdida total de toda esa información.

Cada uno de estos procesos de activos de información que se encuentran alojados en los recursos informáticos debería de contar con una red institucional, la cual genere copias de seguridad en una carpeta específica alojada en un servidor para tal fin.

## DESCRIPCIÓN DEL CICLO DE OPERACIÓN

Se contemplan cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.



Fase de Diagnostico – Etapas previas a la implementación

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.




**INSTRUMENTOS DE LA FASE ETAPAS PREVIAS A LA IMPLEMENTACIÓN**

1. Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad

2. Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad

3. Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: ESTADISTICA GLOBAL | | | | | | | | | | | |
| OBJETIVO: GENERAR INFORMACION NECESARIA PARA PROCESAR LOS DATOS QUE NECESITA EL DEPARTAMENTO Y HACER SEGUIMIENTO A LOS PROCESOS QUE SE GENERAN EN LA SECTORIAL | | | | | | | | | | | |
| SECTORIAL: PLANEACIÓN | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| perdida de la información | 1 | 5 | ALTA | clave personal del funcionario | | | | | reducir el riesgo | Área responsable del manejo del sistema / Área de tecnología | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: VIABILIDAD FINANCIERA DE LOS MUNICIPIOS | | | | | | | | | | | |
| OBJETIVO: ESTA INFORMACION SE PRESENTA A LA ASAMBLEA DEPARTAMENTAL PARA DETERMINAR LA VIABILIDAD DE LOS 25 MUNICIPIOS DEL DEPARTAMENTO Y SI CUMPLEN CON SUS GASTOS | | | | | | | | | | | |
| SECTORIAL: PLANEACIÓN | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| perdida de la información | 1 | 4 | media | solo el equipo tiene una clave de acceso | | | | | implementación de seguridad en los sistemas multimedia | Área responsable del manejo del sistema / Área de tecnología | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: gestión bancaria e informes | | | | | | | | | | | |
| OBJETIVO: generación de informes de la gestión bancaria | | | | | | | | | | | |
| SECTORIAL: TESORERIA | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Daños en el equipo | 4 | 5 | media | El control implementado son claves de acceso que solo la responsable de la información conoce | | | | | cambio y actualización en los sistemas de computo | Área responsable del manejo del sistema / Área de tecnología | |

**MAPA DE RIESGO**

**PROCESO: informes para entidades de control**

**OBJETIVO: suministrar información a los entes de control**

**SECTORIAL: tesorería**

| RIESGO | CALIFICACIÓN | | Evaluación | CONTROLES EXISTENTES | Nuevo control | Nueva calificación | | Evaluación | Medidas de Respuesta | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | |
| perdida de la información | 4 | 5 | media | los controles son implementados con claves de acceso que solo la responsable de la información conoce | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: cuentas y movimientos del sistema general de regalías | | | | | | | | | | | |
| OBJETIVO: guardar registros de los movimientos de las cuentas de las regalías | | | | | | | | | | | |
| SECTORIAL: Hacienda (tesorería) | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| fallas técnicas del equipo | 4 | 5 | media | los controles son implementados con claves de acceso que solo la responsable de la información conoce | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: liquidación de impuestos | | | | | | | | | | | |
| OBJETIVO: determinar el monto de cada contribuyente debe pagar por los diferentes impuestos departamentales | | | | | | | | | | | |
| SECTORIAL: hacienda | | | | | | | | | | | |
| RIESGO | CALIFICACIÓN | | Evaluación | CONTROLES EXISTENTES | Nuevo control | Nueva calificación | | Evaluación | Medidas de Respuesta | Responsable | Indicador |
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | |
| fallas en el sistema operativo | 3 | 5 | alta | no se acceden a páginas de ventas ni a redes sociales, se implementan claves para poder ingresar | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **MAPA DE RIESGO** | | | | | | | | | | | |
| **PROCESO: coordinación de estampillas y degüello** | | | | | | | | | | | |
| **OBJETIVO: determinar el recaudo por el degüello de ganado mayor por diferentes jeroglíficos y mataderos del dpto.** | | | | | | | | | | | |
| **SECTORIAL: Hacienda (rentas)** | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| fallas en el sistema operativo | 3 | 5 | alta | no se acceden a páginas de ventas ni a redes sociales, se implementan claves para poder ingresar | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: seguimiento a las eapb (empresas administradoras de planes y beneficios) | | | | | | | | | | | |
| OBJETIVO: verificar los niños susceptibles. Que no se han vacunado | | | | | | | | | | | |
| SECTORIAL: secretaria de salud, salud pública / dimensión vida saludable, enfermedades transmisibles(componentes inmunoprevenibles) | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| daños al hardware | 3 | 4 | media | se implementas claves de seguridad para el acceso al computador | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: manejo de la circular 030 del año 2013 | | | | | | | | | | | |
| OBJETIVO: hacer conciliaciones y mesas de trabajo trimestrales entre entidades responsables de pago y beneficiarias de pago | | | | | | | | | | | |
| SECTORIAL: secretaria de salud oficina de asuntos en salud, área circular 030 | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| daños al computador | 3 | 5 | alta | se implementan claves personales | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: reporte de la circular única en plataforma de la supersalud | | | | | | | | | | | |
| OBJETIVO: se consolida toda la información de la secretaria de salud(vacunación, vigilancia y control) de cada una de estas áreas | | | | | | | | | | | |
| SECTORIAL: secretaria de salud oficina de asuntos en salud, área circular 030 | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| daños al computador | 3 | 5 | alta | se implementan claves personales | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: reporte de la 2064 ctc | | | | | | | | | | | |
| OBJETIVO: se consolida todos los ctc y tutelas del departamento del cesar | | | | | | | | | | | |
| SECTORIAL: secretaria de salud oficina de asuntos en salud, área circular 030 | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| daños al computador | 3 | 5 | alta | se implementan claves personales | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: reporte 3374 rips | | | | | | | | | | | |
| OBJETIVO: se consolida toda la facturación de las eps e ips que prestan servicios en el departamento | | | | | | | | | | | |
| SECTORIAL: secretaria de salud oficina de asuntos en salud, área circular 030 | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| daños al computador | 3 | 5 | alta | se implementan claves personales | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: reporte resolución 1479 | | | | | | | | | | | |
| OBJETIVO: reporte de todos los procedimientos y medicamentos, diagnósticos no pos | | | | | | | | | | | |
| SECTORIAL: secretaria de salud oficina de asuntos en salud, área circular 030 | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| daños al computador | 3 | 5 | alta | se implementan claves personales | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: gestión estratégica de la secretaria de educación / comunicación | | | | | | | | | | | |
| OBJETIVO: coordinar, supervisar y controlar los procesos relacionados con la gestión estrategia de la secretaria de educación / comunicación | | | | | | | | | | | |
| SECTORIAL: secretaria de educación (despacho) | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| virus informático | 3 | 4 | alta | claves de acceso al computador | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: resolución 7797 2015 es la resolución que establece el proceso de gestión de cobertura (matricula, asignación de cupos, estrategias de permanencia, auditoria de matrículas)** | | | | | | | | | | | |
| **OBJETIVO: establecer los procesos que se van a implementar en los establecimientos educativos y que involucra a toda la población estudiantil** | | | | | | | | | | | |
| **SECTORIAL: secretaria de educación (cobertura)** | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| virus informático | 1 | 4 | media | claves de acceso al computador | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: Proceso de Investigación a funcionarios públicos** | | | | | | | | | | | |
| **OBJETIVO: Vigilar y supervisar que los funcionarios de la gobernación del Cesar cumplan sus funciones y de no hacerlo sancionarlos. Es un ente regulador de la Gobernación del Cesar. Las investigaciones son presentadas A través de quejas de particulares o informes de funcionarios de la entidad.** | | | | | | | | | | | |
| **SECTORIAL: Oficina de Control Interno Disciplinario** | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Software fuera de servicio | 4 | 2 | alta | Asegurarse de cerrar el aplicativo al finalizar la operación | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **MAPA DE RIESGO** | | | | | | | | | | | |
| **PROCESO: Seguridad y Participación Ciudadana** | | | | | | | | | | | |
| **OBJETIVO: Apoyar la elaboración, organización y custodia de los expedientes físicos** | | | | | | | | | | | |
| **SECTORIAL: Secretaría de Gobierno** | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida/hurto de expediente o documentos | 3 | 5 | extrema | No existen controles para salvaguardar la información | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: Etnias** | | | | | | | | | | | |
| **OBJETIVO: Elaboración, organización, custodia y seguimiento de la información de los procesos asociados a los Afros, indígenas y víctimas del conflicto armados.** | | | | | | | | | | | |
| **SECTORIAL: Secretaría de Gobierno** | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Extracción ilegal de información del computador | 3 | 5 | extrema | El equipo además de una clave de administrador cuenta con un código de seguridad para su acceso. Cuando la funcionaria responsable del equipo sale de vacaciones la ONU asigna un profesional provisional | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: Defensa Judicial | | | | | | | | | | | |
| OBJETIVO: Coordinación de la defensa judicial. Sistema judicial. actuaciones jurídicas | | | | | | | | | | | |
| SECTORIAL: Oficina de asuntos jurídicos | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida/hurto de expediente o documentos | 3 | 5 | extrema | No se evidencias controles | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: Gestión financiera (contabilidad)** | | | | | | | | | | | |
| **OBJETIVO: Declaraciones rete fuente reteica, la deuda del departamento interna y externa. En las declaraciones saca informe de pct que no son insumos para la declaración. Toda información la casca de PCT y la otra en recursos humanos y en educación. Esa información la almacena en el computador en un escritorio** | | | | | | | | | | | |
| **SECTORIAL: Secretaría de Hacienda** | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Fallas en servidor | 3 | 4 | extrema | No se evidencian controles | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: Gestión financiera (presupuesto) | | | | | | | | | | | |
| OBJETIVO: Manejo del presupuesto como herramienta para manejar los recursos destinados al gasto del departamento | | | | | | | | | | | |
| SECTORIAL: Oficina de Contabilidad | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Hurto o destrucción de la información | 3 | 4 | extrema | Dejar la oficina con llave y los equipos apagados al termina la jornada. Colocar contraseña al equipo | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: Gestión financiera (presupuesto) | | | | | | | | | | | |
| OBJETIVO: Manejo del presupuesto como herramienta para administrar los recursos destinados al gasto del departamento del Cesar | | | | | | | | | | | |
| SECTORIAL: Secretaría de hacienda | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Fallas en servidor | 3 | 4 | extrema | No se evidencian controles. Cuando la líder se ausenta por un momento de su lugar de trabajo la sesión del PCT queda abierta. Debería existir una regla de validación que después de un determinado tiempo de inactividad se cierre el aplicativo PCT automáticamente por seguridad | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: Gestión financiera (Rentas)** | | | | | | | | | | | |
| **OBJETIVO: Realizar el cobro coactivo a todas las personas que tengan obligaciones pendientes con el Departamento del Cesar siempre y cuando exista un título ejecutivo para poder realizar el cobro.** | | | | | | | | | | | |
| **SECTORIAL: Secretaría de hacienda** | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **CONTROLES EXISTENTES** | **Nuevo control** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Daño del computador | 4 | 4 | extrema | dejar la oficina con llave | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: ATENCIÓN AL CIUDADANO | | | | | | | | | | | | |
| OBJETIVO: Mantener una herramienta de comunicación entre los ciudadanos y la gobernación. | | | | | | | | | | | | |
| SECTORIAL: DESPACHO (ASUNTOS INTERNOS) | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTE** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| Sustracción o destrucción involuntaria de Correos electrónico. | 4 | 4 | Extrema | Reducir el riesgo, evitar, compartir o transferir | No existe medida de control. | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: ATENCIÓN AL CIUDADANO | | | | | | | | | | | | |
| OBJETIVO: Guardar en forma magnética los documentos generados y recepcionados en el área de despacho. | | | | | | | | | | | | |
| SECTORIAL: DESPACHO | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Perdida de la información reservada del despacho | 4 | 4 | Extrema | Reducir el riesgo, evitar, compartir o transferir | El computador tiene código de acceso al inicial sesión, también realiza bloqueo del equipo al levantarse del puesto de trabajo.<br>Mantiene copia de la información en disco de duro externo y USB. | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: ATENCIÓN AL CIUDADANO** | | | | | | | | | | | | |
| **OBJETIVO:** | **Realizar seguimientos a estado de los proyectos prioritarios de la administración departamental y a los compromisos adquiridos por contratistas, operadores y/o ejecutores de los proyectos en estado de atraso.** | | | | | | | | | | | |
| **SECTORIAL: DESPACHO** | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida de la información corrupción de datos | 4 | 4 | Extrema | Reducir el riesgo, evitar, compartir o transferir | Se socializa copia del acta original a los actores involucrados. | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: GESTIÓN DE TRAMITE | | | | | | | | | | | | |
| OBJETIVO: Ejerce gestión y control de registro de títulos profesionales de la salud del departamento del Cesar. | | | | | | | | | | | | |
| SECTORIAL: SECRETARIA DE SALUD (REGISTRO DE TITULO) | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida de la información corrupción de datos | 3 | 3 | Alta | Asumir el Riesgo, Reducir el Riesgo | No se tiene ningún tipo de restricción a la tabla de Excel. | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: INSPECCIÓN, VIGILANCIA Y CONTROL | | | | | | | | | | | | |
| OBJETIVO: Realizar seguimientos a estado de los proyectos prioritarios de la administración departamental y a los compromisos adquiridos por contratistas, operadores y/o ejecutores de los proyectos en estado de atraso. | | | | | | | | | | | | |
| SECTORIAL: SECRETARIA DE SALUD (LABORATORIO DEPARTAMENTAL) | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida de los informes | 3 | 4 | Extrema | Asumir el Riesgo, Reducir el Riesgo | Se realiza un backs de la información cada mes, solo maneja el computador la persona encargada | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: Inspección, vigilancia y control. | | | | | | | | | | | | |
| OBJETIVO: Dar cumplimiento a las metas trazadas en el plan de desarrollo departamental. | | | | | | | | | | | | |
| SECTORIAL: SECRETARIA DE AMBIETE | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida de la información corrupción de datos | 4 | 4 | Extrema | Asumir el Riesgo | No se tiene ningún tipo de control. | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: Inspección, vigilancia y control. | | | | | | | | | | | | |
| OBJETIVO: Dar respuesta y atención precisa a las inquietudes de los ciudadanos. | | | | | | | | | | | | |
| SECTORIAL: SECRETARIA DE MINAS | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida de las respuestas de los PQR | 3 | 3 | Alta | Reducir el Riesgo, Evitar, Compartir o Transferir | Entrega física de la información para archivar y guarda copia digital en su memoria. | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: INFORME DE GESTIÓN** | | | | | | | | | | | | |
| **OBJETIVO: Mantener informados de las distintas actividades que realiza la oficina para el cumplimiento de las metas del plan de desarrollo** | | | | | | | | | | | | |
| **SECTORIAL: SECRETARIA DE GOBIERNO (OFICINA DE LA MUJER)** | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida de los informes | 4 | 3 | Alta | Asumir el Riesgo, Reducir el Riesgo | el computador tiene clave de acceso de inicio | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: GESTIÓN EN SALUD Y PROMOCIÓN SOCIAL** | | | | | | | | | | | | |
| **OBJETIVO: Mantener toda la información documentada sobre casos de desnutrición en niños menores de 5 años de los 25 municipios del Departamento del Cesar incorporando el prestador de salud al cual pertenece.** | | | | | | | | | | | | |
| **SECTORIAL: SECRETARIA DE SALUD (Seguridad Alimentaria y Nutricional)** | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida de la información | 3 | 4 | Extrema | Asumir el Riesgo, Reducir el Riesgo | La base de datos se encuentra dispuesta en carpetas digitales encriptado y con password. | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: GESTIÓN EN SALUD Y PROMOCIÓN SOCIAL | | | | | | | | | | | | |
| OBJETIVO: Contener toda la información relevante durante las visitas de inspección vigilancia y control o de asistencia técnica a la red en prestadores en salud y entes territoriales municipales, a los cuales se les realizan visitas periódicamente. | | | | | | | | | | | | |
| SECTORIAL: SECRETARIA DE SALUD (Seguridad Alimentaria y Nutricional) | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Pérdida de la información | 3 | 4 | Extrema | Asumir el Riesgo, Reducir el Riesgo | Se asegura en archivadores con llaves manteniendo las condiciones ambientales adecuadas para evitar su deterioro. | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: GESTIÓN FINANCIERA (RIESGO) | | | | | | | | | | | | |
| OBJETIVO: Realizar el cobro coactivo a todas las personas que tengan obligaciones pendientes con el Departamento del Cesar siempre y cuando exista un título ejecutivo para poder realizar el cobro. | | | | | | | | | | | | |
| SECTORIAL: SECRETARIA DE HACIENDA (OFICINA DE PRESUPUESTO) | | | | | | | | | | | | |
| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES EXISTENTES | NUEVOS CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Responsable | Indicador |
| | Probabilidad | Impacto | Z. de Riesgo | | | | Probabilidad | Impacto | Z. de Riesgo | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Hurto o destrucción de la información | 3 | 4 | Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | Dejar la oficina con llave y los equipos apagados al terminar la jornada. Colocar contraseña al equipo. No existe una copia de respaldo escaneada almacenada en un medio de almacenamiento externo | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: Servicio de Atención a la Comunidad SAC | | | | | | | | | | | | |
| OBJETIVO: Recepción, trámite y resolución de las PQRD (Peticiones, quejas, reclamos y denuncias) interpuesta por los usuarios del SGSSS. | | | | | | | | | | | | |
| SECTORIAL: Secretaria de salud/Dimensión transversal gestión diferencial de poblaciones vulnerables | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Acceso no autorizado al sistema de información | 3 | 3 | Alta | Reducir el Riesgo, Evitar, Compartir o Transferir | No existen controles. | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO: Oficina de Inspección Vigilancia y Control /Gestión de la calidad | | | | | | | | | | | | | |
| OBJETIVO: Procesos y procedimientos de la secretaría de salud articulado con la oficina MECI de la gobernación del Cesar. Responsable del PAME (Programa de Auditoría para el mejoramiento de la Calidad). Compradores de servicios para la población pobre no asegurada. Se evalúan los servicios de salud con las entidades que la secretaría de salud suscriba convenios. Se evalúan la humanización del servicio. | | | | | | | | | | | | | |
| SECTORIAL: Secretaria de salud/Dimensión transversal gestión diferencial de poblaciones vulnerables | | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Hurto o destrucción de la información | 3 | 3 | Alta | Asumir el riesgo | Se generan 3 copias originales. No obstante no es suficiente este control. Se recomienda escanear. | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

| MAPA DE RIESGO |
|---|
| PROCESO: Inspección Vigilancia y Control |
| OBJETIVO: Procesos y procedimientos de la secretaría de salud articulado con la oficina MECI de la gobernación del Cesar. Responsable del PAME (Programa de Auditoría para el mejoramiento de la Calidad). Compradores de servicios para la población pobre no asegurada. Se evalúan los servicios de salud con las entidades que la secretaría de salud suscriba convenios. Se evalúan la humanización del servicio. |

| SECTORIAL: Secretaria de Salud (Gestión de la Calidad) | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Hurto o destrucción de la información | 3 | 4 | Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | Dejar la oficina con llave y los equipos apagados al termina la jornada. Colocar contraseña al equipo. No existe una copia de respaldo escaneada almacenada en un medio de almacenamiento externo | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: SALUD PUBLICA** | | | | | | | | | | | | |
| **OBJETIVO: Apoyar la gestión de acciones se seguimiento, evaluación, asistencia técnica de la dimensión según línea operativa de gestión de la salud pública con énfasis en VIH/SIDA para la reducción de la transmisión materno-perinatal de VIH del departamento del Cesar** | | | | | | | | | | | | |
| **SECTORIAL: Secretaria de Salud (Sexualidad, derechos sexuales y reproductivos / VIH)** | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Hurto o destrucción de la información | 3 | 4 | Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | Dejar la oficina con llave y los equipos apagados al termina la jornada. Colocar contraseña al equipo. No existe una copia de respaldo escaneada almacenada en un medio de almacenamiento externo | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: SALUD PUBLICA** | | | | | | | | | | | | |
| **OBJETIVO: Apoyar la gestión de acciones se seguimiento, evaluación, asistencia técnica de la dimensión según línea operativa de gestión de la salud pública con énfasis en VIH/SIDA para la reducción de la transmisión materno-perinatal de VIH del departamento del Cesar** | | | | | | | | | | | | |
| **SECTORIAL: Secretaria de Salud (Sexualidad, derechos sexuales y reproductivos / VIH)** | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES EXISTENTES** | **NUEVOS CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | |
| Hurto o destrucción de la información | 3 | 4 | Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | Dejar la oficina con llave y los equipos apagados al termina la jornada. Colocar contraseña al equipo. No existe una copia de respaldo escaneada almacenada en un medio de almacenamiento externo | | | | | | | |

| MAPA DE RIESGO | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCESO: INTERBENTORIA/SUPERVISION** | | | | | | | | | | | | |
| **OBJETIVO: SUPERVISAR UN CONTRATO EN LA FORMA TECNICA ADMINISTRATIVA FINANCIERA** | | | | | | | | | | | | |
| **SECTORIAL: SECRETARIA DE INFRAESTRUCTURA** | | | | | | | | | | | | |
| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Acciones** | **Responsable** | **Indicador** |
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | |
| Pérdida de Información/Perdida, mala manipulación, saboteo y retención indebida de información clasificada de la entidad y datos de terceros. | Probable(4) | Mayor(4) | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: CONTRATACION**

**OBJETIVO: REALIZAR EL DISEÑO DE LA LICITACIÓN BORRADOR Y LA LICITACIÓN DEFINITIVA**

**SECTORIAL: SECRETARIA DE INFRAESTRUCTURA**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| PERDIDA DE INFORMACION | Posible(3) | Moderado(3) | Zona de Riesgo Alta | Asumir el Riesgo, Reducir el Riesgo | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: ESTADISTICAS AGROPECUARIAS**

**OBJETIVO: ESTADISTICAS**

**SECTORIAL: SECRETARIA DE AGRICULTURA**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| PERDIDA DE INFORMACIÓN | Posible(3) | Moderado(3) | Zona de Riesgo Alta | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: NOMINA**

**OBJETIVO: FORMULACION NOMINA**

**SECTORIAL: SECRETARIA DE GENERAL**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| PERDIDA DE INFORMACION | Posible(3) | Catastrófico(5) | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: PROCESO PRECONTRACTUALES**

**OBJETIVO: ARCHIVO DIGITAL DE TDA LA CONTRATACION DE LA SECRETARIA**

**SECTORIAL: SECRETARIA GENERAL**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| PERDIDA DE INFORMACION | Posible(3) | Mayor(4) | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: ARCHIVO**

**OBJETIVO: DIRECIONAMIENTO DE LAS ACTIVIDADES Y OBJETIVO DL ARCHIVO DEPARTAMENTAL**

**SECTORIAL: SECRETARIA GENERAL/ARCHIVO**

| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Acciones** | **Responsable** | **Indicador** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | |
| PERDIDA DE INFORMACION | Posible(3) | Catastrófico(5) | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |
| | | | | | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: ARCHIVO**

**OBJETIVO: SALVAGUARDAR LA DOCUMENTACION QUE SE DEBE DE ARCHIVAR CORRESPONDIENTE A LA GOBERNACION DEL CESAR**

**SECTORIAL: SECRETARIA GENERAL/ARCHIVO**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| PERDIDA DE INFORMACION | Improbable(2) | Mayor(4) | Zona de Riesgo Alta | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: ARCHIVO**

**OBJETIVO: CREACIÓN DEL PROCESO DE DISPOSICION FINAL DE LOS ARCHIVOS**

**SECTORIAL: SECRETARIA GENERAL/ARCHIVO**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| PERDIDA DE INFORMACION | Posible(3) | Moderado(3) | Zona de Riesgo Alta | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: CONTRATO DE COMODATOS**

**OBJETIVO: ENTREGAR EL USO DE ACTIVOS DEL DEPARTAMENTO**

**SECTORIAL: SECRETARIA GENERAL/ALMACEN**

| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Acciones** | **Responsable** | **Indicador** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | |
| PERDIDA DE INFORMACION | Posible(3) | Moderado(3) | Zona de Riesgo Alta | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: CONTRATO DE COMODATOS**

**OBJETIVO: ENTREGAR EL USO DE ACTIVOS DEL DEPARTAMENTO**

**SECTORIAL: SECRETARIA GENERAL/TALENTO HUMANO**

| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Acciones** | **Responsable** | **Indicador** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | |
| PERDIDA DE INFORMACION | Posible(3) | Catastrófico(5) | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: Gestión Jurídica**

**OBJETIVO: Revisar los actos administrativos que firma el secretario de salud; contestar e impugnar las acciones de tutela que se proponen en contra de la secretaria de salud, derechos de peticiones; respuesta, seguimiento y control de los incidentes de desacato que se proponen en contra del secretario de salud y funcionarios de la secretaria de salud por algún incumplimiento de los fallos de tutela; emisión de conceptos dirigidos a la oficina de contratación por solicitud de esta en aquellos casos donde se pretenda demandar al Dpto. del Cesar por la vía administrativa; Revisión eventual de las liquidaciones de los contratos.**

**SECTORIAL: Secretaria de salud**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| Hurto o destrucción de la información/Destrucción del expediente a causa del fuego, agua, humedad hurto o extravío de la información. | Posible(3) | Mayor(4) | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: Autorizaciones**

**OBJETIVO: Autorización de servicio de salud a la población pobre no asegurada del Dpto. del Cesar. Apoyo técnico científico a la parte jurídica; Apoyo al proceso de alto costo.**

**SECTORIAL: Secretaria de salud**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| Pérdida de información/Pérdida de información por daño de servidor | Posible(3) | Mayor(4) | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: Radicación de cuentas médicas**

**OBJETIVO: Llevar la información de las cuentas que ingresar al ente, manejar las fechas de dichas cuentas de los prestadores IPS EPS EVENTOS NO POS PPNA (Población Pobre no asegurada)**

**SECTORIAL: Secretaria de salud**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| Colapso del sistema de información (Pérdida de información) | Casi Seguro(5) | Catastrófico(5) | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: Sistemas**

**OBJETIVO: Soporte a las IPS-EPS y personas de aseguramiento para el manejo de la plataforma SITIS.**

**SECTORIAL: Secretaria de salud**

| RIESGO | CALIFICACIÓN | | Evaluación | Medidas de Respuesta | CONTROLES | Nueva calificación | | Evaluación | Medidas de Respuesta | Acciones | Responsable | Indicador |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Impacto | Z. de Riesgo | | | Probabilidad | Impacto | Z. de Riesgo | | | | |
| Colapso del sistema de información (Pérdida de información) | Casi Seguro(5) | Catastrófico(5) | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

**MAPA DE RIESGO**

**PROCESO: Validación**

**OBJETIVO: Comprobación de derecho al momento de la atención tanto de usuarios PPNA como de actividades no contempladas en el plan de beneficios de salud NO POS. Se manejan bases de datos ADRES, MAESTRO CONPENSADOS, RUAF, SISBEN REGISTRADURIA NACIONAL, BASE MAESTRA DEPARTAMENTAL (EXCEL) Y VERIFICADOR (CONSULTA SOFTWARE SITIS) nacionales y departamentales como insumo para este proceso.**

**SECTORIAL: Secretaria de salud /Asuntos en salud**

| **RIESGO** | **CALIFICACIÓN** | | **Evaluación** | **Medidas de Respuesta** | **CONTROLES** | **Nueva calificación** | | **Evaluación** | **Medidas de Respuesta** | **Acciones** | **Responsable** | **Indicador** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | **Probabilidad** | **Impacto** | **Z. de Riesgo** | | | | |
| Pérdida de información/daño en disco duro | Posible(3) | Moderado(3) | Zona de Riesgo Alta | Reducir el Riesgo, Evitar, Compartir o Transf | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | erir | | | | | | | | |

## DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad, por sus siglas en ingles Statement of Applicability (SoA), es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

- La declaración de aplicabilidad se debe realizar luego del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos.

- La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y la razón del por qué no son requerías por la Entidad).

| | | Objetivo de control o control seleccionado Si/No | Razón de la Selección | Objetivo de control o control Implementado Si/No | Justificación de exclusión | Referencia | Aprobado por la alta dirección Firma director de la entidad |
|---|---|---|---|---|---|---|---|
| Dominio | A.5 Políticas de seguridad de la información | | | | | | |
| Objetivo de control | A. 5.1 Directrices establecidas por la dirección para la seguridad de la información | | | | | | |
| Control | A. 5.1.1 Políticas para la seguridad de la información | | | | | | |
| Control | A. 5.1.2 Revisión de las políticas para seguridad de la información | | | | | | |

## COMUNICACIÓN Y CONSULTA

La comunicación es muy importante porque permite que todas las partes interesadas emitan su propio juicio sobre los riesgos; es importante tener en cuenta que las percepciones variarán en cuanto a los valores, necesidades, suposiciones, conceptos y preocupaciones de los interesados.

## MONITOREO Y REVISIÓN

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación:

En primera instancia el seguimiento se debe llevar a cabo por el responsable del proceso (Director, Jefe, Líder). Segundo momento de seguimiento por parte del Subgerente (Procesos asistenciales, procesos administrativos y financiero).

La Oficina de Control Interno comunicará y presentará luego del seguimiento y evaluación, los resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas

Por lo menos cada semestre, cada responsable de proceso realizará una autoevaluación a la gestión del riesgo, determinando la efectividad de sus controles para minimizar el riesgo, a su vez la Oficina de Control Interno realizará su propio informe de evaluación de riesgos y controles de segundo orden.

## MECANISMOS DE SEGUIMIENTO Y VERIFICACIÓN

Los atributos establecidos para valorar el desempeño de la gestión de riesgos es una parte de la evaluación global de la institución y de la medición del desempeño de las áreas y de las personas.

Las valoraciones integrales de toda la institución y particulares por proceso, proyecto o estrategia correspondiente a la disminución del nivel de vulnerabilidad, por lo que se tiene el siguiente indicador:

Índice de riesgo residual por proceso: Expresado como proporción o porcentaje de la reducción de los valores estimados de probabilidad e impacto, luego de aplicar las medidas de gestión de riesgos para cada proceso o proyecto.

Formula:

RIESGO INHERENTE – **EFECTIVIDAD GESTIÓN DEL RIESGO** = RIESGO RESIDUAL

| RIESGO CONTROLADO |
|---|

Meta: Índice de riesgo residual por proceso: Menor de 25

Por lo menos cada semestre, cada responsable de proceso realizará una autoevaluación a la gestión del riesgo, determinando la efectividad de sus controles para minimizar el riesgo, a su vez la Oficina de Control Interno realizará su propio informe de evaluación de riesgos y controles de segundo orden.

Se tiene dispuesto en la intranet el Mapa de los riesgos tanto clínicos como administrativos segregados por procesos y responsables para su debida consulta y gestión, este engloba la totalidad de los riesgos a gestionar alojados en una tabla de Excel debidamente clasificados y valorados.

### Nivel de Madurez de la Gestión del Riesgo

Herramienta utilizada para capturar y evaluar las prácticas de riesgos de la institución y proporcionar realimentación en forma de una calificación de Madurez de la Gestión de Riesgos. El índice se calcula en base a preguntas relacionadas con las actuales prácticas de gestión de riesgos, la estructura de gobierno corporativo y el proceso de toma de decisiones de la entidad.

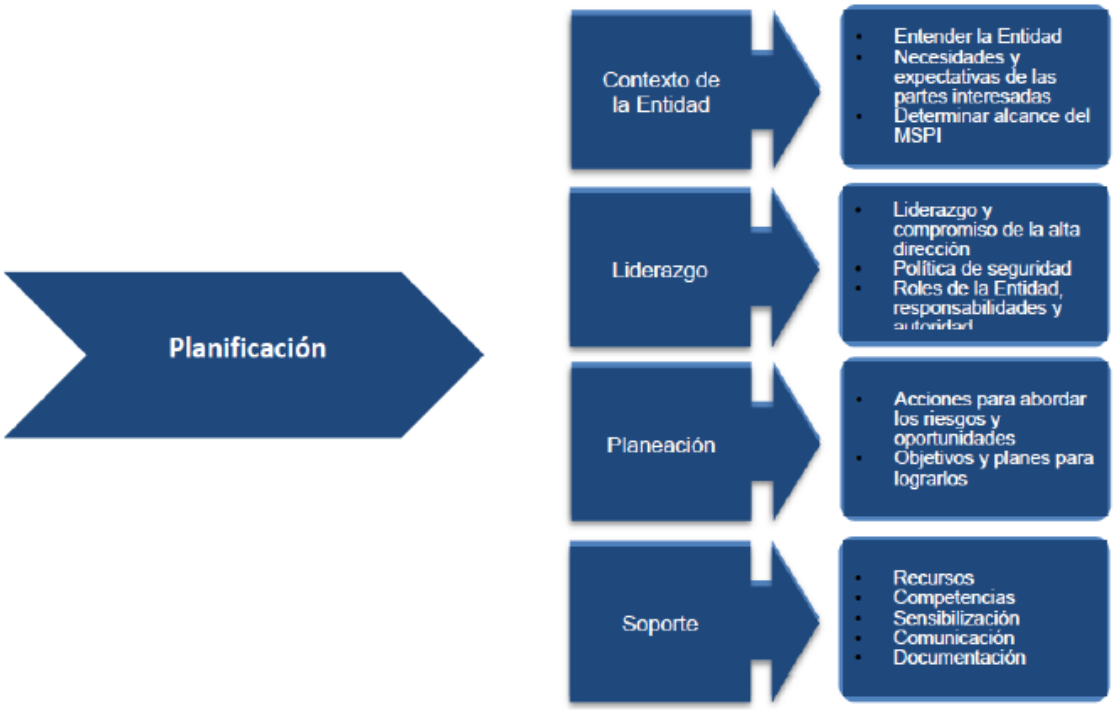
Meta: Nivel de Madurez de la Gestión del Riesgo: Mayor de 3.0

**FASE DE PLANIFICACIÓN**

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad.

Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.




**Resultados e Instrumentos de la Fase de Planificación**

| | |
|---|---|
| Seguridad y Privacidad de la Información | Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad. |
| Políticas de seguridad y privacidad de la información | Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad. |
| Procedimientos de seguridad de la información. | Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional. |
| Roles y responsabilidades de seguridad y privacidad de la información. | Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad. |
| Inventario de activos de información. | Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.<br>Matriz con la identificación, valoración y clasificación de activos de información.<br>Documento con la caracterización de activos de información, que contengan datos personales<br>Inventario de activos de IPv6 |
| Integración del MSPI con el Sistema de Gestión documental | Integración del MSPI, con el sistema de gestión documental de la entidad. |
| Identificación, Valoración y tratamiento de riesgo. | Documento con la metodología de gestión de riesgos.<br>Documento con el análisis y evaluación de riesgos.<br>Documento con el plan de tratamiento de riesgos.<br>Documento con la declaración de aplicabilidad.<br>Documentos revisados y aprobados por la alta Dirección. |
| Plan de Comunicaciones. | Documento con el plan de comunicación, sensibilización y capacitación para la entidad. |
| Plan de diagnóstico de IPv4 a IPv6. | Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. |

## DESCRIPCIÓN DE FASE DE PLANIFICACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

### Política de seguridad y privacidad de la información.

La Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento.

La política debe ser aprobada y divulgada al interior de la entidad.

Políticas de Seguridad y Privacidad de la Información.

Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información

En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente.

La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

### Procedimientos de Seguridad de la Información.

En este Ítem se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.

Esta actividad describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior de la entidad.

### Roles y Responsabilidades de Seguridad y Privacidad de la Información.

La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

### Inventario de activos de información.

La entidad debe desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

**Integración del MSPI con el Sistema de Gestión documental.**

La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación.

**Identificación, Valoración Y Tratamiento de Riesgos.**

La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad.

Para definir la metodología, la entidad puede hacer uso de buenas prácticas vigentes tales como: ISO 27005, Margerit, Octave, ISO 31000 o la Guía No 7 - Gestión de Riesgos emitida por el MinTIC.

**Plan de Comunicaciones.**

La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad.

Este plan será ejecutado, con el aval de la Alta Dirección, a todas las áreas de la Entidad.

**Plan de transición de IPv4 a IPv6.**

Para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir con la fase de planeación establecida en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

## BIBLIOGRAFIA

Guía 7 gestión de riegos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

Guía 8 controles de seguridad y privacidad de la información. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

Administración de riesgos: Contexto estratégico del riesgo, ministerio de hacienda.

GUÍA 24, instructivos para la implementación del Estándar de Control Contexto Estratégico del Riesgo.

Matriz de riesgos sistema de gestión de seguridad de la información, Instituto Nacional de Metrología de Colombia.

Guía para la administración del riesgo, departamento administrativo de la función pública.

## SEGUIMIENTO, CONTROL Y MEJORA

Las acciones y actividades articuladas al plan de acción de acuerdo a lo estipulado en el decreto 612 de 2018 se encuentran diligenciadas en el formato ES-PLI-GP003F01 Formulación y Evaluación Plan de Acción.

## CONTROL DE CAMBIOS

| FECHA | VERSION | CAMBIOS |
|---|---|---|
| 18/01/2019 | VER- 1.0 | |
| | | |
| | | |