PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

PG01-P06-GAF

Versión: Versión 04

2022 - 01 - 20

TABLA DE CONTENIDO

1. OBJETIVO

Atender y minimizar los riesgos asociados a los procesos tecnológicos existentes en la Dirección Territorial de Salud de Caldas, con el fin de salvaguardar los activos de información, definir el manejo de medios digitales, permitir el control de acceso y la gestión de los usuarios.

1.1. Objetivos Específicos

- Construir el plan de trabajo validando los recursos con los que se cuentan en la actualidad la Dirección Territorial de Salud de Caldas para obtener el plan adecuado.
- Socializar a funcionarios y contratistas de la entidad las medidas adoptadas y concientizarlos acerca de la importancia de gestionar de manera adecuada las tecnologías para mitigar los riesgos en la entidad.
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y mitigar los riesgos.

2. ALCANCE

El plan de tratamiento de riesgos tiene alcance para los procesos de la Dirección Territorial de Salud de Caldas, en concordancia con el alcance del Modelo de Seguridad y Privacidad de la información utilizando la metodología PHVA del modelo Integrado de Planeación y Gestión – MIPG.

3. TÉRMINOS Y DEFINICIONES

- **Activo de Información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

- **Análisis de riesgos**: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización.
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Causa**: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Consecuencia**: Resultado de un evento que afecta los objetivos.
- **Criterios del riesgo**: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- **Control**: Medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio,

particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Impacto:** Son las consecuencias que genera un riesgo una vez se materialice.
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mitigación:** Aplicación de acciones para reducir la vulnerabilidad frente a ciertas amenazas.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Prevención:** Aplicación de medidas para evitar que un evento se convierta en un desastre.
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL (ahora Gobierno Digital) la correlativa obligación de proteger dicha información

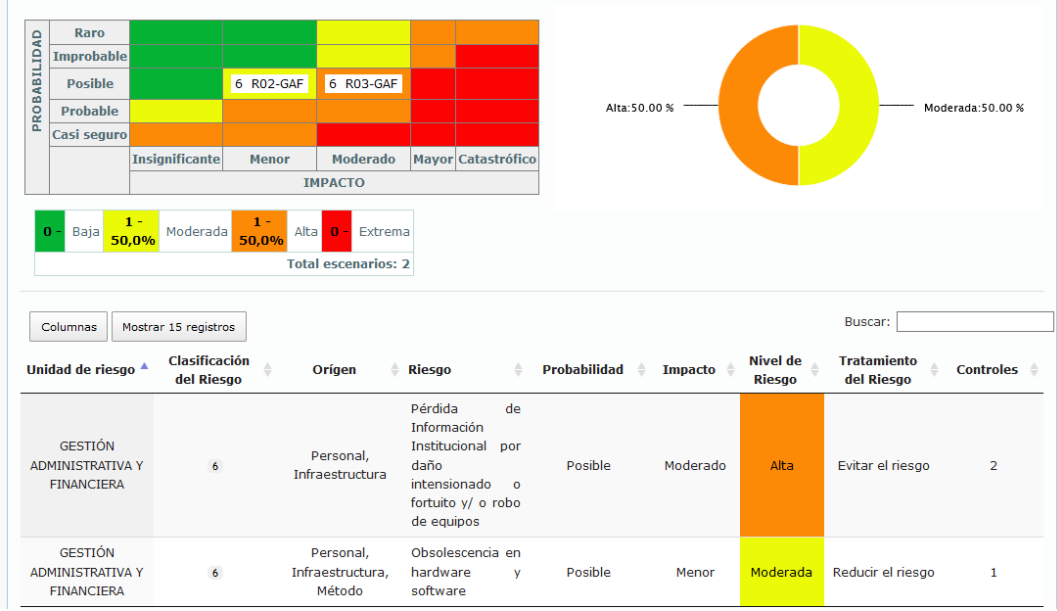
en observancia del marco legal vigente.

- **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:** Expectativa 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.
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

4. RIESGOS

A continuación, se muestran los riesgos determinados actualmente para el procedimiento de tecnología y que se encuentran en el sistema de gestión de calidad de la Entidad.



Unidad de riesgo	Clasificación del Riesgo	Origen	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Tratamiento del Riesgo	Controles
GESTIÓN ADMINISTRATIVA Y FINANCIERA	6	Personal, Infraestructura	Pérdida de Información Institucional por daño intensionado o fortuito y/ o robo de equipos	Posible	Moderado	Alta	Evitar el riesgo	2
GESTIÓN ADMINISTRATIVA Y FINANCIERA	6	Personal, Infraestructura, Método	Obsolescencia en hardware y software	Posible	Menor	Moderada	Reducir el riesgo	1

Ilustración 1. Riesgos actuales de TI

4.1. Riesgos determinados:

4.1.1. Pérdida de Información Institucional por daño intencionado o fortuito y/ o robo de equipos.

4.1.2. Obsolescencia en hardware y software.

Adoptando el modelo IT4+ y basándonos en la norma ISO27005, la Entidad realiza el análisis de riesgos actualizados del proceso, siguiendo las siguientes recomendaciones:

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológico	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A, D
	Perdida de suministro de energía	A, D
	Falla en equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	E
	Radiación térmica	E
	Impulsos electromagnéticos	E
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados.	D
	Divulgación.	D
	Datos provenientes de fuentes no confiables	D
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D

Fallas técnicas	Fallas del equipo	A, D
	Mal funcionamiento del equipo	A, D
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A, D
	Incumplimiento en el mantenimiento del sistema de información.	D
Convenciones: A: Accidental D: Deliberada E: Ambiental		

Tabla 1. Amenazas

4.2. Identificación del riesgo:

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida.

Los activos de información se clasifican en dos tipos:

4.2.1. Primarios:

Procesos o subprocesos y actividades del Negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

- Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
- Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las

tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

4.2.2. De Soporte

- Hardware: Los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, etc.).
- Software: Los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- Redes: Todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- Personal: Grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
- Estructura organizativa: responsables, áreas, contratistas, etc.

PROBABILIDAD			
Concepto	**Valor**	**Descripción**	**Frecuencia**
Raro	1	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en

PROBABILIDAD			
			El último año.
Casi Seguro	5	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

Tabla 2. Probabilidad

IMPACTO		
Concepto	**Valor**	**Descripción**
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	6	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la Agencia. Tiene un impacto bajo en los procesos de otras áreas de la Agencia.
Moderado	7	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la Agencia. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	11	La materialización del riesgo **retrasa el cumplimiento de los objetivos de la DTSC** y tiene un **impacto significativo en la imagen pública** de la Agencia y/o de la Nación. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	13	La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la Agencia**, tiene un **impacto catastrófico en la imagen pública de la Agencia y/o de la Nación**. Puede además generar impactos en: sectores económicos, los

IMPACTO	
	mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.

Tabla 3. Impacto

4.3. Identificación de los activos

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Para esto se cuenta con el inventario de activos de información, que incluye todo el hardware y software que compone la infraestructura tecnológica de la DTSC. Este inventario se administra a través del aplicativo OCS Inventory para equipos de cómputo y se emplea una hoja de cálculo para otros elementos que no poseen capacidad de conexión a red como los equipos de respaldo de energía (UPS), refrigeración (cuarto frio, aires acondicionados, ultra-congeladores, etc.), sensores de humo y temperatura, elementos pasivos de red, entre otros equipos que posee la DTSC. De igual forma se maneja un inventario de activos de información en hoja de cálculo, donde se almacena información de los diferentes sistemas de información, bases de datos y otra información ordenada de gran valor para los procesos de la Entidad.

4.4. Identificación de las amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. El modelo IT4+ presenta los siguientes riesgos, que según análisis del área de TIC aplican a la tecnología de nuestra Entidad:

Otras fuentes de amenazas son las humanas, a las cuales se debe prestar especial atención, máxime cuando la Entidad posee un porcentaje alto de contratistas y adicionalmente se cuenta con alta rotación de personal, debido principalmente a factores de origen político, de estructuración organizacional y a factores económicos. Se describen a continuación:

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto. Ego. Rebelión. Estatus. Dinero.	Piratería Ingeniería Social Intrusión, accesos forzados al sistema Acceso no autorizado
Criminal de la computación	Destrucción de la información. Divulgación ilegal de la información. Ganancia monetaria. Alteración no autorizada de los datos.	Crimen por computador. Acto fraudulento. Soborno de la información. Suplantación de identidad. Intrusión en el sistema.
Terrorismo	Chantaje. Destrucción. Explotación. Venganza. Ganancia política. Cubrimiento de los medios de comunicación.	Bomba/Terrorismo. Guerra de la información. Ataques contra el sistema DDoS[1]. Penetración en el sistema. Manipulación en el sistema.
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Ventaja política Explotación económica Hurto de información. Intrusión en privacidad personal. Ingeniería social. Penetración en el sistema. Acceso no autorizado al sistema.

[1] DDoS: Ataque de denegación de servicio distribuido del inglés Distributed Denial of Service

Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad. Ego. Inteligencia. Ganancia monetaria. Venganza. Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado. Chantaje. Observar información reservada. Uso inadecuado del computador. Fraude y hurto. Soborno de información. Ingreso de datos falsos o corruptos. Interceptación. Código malicioso. Venta de información personal. Errores en el sistema. Intrusión al sistema. Sabotaje del sistema. Acceso no autorizado al sistema.

Tabla 4. Amenazas humanas.

Actualmente, para los riesgos determinados en el numeral anterior para la unidad de riesgo de Gestión Administrativa son los siguientes:

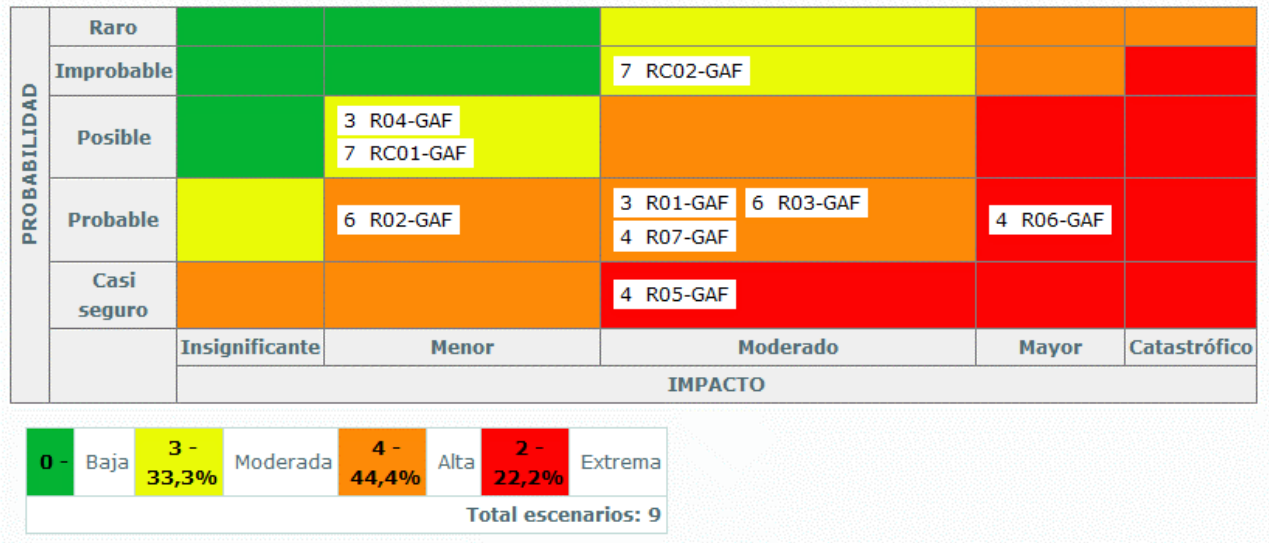


Ilustración 2. Matriz de riesgo institucional (Riesgo Absoluto)

Cód. Riesgo	Riesgo	Control
R02-GAF	Obsolescencia en hardware y software	Seguimiento a los lineamientos para la adquisición de tecnología
R03-GAF	Pérdida de Información Institucional por daño intencionado o fortuito y/ o robo de equipos	Monitoreo de los sistemas de seguridad de TIC con los que cuenta la entidad

Tabla 5 Riesgos determinados

5. Controles

Los controles de seguridad son medidas o contramedidas tomadas para evitar, contrarrestar o minimizar los riesgos TIC que se puedan presentar y que fueron descritos anteriormente en la tabla 5.

5.1. Obsolescencia tecnológica.

Las compras de tecnología deberán contar con el concepto técnico del área TIC o en su defecto de personal contratista de la entidad o externo, que cuente con el conocimiento y que garantice idoneidad e independencia en su concepto para permitir a la Entidad adquirir lo más conveniente y con las mejores características.

5.2. Estrategia de Respaldo y Recuperación

- Mantener actualizados y en sus últimas versiones los aplicativos de seguridad y respaldo de información.

- Realizar pruebas de recuperación de los datos de copias de seguridad para validar su integridad.
- Planificar la necesidad de personal adicional para atender los problemas que ocurran y requieran de apoyo especializado.
- Recurrir al procesamiento manual en los procesos que lo puedan soportar, si fallan los sistemas automatizados.
- Planificar el cierre y reinicio progresivo de los dispositivos y sistemas que se consideran en riesgo.
- Disponer del suministro adicional de combustible para los generadores, en caso de fallas eléctricas prolongadas.
- Elaborar un programa de disponibilidad que garantice la presencia permanente del personal.

5.3. Almacenamiento y Respaldo de la Información.

- Protocolo de copia de seguridad que defina la frecuencia de las copias (diario o periódico, incremental o total) considerando la criticidad de los datos y la frecuencia con que se introduce nueva información.
- Manual de procedimiento de copias de seguridad que defina la ubicación de las copias, los estándares de identificación, la frecuencia de rotación de medios y el modo de transporte al sitio externo.
- Los datos se respaldaran en discos magnéticos, cintas o discos ópticos.
- En lo posible, contar con lugar alternativo externo para el almacenamiento de la información más importante.

5.4. Sedes alternas para el Centro de Datos

- El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido; los sitios alternativos pueden ser:

- Propios de la entidad.
- De otra entidad con la que se firme un convenio de servicios de reciprocidad.
- Instalaciones alquiladas a terceros físicas o en la nube.

5.5. Divulgación de información confidencial.

- Implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la DTSC.
- Proteger la información contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio, empleando herramientas de DLP.
- Toma de conciencia, educación y formación de la Seguridad de la Información para todos los funcionarios y contratistas de la Entidad.

5.6. Acceso no autorizado a sistemas de información.

- Implementar protocolos de uso de contraseña segura en los sistemas de información.
- Restringir los accesos a los sistemas de información mediante perfiles restringidos.
- Gestionar con el área de talento humano, los registros de usuarios activos y desactivar las cuentas que estén caducadas o los funcionarios que se encuentren en períodos de vacaciones.
- Capacitar a los funcionarios y contratistas en el manejo de contraseñas seguras.

6. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Dirección Territorial de Salud de Caldas, busca minimizar los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

De esta forma, se garantiza el tratamiento de los riesgos de seguridad de la información y la gestión de riesgo positivo y oportunidad, acorde con lo establecido en la Política de Privacidad de la información.

6.1. PLANES DESARROLLADOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Desde la vigencia 2020 se definieron los lineamientos y las oportunidades de mejora creación y documentación de Matriz de riesgos de seguridad de la información; de tal forma que se definen nuevos riesgos de seguridad de la información y se asocia a los existentes según Norma ISO 27001:2013, a cada uno de ellos para evitar la materialización de los mismos.

6.2. Implementación

Para la implementación del Plan de Tratamientos de Riesgos de Seguridad y Privacidad de la Información de la entidad, se utilizará como metodología PHVA (Planear, Hacer, Verificar y Actuar), y los lineamientos y estrategias definidos por el Departamento Administrativo de la Función Pública – DAFP, con el apoyo de las herramientas que aporta la política Gobierno Digital de la mano con el Ministerio de las Tecnologías y las Comunicaciones MinTic.

6.3. Actividades

- Actualizar de forma semestral el diagnóstico de la situación actual de la Dirección Territorial de Salud de Caldas. Se deben identificar los nuevos activos de información (se incluyen los que corresponden a la Infraestructura Crítica Cibernética (ICC) y se clasifican de acuerdo con la normatividad vigente y aplicable (por ejemplo, para entidades públicas se deben tener en cuenta la ley 1712 de 2014 y la ley 1581 de 2012), que determinan la importancia del activo para la entidad e identifican el nivel de criticidad.

  Es importante resaltar que si la entidad presta servicios esenciales, "los necesarios para el mantenimiento de las funciones sociales básicas, salud, seguridad, bienestar social y económico de los ciudadanos o el funcionamiento de las instituciones del Estado y las administraciones públicas" , se deben establecer cuáles de los servicios esenciales hacen parte de la infraestructura crítica nacional, de acuerdo con los criterios de criticidad definidos por el CCOC, en la "Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia Primera Edición" y en ese caso, deben reportarse al CCOC y, posteriormente, a la aplicación del proceso de la gestión de riesgos. Es decir, se deben reportar las ICC identificadas en la entidad y también los riesgos asociados a estas infraestructuras críticas.
- Realizar la actualización de los riesgos por áreas con los líderes de cada proceso, se deben tener en cuenta las amenazas y las vulnerabilidades asociadas a cada activo de información.
- Valoración de los riesgos encontrados. Una vez actualizados los riesgos inherentes de seguridad digital para cada activo identificado, se deben

determinar la probabilidad e impacto de los criterios establecidos, durante la fase de planeación.

- Actualizar el plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia 2022, de acuerdo a las nuevas variables de seguridad encontradas en las revisiones.
- Comunicar, revisar y/o modificar el plan definido con los líderes de los procesos.
- Seguimiento y evaluación. La entidad debe determinar la efectividad de las actividades; esto se puede hacer mediante una revisión periódica y usando diferentes estrategias como las descritas a continuación:
  - **Revisión por la alta dirección:** El compromiso y liderazgo establecido por la alta dirección de la entidad se ve reflejado con la ejecución de revisiones periódicas y el seguimiento al proceso de gestión de riesgo de seguridad digital.
  - **Auditorías internas y externas:** Para realizar un monitoreo efectivo, así como las revisiones periódicas, la entidad debe programar y ejecutar auditorías internas y externas, con alcances definidos, con el fin de asegurar la efectividad en la gestión de riesgos de seguridad.
  - **Medición del desempeño:** La entidad podrá asegurar que las medidas de gestión de riesgos de seguridad digital son apropiadas para cumplir los objetivos económicos y sociales, a través de la definición y establecimiento de métricas para evaluar periódicamente la gestión. Esto incluye la definición de indicadores que permitan mantener monitoreados y controlados los riesgos de seguridad digital y así propender por minimizar su materialización.
  - **Rendición de cuentas:** Como parte integral de la gestión de riesgos, es importante tener presente que una vez la entidad haya implementado o

adaptado, los resultados obtenidos durante la medición del desempeño y los cambios correspondientes a la mejora continua, deben comunicarse y reportarse a la alta dirección y a las partes interesadas. Lo anterior, con el fin de que la evaluación de riesgos se contemple como insumo para la toma de decisiones.

6.4. PROGRAMACIÓN DE MONITOREO DE CONTROLES DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

De forma semestral se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración de los riesgos de seguridad de la información. Se podrá establecer una revisión anticipada de los controles de riesgos ante la aparición de un hecho que vulnere la seguridad o ante restructuraciones en la Entidad que modifiquen de forma notable su funcionamiento.

Los riesgos son dinámicos como la misma Entidad por tanto podrá cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: (1) nuevos activos o modificaciones en el valor de los activos, (2) nuevas amenazas (3) cambios o aparición de nuevas vulnerabilidades (4) aumento de las consecuencias o impactos, (5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

7. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO.

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- **Alta Dirección:** En responsabilidad del Comité de Gestión Institucional quien aprueba las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.
- **Proceso Administración del Sistema Gestión de Seguridad de la Información- SGSI:** Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.
- **Responsables de los procesos:** Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos institucionales) al menos una vez al año. Si bien los Líderes SGSI apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.
- **Servidores públicos y contratistas:** ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

8. RECURSOS PARA EL DESARROLLO DEL PLAN

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

La entidad con la destinación de los recursos suficientes para el desarrollo del plan y para el seguimiento y control de así:

- La ejecución del presupuesto asignado.
- Los recursos humanos destinados para tal efecto.
- Las herramientas que se determinen para la aplicación de los controles.
- En general, todo lo asociado con los proyectos estratégicos donde se registre evidencia del desarrollo de esta actividad.

9. MARCO LEGAL

Actualmente, el marco legal en el cual se apoya la implementación de este plan es el siguiente:

Norma	Descripción
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Decreto Nacional 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.
Ley 1581 de 2012	Por el cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto Nacional 103 del 20 de enero de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Ley 1955 de 2019	Por la cual se expide el Plan Nacional de Desarrollo 2018-2022 “To Pacto por Colombia, pacto por la equidad”
Decreto 415 de 2016- DAFP	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Resolución 2710 de 2017 - MinTic	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
Decreto No.1008 del 14 de Junio de 2018 - MinTic	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las comunicaciones.
CONPES 3854	Política Nacional de Seguridad Digital, se tiene como objetivo: “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país”.