• EJERCICIO • DE • ARQUITECTURA • EMPRESARIAL •

GOBIERNO DIGITAL

2022

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Actualización 2022

Octubre de 2022

RTVC
Sistema de Medios Públicos

CONTENIDO

CONTROL DE VERSIONES

Versión	Elaborado por	Revisado por	Aprobado por	Fecha	Motivo
1.0	MERLY TORRES BERNAL DIANA ROJAS LUIS	LAURA MARCELA PERDOMO FONSECA	LAURA MARCELA PERDOMO FONSECA	29-03-2021	Versión inicial
2.0	MERLY TORRES BERNAL JOSÉ DAVID ROJAS	LAURA MARCELA PERDOMO FONSECA	LAURA MARCELA PERDOMO FONSECA	15-11-2022	Actualización

1. OBJETIVOS

El documento Modelo de Seguridad y Privacidad de la Información para RTVC tiene como objetivos:

- Describir el entorno general de la seguridad y privacidad de la información en RTVC, así como el marco normativo aplicable.
- Definir de forma detallada el modelo de seguridad y privacidad de la información que se aplica en RTVC.
- Representar las etapas del modelo y la forma en que se abordarán por parte de la organización.

2. RESPONSABILIDADES QUE GENERA EL MODELO

ROL O DEPENDENCIA	RESPONSABILIDAD QUE SE GENERA A ESE ROL O DEPENDENCIA
Dirección de Tecnologías Convergentes	Es responsable de: • Llevar a los comités pertinentes, socializar y lograr la aprobación del modelo a nivel directivo. • Motivar a sus pares directivos y a los colaboradores de la Dirección de Tecnologías Convergentes para que apropien el modelo y todas las implicaciones que éste conlleva.
Colaboradores de la Dirección de Tecnologías Convergentes	Son responsables de: • Participar activamente en la implementación del modelo, siguiendo los lineamientos que éste produce. • Velar por que sus pares colaboradores de la entidad apropien el modelo y sus lineamientos. • Implementar y aplicar las diferentes tareas y actividades que generan el modelo y sus instrumentos.
Líderes de dependencias Jurídicas, Servicios Generales, Talento Humano	Son responsables de: • Conocer y aplicar, con base en las responsabilidades definidas en la matriz RASCI, los requisitos del modelo. • Aplicar y promover las mejores prácticas de seguridad y privacidad de la información con base en el modelo.
Comité Institucional de Gestión y Desempeño	Es responsable de: • Aprobar el modelo y todos los planes, actividades e iniciativas que éste genera, en el marco de la normatividad aplicable.

Tabla 1. Roles y Responsabilidades que genera el Modelo de Seguridad y Privacidad de la Información
Fuente: Coordinación de TI - RTVC

3. ALCANCE

El Modelo de Seguridad y Privacidad de la Información de RTVC, tiene como alcance todas las dependencias de RTVC, servidores públicos, colaboradores y visitantes en los casos que aplique. Apunta a proteger y preservar las características de la integridad, confidencialidad y disponibilidad de los activos de información que se identifiquen como parte de este modelo.

Está hecho para lectura y aplicación por parte de todos los funcionarios y colaboradores de RTVC, especialmente aquellos que tienen bajo su responsabilidad activos de información de todo tipo.

También debe extenderse a visitantes que tengan acceso en mayor o menor grado a la infraestructura de almacenamiento, transporte o procesamiento de datos e información de RTVC.

4. NORMATIVIDAD APLICABLE

El Modelo de Seguridad y Privacidad de la Información se basa, principalmente, en las siguientes leyes, normas o decretos:

Ley, Norma o Decreto	Ámbito de aplicación
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales.
Ley 1341 de 2009	Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC.
Ley 1581 de 2012	Protección de datos personales.
Decreto 1377 de 2013	Reglamentación parcial de la Ley 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 único reglamentario 1078 de 2015	Define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

Tabla 2. Normatividad aplicable RTVC
Fuente: Coordinación de TI - RTVC

5. DEFINICIONES

Acceso a la información pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados[1].

[1] Ley 1712 de 2014, art 4

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo[2].

Acuerdo de confidencialidad o contrato de confidencialidad: Es un acuerdo legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

Administración de riesgos: Conjunto de elementos de control que al interrelacionarse permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos[3].

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.[4]

Análisis de riesgo: en este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo.[5]

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.[6]

Auditoría - auditoría interna: Proceso sistemático, independiente y documentado para obtener evidencias que al evaluarse de manera objetiva permiten determinar la extensión en que se cumplen los criterios de auditoria, concebida para agregar valor y mejorar las operaciones de la organización.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.[7]

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.[8]

---

[2] CONPES 3854:2016, pág.56
[3] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018
[4] ISO/IEC 27000
[5] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 36
[6] Ley 594 de 2000, art 3
[7] Ley 1581 de 2012, art 3
[8] Ley 1581 de 2012

Bases de datos personales: Conjunto organizado de datos personales que sea objeto de tratamiento[9].

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas y programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.[10]

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.[11]

Clasificación de la información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la organización. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Confidencialidad: propiedad de la información que la hace no disponible, es decir divulgada a individuos, entidades o procesos no autorizados.[12]

Contingencia - desastre: Interrupción de la capacidad de procesamiento y/o acceso a la misma desde cualquier medio, que puede generar dificultades en la operación normal de un negocio.

Contramedida (salvaguarda): Medida o medidas de control que se establecen para evitar una situación de riesgo.

Control: medida que modifica el riesgo (proceso, políticas, dispositivos, practicas u otras acciones.[13]

Control de acceso: Mecanismos que en función de la identificación ya autenticada permite acceder a datos o recursos.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado[14] .

Dato público: 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.[15]

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

[9] Ley 1581 de 2012, art 3
[10] Resolución CRC 2258 de 2009
[11] CONPES 3701
[12] Norma ISO 27000 Términos y definiciones
[13] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 8
[14] ISO/IEC 27002:2013
15 Decreto 1377 de 2013, art 3

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.[16]

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.[17]

Datos personales mixtos: Es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos personales privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.[18]

Datos 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.[19]

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma ISO 27001.[20]

Derecho a la intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural[21].

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por la entidad.[22]

Documento en construcción: No será considerada información pública aquella información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal.

Encargado del tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.[23]

16 Ley 1712 de 2014, art 6
17 Ley 1581 de 2012, art 3
18 Ley 1581 de 2012, art 3 literal h
19 Decreto 1377 de 2013, art 3
20 ISO/IEC 27000
21 Jurisprudencia Corte Constitucional
22 Norma ISO 27000 Términos y definiciones
23 Ley 1581 de 2012, art 3

Etiquetado: El etiquetado de la información también se conoce como rotulado y tiene como propósito advertir de manera explícita a la persona que debe hacer la custodia de la información o quien la consulta, acerca del nivel de confidencialidad que tiene y por tanto las restricciones para su utilización y divulgación.

Evaluación del riesgo: Su objetivo es comparar los resultados del análisis de riesgos inherentes con los controles establecidos, para determinar la zona de riesgo final.[24]

Gestión del riesgo: proceso efectuado por la alta dirección de la organización y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. [25]

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.[26]

Información: Conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.[27]

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.[28]

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.[29]

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.[30]

Integridad: Propiedad de exactitud y completitud.[31]

Lista de chequeo de seguridad: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

---

[24] Norma ISO 31000 numeral 2.24

[25] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 8

[26] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 8

[27] ley 1712 del 2014

[28] ley 1712 del 2014

[29] Ley 1712 de 2014, art 6

[30] Ley 1712 de 2014, art 6

31 Norma ISO 27001 Términos y definiciones

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, de anonimización o cifrado.

Partes interesadas (stakeholder): Persona u organización que puede verse involucrada interna o externamente.

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.[32]

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.[33]

Política: Directriz emitida por la dirección que constituye la base de los procedimientos.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Privacidad: Es 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 la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Probabilidad: Se entiende como la posibilidad de que ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad. [34]

Procedimiento documentado: Documento en donde se establece la forma para llevar a cabo una actividad o un proceso, en la cual se debe definir como mínimo quien hace que, donde, cuando, porque y como.

Propietario de la información: Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

Registro: Documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas.

Registro nacional de bases de datos: Directorio público de las bases de datos sujetas a tratamiento que operan en el país.[35]

---

[32] ISO/IEC 27000

[33] ISO/IEC 27000

34 DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 8

[35] Ley 1581 de 2012, art 25

Responsabilidad demostrada: Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias[36].

Responsable del tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.[37]

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.[38]

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.[39]

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.[40]

Tabla de retención documental: Listado de series con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos.

Titulares de la información: Personas naturales cuyos datos personales sean objeto de tratamiento[41].

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en el país, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.[42]

Transmisión: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del país, cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable[43]

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.[44]

Tratamiento del riesgo: El resultado obtenido a través de la valoración del riesgo es denominado también valoración del riesgo de proceso ya que se "involucra la selección de una o más opciones para modificar los

36 Ley 1581 de 2012
37 Ley 1581 de 2012, art 3
38 ISO/IEC 27000
39 ISO/IEC 27000
40 ISO/IEC 27000
41 Ley 1581 de 2012, art 3
42 Ley 1581 de 2012
43 Ley 1581 de 2012
44 Ley 1581 de 2012, art 3

riesgos y la implementación de tales acciones" así el desplazamiento dentro de la matriz de evaluación y calificación determinará finalmente la selección de las opciones de tratamiento del riesgo, así: evitar, reducir, compartir, transferir o asumir un riesgo.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.[45]

Triada de seguridad: Denominación que se da a las tres características fundamentales de la seguridad de la información: confidencialidad, disponibilidad e integridad.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la organización, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.[46]

Valor jurídico: Nivel de protección legal que requiere la información para el logro de objetivos misionales.

Valor organizacional: Nivel de importancia de la información en el logro de los objetivos misionales.

Valoración de los riesgos: La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas.[47]

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.[48]

[45] ISO/IEC 27000

[46] ISO/IEC 27002:2013

[47] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018.

[48] ISO/IEC 27000

6. MARCO NORMATIVO Y CORPORATIVO DEL MODELO

La figura N° 1, muestra cómo se articula el modelo de seguridad y privacidad de la información de RTVC, con su modelo de madurez, con las normas de gobierno digital y con los objetivos estratégicos del PETI:

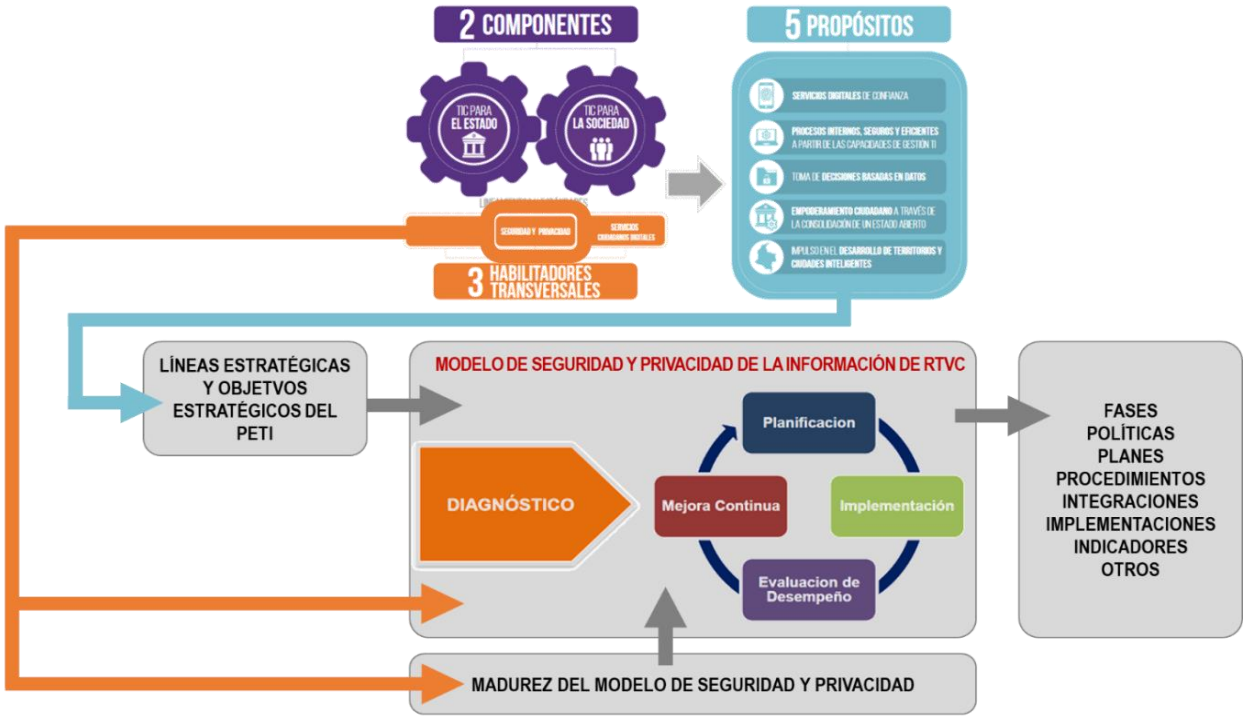

Figura 1. Articulación del modelo de seguridad y privacidad de la información de RTVC
Fuente: Coordinación de TI - RTVC

6.1. NORMA DE GOBIERNO DIGITAL

La estrategia de Gobierno Digital le provee al Modelo de Seguridad y Privacidad de la Información de RTVC lo siguiente:

- Lineamientos gubernamentales al Plan Estratégico de Tecnologías de la información (PETI) el cual, a su vez, provee las líneas y objetivos estratégicos para el cumplimiento de la seguridad y privacidad de la información.
- Lineamientos gubernamentales sobre los 5 propósitos del Gobierno Digital. Estos propósitos también influyen en la generación de las líneas estratégicas de RTVC.
- Lineamientos gubernamentales al Modelo de Seguridad y Privacidad de la Información desde el habilitador transversal Seguridad y Privacidad. Estos lineamientos permiten establecer que tan adelantado está el modelo respecto de lo esperado por la estrategia de Gobierno Digital.

6.2. OBJETIVOS ESTRATÉGICOS DEL PETI

El Modelo de Seguridad y Privacidad de la Información de RTVC se enmarca en el eje estratégico *"Se basa en seguridad"* del PETI cumpliendo con el objetivo estratégico de *"Fortalecer las capacidades de arquitectura y de gerencia estratégica de TI soportada en mejores prácticas"*

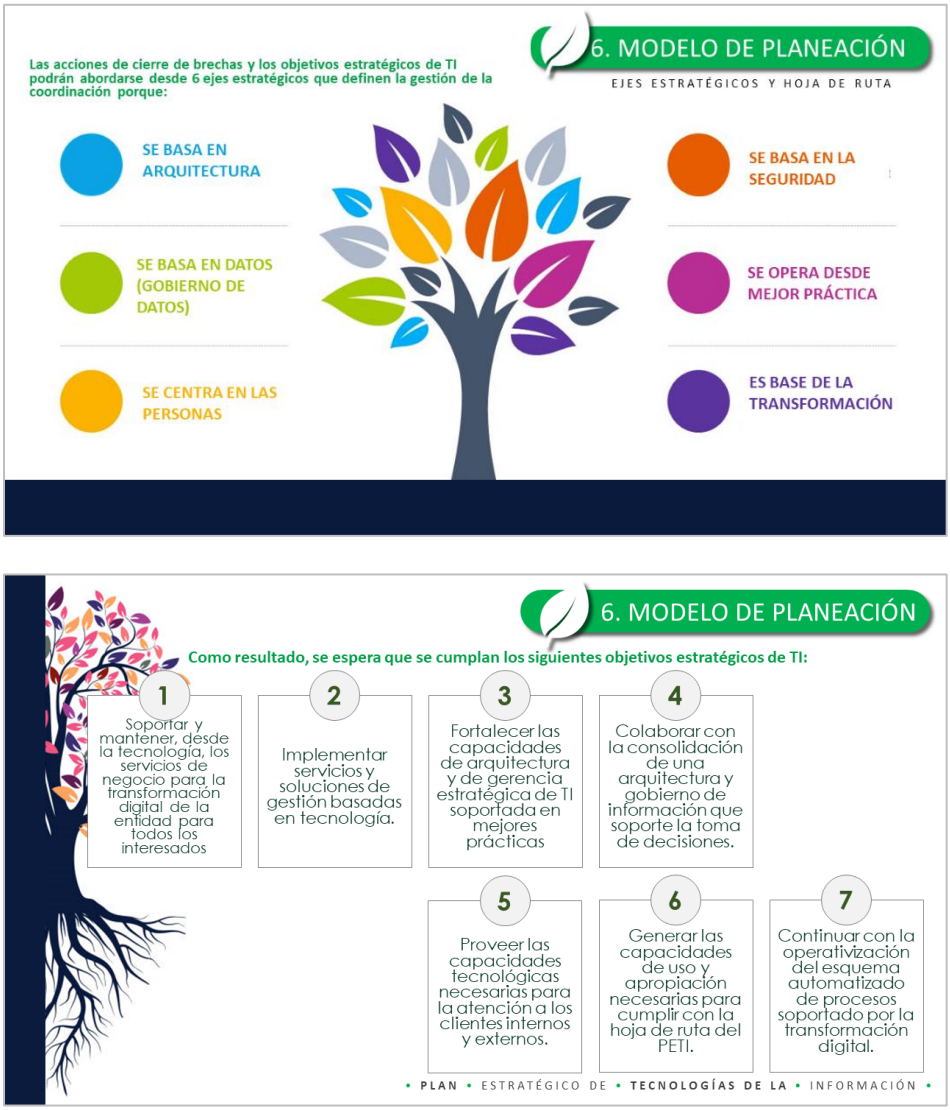

Figura 2. Plan Estratégico de Tecnologías de la Información de RTVC
Fuente: Coordinación de TI - RTVC

6.3. MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN RTVC

La madurez del Modelo de Seguridad y Privacidad de la Información de RTVC se evalúa con base en el modelo propuesto por la estrategia de Gobierno Digital del Ministerio de Tecnología de la Información. En este sentido, se toman las variables y mediciones sugeridas, así como los ejercicios previos de diagnóstico de años anteriores.

7. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA RTVC

La figura N° 3, muestra el Modelo de Seguridad y Privacidad de la Información de RTVC y cada uno de sus componentes, entradas y salidas.
El modelo se basa en uno de los 3 habilitadores transversales de la estrategia de Gobierno Digital del Ministerio de Tecnología de la Información:

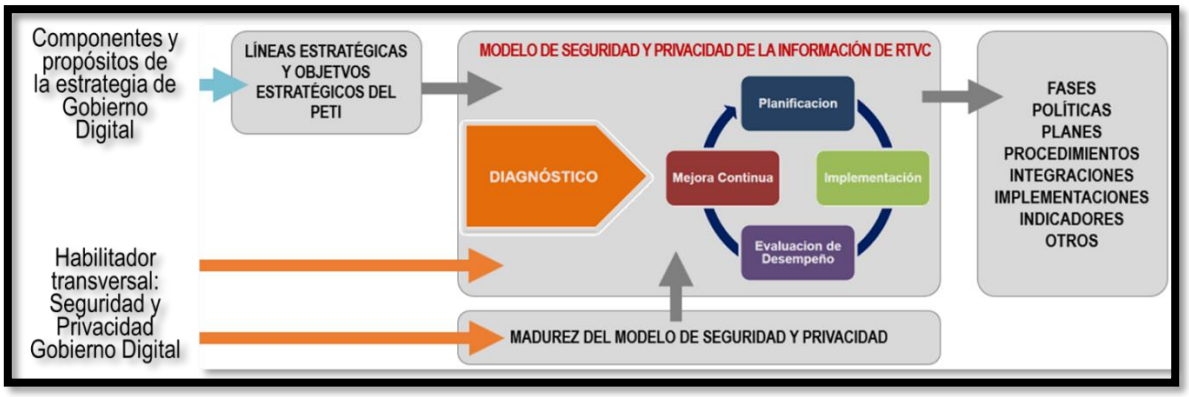

Figura 3. Modelo de seguridad y privacidad de la información de RTVC.
Fuente: Coordinación de TI RTVC

7.1. DIAGNÓSTICO

RTVC realizó un ejercicio de sensibilización, diagnóstico y autoevaluación del Modelo de Seguridad y Privacidad de la información durante el periodo 2021 - 2022 como resultado:

- Una evaluación cualitativa del componente de seguridad y privacidad desde la perspectiva TIC para la gestión de la Política de Gobierno Digital
- Una evaluación cuantitativa de la efectividad de los Controles ISO 27001.
- Un checklist con la evaluación cualitativa de los instrumentos y entregables de cada fase del modelo

Figura 4. Resultado de la evaluación cuantitativa de los componentes de seguridad y privacidad 2019-2020.
Fuente: Herramienta de Autodiagnóstico del MSPI Modelo de Seguridad y privacidad de la Información

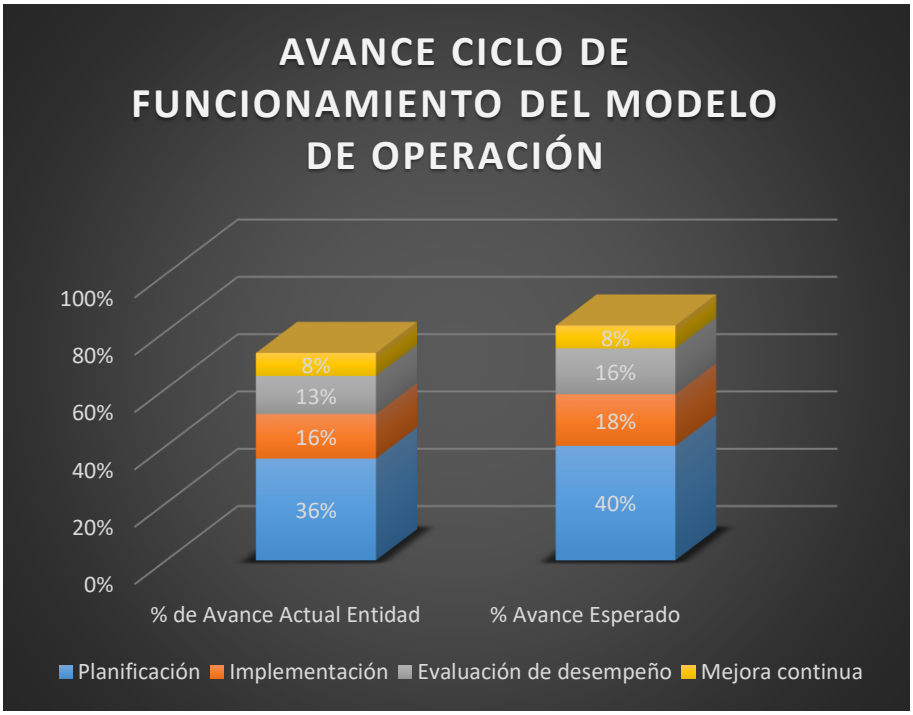

Figura 5. Checklist cualitativo de los instrumentos que hacen parte de las fases del modelo.
Fuente: Herramienta de Autodiagnóstico del MSPI Modelo de Seguridad y privacidad de la Información

7.2. PLANEACIÓN

La siguiente figura muestra el esquema general de planeación del Modelo de Seguridad y Privacidad de la Información para RTVC, de acuerdo con los lineamientos de la estrategia de Gobierno Digital, el Plan Estratégico de TI de RTVC y el diagnóstico descrito anteriormente:

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN RTVC					
			REQUISITO		
			1.MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	2.HERRAMIENTA DE AUTODIAGNOSTICO	3. MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN
No.	META	FASE	Resultados	Prueba	Actividad de Gestión
1	DIAGNOSTICO	DIAGONSTICO	Documento de diagnósticos del MSPI	Documento actualizado periodicamente	Documento actualizado periodicamente
2	VULNERABILIDADES	DIAGONSTICO	Documento con los hallazgos en la Prueba de Vulnerabilidad		Identificar vulnerabilidades Técnicas y administrativas
3	PLAN	PLANIFICACIÓN	Plan de seguridad y privacidad de la información alineado con el objetivo	Solicite el documento del alcance que debe estar aprobado, socializado	Definición de la implementación de las actividades
4	PRESUPUESTO	PLANIFICACIÓN	Asignación del presupuesto para la implementación del SGSI	Su cuenta con un presupuesto formalmente asignado	Asignación presupuesto para la implementación del SGSI
5	POLITICA	PLANIFICACIÓN	Política de Seguridad y Privacidad de la Información - Alineada con los objetivos	Solicita la política de seguridad de la información de la entidad	Política alineada con los objetivos estratégicos de la entidad.
6	MANUAL DE POLITICAS	PLANIFICACIÓN	Manual de Políticas de la entidad, con las políticas de Seguridad - Revisado		Manual con las políticas de la Seguridad y Privacidad de la Información.
7	PROCEDIMIENTO	PLANIFICACIÓN	Procedimiento de seguridad de la Información	Solicite formats de procesos y procedimientos debidamente definidos	
8	ACTO ADMINISTRATIVO	PLANIFICACIÓN	Acto administrativo a traves del cual se crea las funciones del Oficial de Seguridad de la Información	Solicite el acto administrativo a traves de la cual se crea y modifica las funciones	Acto Administrativo a través del cual se crean o modifican las funciones de Oficial de seguridad de la Información
9	METODOLOGIA ACTIVOS	PLANIFICACIÓN	Metodología para la identificación, clasificación y valoración de los activos de la información.		Metodología de gestión de activos
10	INVENTARIO DE ACTIVOS	PLANIFICACIÓN	Documento con el inventario de Activos, Matriz con la identificación, valoración de activos	Solicite el inventario de activos validado y aprobado	Inventario de activos de información, acorde a la metodología
11	INTEGRACIÓN DEL SISTEMA DE GESTIÓN	PLANIFICACIÓN	Integración del MSPI , con el sistea de Gestión documental de la entidad.		

Figura 6. Esquema general de planeación del modelo de seguridad y privacidad para RTVC.
Fuente: Herramienta de Autodiagnóstico del MSPI Modelo de Seguridad y privacidad de la Información

7.2.1. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Política Operacional de seguridad y privacidad de la información.

RTVC cuenta con la Política Operacional Seguridad de la Información – V4, disponible en el Sistema de Gestión de Planeación – Kawak, ruta: https://www.kawak.com.co/RTVC/gst_documental/doc_visualizar.php?v=1673

Políticas específicas de seguridad y privacidad de la información.
Corresponde al conjunto de políticas que integran los componentes de seguridad y privacidad de la información, dentro de estas se cuenta en RTVC con:

- Política operacional para la administración de la infraestructura – V4 https://www.kawak.com.co/RTVC/gst_documental/doc_visualizar.php?v=1044&m=43
- Política operacional de Seguridad de la Información y Seguridad digital – V5
- https://www.kawak.com.co/RTVC/gst_documental/doc_visualizar.php?v=1208&m=78
- Politica De protección de Datos
- https://www.kawak.com.co/RTVC/gst_documental/doc_visualizar.php?v=1435

- Política operacional de desarrollo y administración de software – V5 https://www.kawak.com.co/RTVC/gst_documental/doc_visualizar.php?v=1156&m=34
- Política operacional de gestión de la infraestructura física – V6 https://www.kawak.com.co/RTVC/gst_documental/doc_visualizar.php?v=917&m=90

Disponibles en el Sistema de Gestión de Planeación – Kawak, ruta: https://www.kawak.com.co/RTVC/main/home.php

Procedimientos de Seguridad de la Información

A continuación, se relacionan el estado de implementación de cada uno de los controles que propone el Modelo MSPI a través de la Guía No. 3 Procedimientos de Seguridad de la Información.

Los procedimientos referenciados en Construcción hacen parte de la Gestión del año 2021.

No	DOMINIO - CONTROL		APLICA (SI/NO)	EVIDENCIA
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**			
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**			
0bjetivo. Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.				
A.5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	SI	Se cuenta con políticas de seguridad de la información por cada uno de los dominios. I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4. Políticas de Seguridad de la Información y Seguridad Digital
A.5.1.2	Revisión de las políticas para la seguridad de la información.	Control. Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	SI	Se realiza la revisión y aprobación por parte del Comité Institucional de Gestión y Desempeño; en casos especiales por cambios en la Organización, o en la operación estos serán revisados de manera oportuna.

.

A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**			
A.6.1	**Organización interna**			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI	Se cuenta con la I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital, donde se discriminan los roles en seguridad de la información. Las cuales se encuentran en Kawak 4.6.1.1 Roles y Responsabilidades
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	SI	Se cuenta con la Resolución 147 de 2018, donde se crea el Comité Institucional de Gestión y Desempeño de Radio Televisión Nacional de Colombia- RTVC. Se cuenta la Política Operacional de Seguridad de la Información y Seguridad Digital, donde se discriminan los roles en seguridad de la información. Las cuales se encuentran en Kawak.

.

A.6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	SI	Se cuenta con el Documento Contacto con autoridades y grupos de interés especial.
A.6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	SI	Se cuenta con el Documento Contacto con autoridades y grupos de interés especial. Se tiene contacto con el Ministerio de las TIC y con CSIRT Gobierno
A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak
A.6.2	**Dispositivos móviles y teletrabajo**			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles				
A.6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	I-A-3 Política Operacional para la administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.7.2. Administración de la Red Inalámbrica 4.9.7. Acceso a WLAN
A.6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	SI	Boletín No. 50 del 26 de marzo de 2020, el cual señala que, como parte del compromiso con la transformación digital, RTVC – Sistema de Medios Públicos, mediante la Resolución 473 de 2017, adoptó el teletrabajo en modalidad suplementario, como una forma de organización laboral a distancia, utilizando como soporte las tecnologías de la información y las comunicaciones. H-F-20 Solicitud Incorporación del Teletrabajo
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A.7.1	**Antes de asumir el empleo**			
Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	SI	Procedimiento H-P-5 Procedimiento Selección y Contratación de Personal Formato H-F-14 Formato de Requisición de personal Revisión Antecedentes: Procuraduría, Contraloría, Policía y extranjeros (Interpol)
A.7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	SI	Procedimiento H-P-5 Procedimiento Selección y Contratación de Personal Formato H-F-14 Formato de Requisición de personal Revisión Antecedentes: Procuraduría, Contraloría, Policía y extranjeros (Interpol)

A.7.2	**Durante la ejecución del empleo**			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.4. Lineamientos para la Gestión de la Seguridad de la Información y de las Seguridad Digital Contrato de Trabajo.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la in formación.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	SI	H-P-4 Proceso de Desarrollo y formación de Personal y Evaluación de Desempeño
A.7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	B- P -1 Control Disciplinario B-A-1 Política Operacional de Control de Asuntos Disciplinarios
A.7.3	**Terminación y cambio de empleo**			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo				
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	SI	H- P-3 Proceso de Desvinculación I- F-14 Formato de Certificado de Paz y Salvo Informático H -F- 13 Formato de Entrevista Retiro de Trabajo Formato P-F-21 Formato de aprobación para la terminación Anticipada S-M-2 Manual Administrativo y Financiero para el manejo de contratos de Administración Delegada
A.8	**GESTION DE ACTIVOS**			
A.8.1	**Responsabilidad por los activos**			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.				
A.8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	Se cuenta con la Matriz de Inventario y Clasificación de activos de la Información Se cuenta con la Guía para la Gestión y clasificación de activos de Información

A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	SI	Se cuenta con la Matriz de Inventario y Clasificación de activos de la Información Se cuenta con la Guía para la Gestión y clasificación de activos de Información
A.8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.4. Lineamientos para la Gestión de la Seguridad de la Información y de las Seguridad Digital
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI	I-F-14 Formato Certificado Paz y Salvo Informático I- A-2 Política Operacional para la Administración de la Infraestructura de TI

A.8.2	**Clasificación de la información**			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A.8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak Se cuenta con el documento de Gestión y Clasificación de Activos de Información y la Matriz de Inventario y Clasificación de Activos de Información
A.8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Se cuenta con el documento de Gestión y Clasificación de Activos de Información Se cuenta con la Matriz de Inventario y Clasificación de Activos de Información Se cuenta con el Procedimiento de Etiquetado de Información
A.8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Se cuenta con el documento de Gestión y Clasificación de Activos de Información Se cuenta con la Matriz de Inventario y Clasificación de Activos de Información Se cuenta con el Procedimiento de Etiquetado de Información

A.8.3	**Manejo de medios**			
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios				
A.8.3.1	Gestión de medios removibles	Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.9.2. Seguridad del equipo fuera de RTVC 4.9.3. Escritorio y Pantalla limpia

A.8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI R-A-2 Política operacional de Gestión Ambiental R-S-1 Plan Institucional de Gestión Ambiental RTVC 5.3 Condición Ambiental Institucional
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak Criptografía

A.9	**CONTROL DE ACCESO**			
A.9.1	Requisitos del negocio para el control de acceso			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				
A.9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI
A.9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI
A.9.2	Gestión de acceso de usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Si	Política Operacional de Seguridad de la Información y Seguridad Digita Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos

A.9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos

A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos

A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Si	Política Operacional de Seguridad de la Información y Seguridad Digita Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos
A.9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos
A.9.3	Responsabilidades de los usuarios			
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
A.9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak

A.9.4	Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				
A.9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO

A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak b. CONTROL DE ACCESO LÓGICO
A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	Si	El Líder Soluciones de Software - Desarrollo es quien autoriza el manejo y control del código fuente. T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC 6. Políticas de Desarrollo de Software
A.10	**CRIPTOGRAFIA**			
A.10.1	Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información				
A.10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.7. CRIPTOGRAFÍA Se cuenta con el documento de Criptografía
A.10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.7. CRIPTOGRAFÍA Se cuenta con el documento de Criptografía

A.11	**SEGURIDAD FISICA Y DEL ENTORNO**			
A.11.1	Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A.11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico

A.11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico
A.11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico
A.11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico
A.11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.		I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico
A.11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI	Las áreas de cargue y despacho se encuentran aisladas de las áreas de procesamiento de información
A.11.2	Equipos			
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A.11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.9 Políticas de Usuarios 4.9.1 Equipos de computo
A.11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2 Políticas Generales
A.11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2 Políticas Generales
A.11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2 Políticas de Mantenimiento Preventivo de la Infraestructura Tecnológica

A.11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.9.2 Seguridad de equipos fuera de RTVC.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.9.2 Seguridad de los equipos fuera de RVC
A.11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak
A.11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.9.3 Escritorio y pantalla limpia
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.9.3 Escritorio y pantalla limpia
A.12	**SEGURIDAD DE LAS OPERACIONES**			
A.12.1	Procedimientos operacionales y responsabilidades			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	SI	I - P-7 Proceso Gestión de Incidentes Internos I- P- 9 Proceso Mantenimiento Preventivo Tecnológico Interno I-P-10 Proceso Monitoreo Tecnológico Interno T-P-1 Proceso Planificación de la Infraestructura Tecnológica T-P-4 Proceso Soluciones de Software T-S-1 Plan de Continuidad del Negocio
A.12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Pendiente el proceso Gestión de Cambios
A.12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Pendiente el proceso Gestión de la Capacidad
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.3.2 Servidores

A.12.2	Protección contra códigos maliciosos			
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.				
A.12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Se cuenta con la consola de Antivirus BitDefender, por medio de él se tiene control de tráfico de todo lo que pase por la Red.
A.12.3	Copias de respaldo			
Objetivo: Proteger contra la perdida de datos				
A.12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.2 Políticas de Backup
A.12.4	Registro y seguimiento			
Objetivo: Registrar eventos y generar evidencia				
A.12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.3.2 Servidores
A.12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.3.2 Servidores Las herramientas no permiten borrar los logs, si se desea realizar alguna actividad esta debe ser exportada para poder trabajar los logs de las actividades.
A.12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.3.2 Servidores Todo registro que se realice independiente del rol desempeñado queda registrado en los logs de los sistemas
A.12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	SI	Los relojes se sincronizan con Hora Legal Colombiana del INM

A.12.5	Control de software operacional			
Objetivo: Asegurarse de la integridad de los sistemas operacionales				
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak
A.12.6	Gestión de la vulnerabilidad técnica			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	SI	Se realiza anualmente el Análisis de Vulnerabilidades y Ethical Hacking.
A.12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.		I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak
A.12.7	Consideraciones sobre auditorias de sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos				
A.12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI	Se cuenta con Logs de Auditorías y las auditorías a los sistemas de información se encuentran debidamente programadas, las cuales quedan registradas en el formato
A.13	**SEGURIDAD DE LAS COMUNICACIONES**			
A.13.1	Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A.13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Se cuenta con Firewall Perimetral Se cuenta con el Diagrama de Red
A.13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Se cuenta con Firewall Perimetral Se cuenta con el Diagrama de Red

A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Se cuenta con Firewall Perimetral Se cuenta con el Diagrama de Red
A.13.2	Transferencia de información			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A.13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.		I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak
A.13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak "Cualquier copia, uso o distribución no autorizados de este mensaje y sus adjuntos puede generar responsabilidades legales. • Si usted no es destinatario de este correo, por favor notifíquelo al remitente. • Aplicamos la Ley Estatutaria 1581 de 2012, que protege el derecho de acceso a la información pública. • Antes de imprimir este mensaje, compruebe si es necesario hacerlo. El Medio Ambiente es cuestión de TODOS."
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	SI	Se cuenta con acuerdos de confidencialidad con funcionarios, proveedores y clientes debidamente firmados. Contrato laboral.
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**			
A.14.1	**Requisitos de seguridad de los sistemas de información**			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak Se realiza Sensibilización y Capacitación en Seguridad de la Información.

A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-F-1 Formato requerimientos iniciales para el desarrollo Web y Aplicaciones Las cuales se encuentran en Kawak
A.14.2	Seguridad en los procesos de Desarrollo y de Soporte			
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software T-F-1 Formato requerimientos iniciales para el desarrollo Web y Aplicaciones Las cuales se encuentran en Kawak
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak

A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.3	Datos de prueba			
Objetivo: Asegurar la protección de los datos usados para pruebas.				
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak

A.15	**RELACIONES CON LOS PROVEEDORES**			
A.15.1	Seguridad de la información en las relaciones con los proveedores.			
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak. Se cuenta con los acuerdos contractuales, Pólizas y Seguros.

A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak Acuerdos de confidencialidad firmados con los proveedores
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	SI	Se tienen en los contratos firmados con los proveedores que los mismos se comprometen a hacer cumplir las políticas de seguridad de la información Acuerdos de confidencialidad firmados con los proveedores
A.15.2	Gestión de la prestación de servicios de proveedores			
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI	Se realizan auditorías a los proveedores de tecnología de la información y las comunicaciones.
A.15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	SI	Se tienen establecidas cláusulas en los contratos firmados con los proveedores.

A.16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**			
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A.16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	Procedimiento de Gestión de Incidentes En los perfiles se tiene establecido que todos los funcionarios deben reportar los diferentes incidentes que se puedan presentar en la organización.
A.16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	SI	Procedimiento de Gestión de Incidentes

A.16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	SI	Procedimiento de Gestión de Incidentes
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	SI	Procedimiento de Gestión de Incidentes
A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI	Procedimiento de Gestión de Incidentes
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	SI	Procedimiento de Gestión de Incidentes
A.16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI	Procedimiento de Gestión de Incidentes
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**			
A.17.1	Continuidad de Seguridad de la información			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	SI	T-S-1 Plan de Continuidad del Negocio
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	SI	T-S-1 Plan de Continuidad del Negocio Falta la Implementación
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	SI	T-S-1 Plan de Continuidad del Negocio Falta las pruebas
A.17.2	Redundancias			

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	T-S-1 Plan de Continuidad del Negocio Se cuenta con redundancia en equipos y no de instalaciones. Diagrama de Red

A.18	**CUMPLIMIENTO**			
A.18.1	Cumplimiento de requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
A.18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	SI	Se cuenta con la Matriz de Verificación de Requisitos Legales de Seguridad de la información. La Organización cumple con los lineamientos y normatividad exigida por el Ministerio de las TIC.
A.18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	SI	Se cuenta con la Matriz de Verificación de Requisitos Legales de Seguridad de la información. La Organización cumple con los lineamientos y normatividad exigida por el Ministerio de las TIC.
A.18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	SI	Cuenta con las tablas de retención documental de acuerdo con las disposiciones del Archivo General de la Nación.
A.18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI	Se cuenta con el documento J-A-3 Política Operacional de Protección de Datos
A.18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak Documento Criptografía Se cuenta con los Procedimientos de Controles Criptográficos

A.18.2	Revisiones de seguridad de la información			
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	SI	Se realizan auditorías, revisión de políticas y procedimientos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak Se cuenta con la Matriz de Verificación de Legalidad
A.18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI	Anualmente se realizan pruebas de Vulnerabilidades Técnicas.

Tabla 3 – Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece
Fuente: Coordinación de TI

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

Se cuenta con la Resolución 147 de 2018 de RTVC, https://s3.amazonaws.com/rtvc-assets-qa-sistemasenal-colombia.gov.co/resolucion_147-2018_mipg.pdf, así como se tienen definidos los roles y responsabilidades en la Política operacional de seguridad y privacidad de la información, disponible en la ruta: https://www.kawak.com.co/RTVC/gst_documental/doc_visualizar.php?v=1208&m=78

7.2.3. Inventario de activos de información

Se cuenta con la Matriz de inventario y clasificación de activos de información, disponible en el link: https://s3.amazonaws.com/rtvc-assets-intranet.rtvc.gov.co/field/fileDocument/Matriz%20Inventario%20y%20Clasificaci%C3%B3n%20de%20Activos%20de%20Informaci%C3%B3n%20RTVC.pdf – ubicada en la intranet de la entidad ruta: https://intranet.rtvc.gov.co/documentos/seguridad-de-la-informaci%C3%B3n.

7.2.4. Integración del MSPI con el Sistema de Gestión documental

Se encuentra alineado al PROCEDIMIENTO GUIA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS ubicado en la intranet de RTVC en el link: https://s3.amazonaws.com/rtvc-assets-intranet.rtvc.gov.co/field/fileDocument/Guia%20para%20la%20Gesti%C3%B3n%20y%20Clasificaci%C3%B3n%20de%20activos%20de%20Informaci%C3%B3n.pdf .

7.2.5. Plan de Capacitación, Sensibilización y Comunicación

Se cuenta con el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación ubicado en la intranet de RTVC en el link: https://s3.amazonaws.com/rtvc-assets-intranet.rtvc.gov.co/field/fileDocument/Plan%20de%20Cambio%20y%20Cultura%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informaci%C3%B3n%2C%20Seguridad%20Digital%20y%20Continuidad%20de%20la%20Operaci%C3%B3n.pdf.

7.2.6. IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS

La figura N° 7, muestra el esquema de identificación, valoración y tratamiento de riesgos relacionados con el Modelo de Seguridad y Privacidad de la Información, alineado con la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital – del Departamento Administrativo de la Función Púbica DAFP y el Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas:

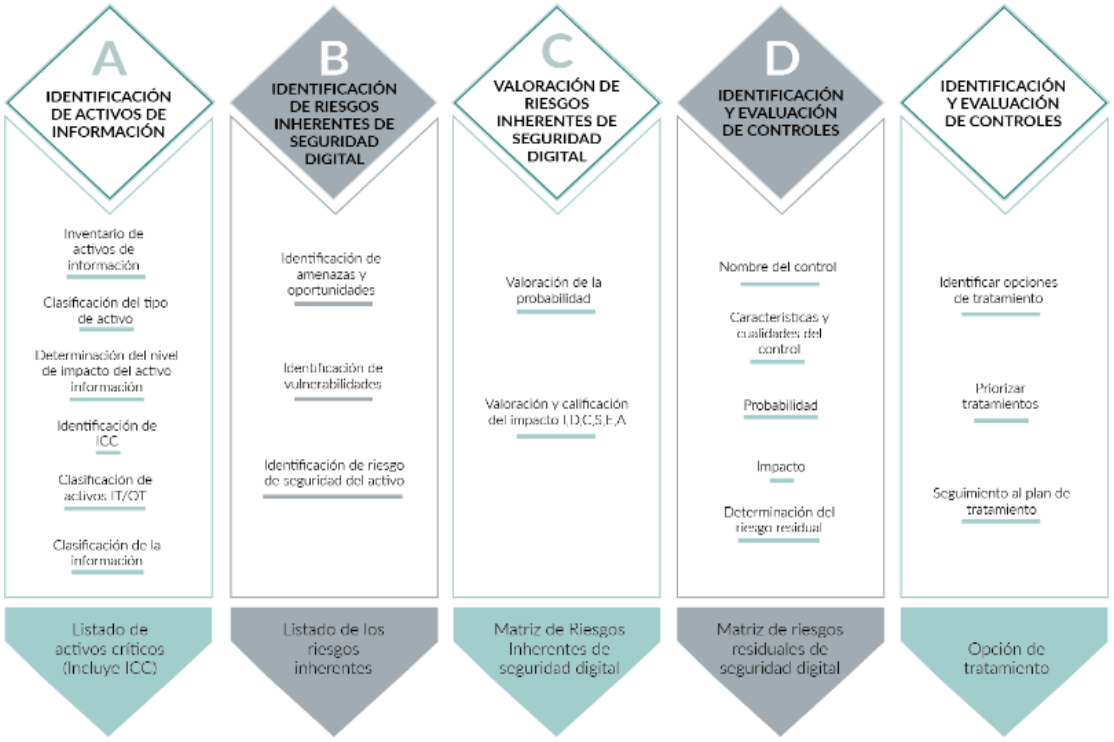

Figura 7. Ejecución de la Gestión de Riesgo de Seguridad Digital
Fuente: Modelo de Gestión de Riesgos de Seguridad Digital Mintic

De acuerdo con el inventario de activos de información, los líderes de procesos deben revisar anualmente los cambios en el direccionamiento estratégico o en el entorno y como estos pueden generar nuevos riesgos de Seguridad y Privacidad de la Información o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de riesgos de su proceso. Así como realizar una revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos, tomando como referencia la tabla de Controles propuesta por el MSPI, producto de lo anterior se generan los planes de acción y el plan de control operacional para la implementación de los controles, y se actualiza la Declaración de Aplicabilidad de la Entidad.

7.3. IMPLEMENTACIÓN

El Modelo de Seguridad y Privacidad de la Información se implementa en cuatro temas principales como son: la planificación, implementación, evaluación del desempeño y mejora continua y a futuro se espera tener un Modelo maduro autónomo y eficiente, donde cada líder de proceso conozca y sepa proteger sus activos de información y llegue al fortalecimiento de los controles de seguridad de la información.

7.3.1. PLANIFICACIÓN Y CONTROL OPERACIONAL

RTVC debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos 2020. Acciones que serán ejecutadas en la vigencia 2020 y 2022, según se definan por los líderes de los procesos, el comité de seguridad y demás responsables.

Se debe tener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomar acciones para mitigar efectos adversos cuando sea necesario.

7.3.2. IMPLEMENTACIÓN DEL CONTROL DE RIESGOS

El plan de tratamiento de riesgos de seguridad de la información debe identificar los controles a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad, en donde la base para ejecutar esta actividad es la Guía No 8 - de controles de seguridad y privacidad del MSPI. En donde la aplicación de los controles sobre los riesgos detectados debe estar aprobada por el responsable de cada proceso. El estado de implementación de los controles se revisará periódicamente y estará alineado a los planes de acción propuestos la revisión y actualización de la matriz de riesgos de seguridad y privacidad de la información

7.3.3. INDICADORES DE GESTIÓN

La tabla N°5, muestra la estructura de los indicadores de gestión definidos para la medición y seguimiento del modelo de seguridad y privacidad de la información:

2019 (Línea Base)	2020	2021	2022
70	74	80	88

Tabla 5. Definición de los indicadores de gestión del modelo y el plan asociado de seguridad y privacidad
Fuente: Coordinación de TI - RTVC

7.4. EVALUACIÓN DE DESEMPEÑO

Se realiza evaluación y monitoreo periódico del modelo con base en los resultados de los indicadores propuestos, a través de los Comité de Seguridad.

Adjunto actas del Comité:

- https://www.kawak.com.co/RTVC/index.php?ref=cnZnX3JldmIzaW9uX2dlcmVuY2lhbC9kcnZfbW9kaWZpY2FyX2FjdGFzLnBocD9vcD1lZGl0JmxsYXZlPTMzMw==

- https://www.kawak.com.co/RTVC/index.php?ref=cnZnX3JldmIzaW9uX2dlcmVuY2lhbC9kcnZfbW9kaWZpY2FyX2FjdGFzLnBocD9vcD1lZGl0JmxsYXZlPTU1Mw==

- https://www.kawak.com.co/RTVC/index.php?ref=cnZnX3JldmIzaW9uX2dlcmVuY2lhbC9kcnZfbW9kaWZpY2FyX2FjdGFzLnBocD9vcD1lZGl0JmxsYXZlPTYxNA==

7.4.1. PLAN DE REVISIÓN Y SEGUIMIENTO A LA IMPLEMENTACIÓN DEL MODELO

ACTIVIDAD	PERIODICIDAD MINIMA DE EJECUCIÓN
Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.	Dos veces al año
Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.	Una vez al año
Seguimiento a la programación y ejecución de las actividades de auto-rías internas y externas del MSPI.	Una vez al año
Seguimiento al alcance y a la implementación del MSPI.	Dos veces al año
Seguimiento a los registros de acciones y eventos / incidentes que po-drían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.	Trimestralmente
Medición de los indicadores de gestión del MSPI	Cuatrimestralmente
Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)	Una vez al año

Tabla 5. Plan de Revisión y seguimiento a la implementación del Modelo
Fuente: Coordinación de TI

7.4.2. PLAN DE EJECUCIÓN DE AUDITORÍAS

Auditorías Internas: El plan de ejecución de auditorías se origina en el Programa Anual de Auditorías de Control Interno y/o el programa de auditorías internas de calidad.

7.5. PLAN DE MEJORA CONTINUA

Las acciones de mejora (acciones preventivas, correctivas y/o de mejora) correspondientes a las auditorías realizadas a la implementación del MSPI, son tratadas de acuerdo con el Proceso de Mejora Continua y son documentadas en el módulo Mejoramiento Continuo del Sistema de Planeación y Gestión Kawak (https://www.kawak.com.co/senalcolombia).

8. REFERENCIAS Y DOCUMENTOS ASOCIADOS

- **Modelo integrado de planeación y gestión**. Departamento Administrativo de Planeación Nacional
- **Estrategia de gobierno digital**. Ministerio de Tecnologías de la Información y las Comunicaciones
- **Plan de tratamiento de riesgos de seguridad y privacidad de la información**. Decreto 612 de 2018 – Departamento Administrativo de la Función Pública - DAFP.
- **Plan de seguridad y privacidad de la información**. Decreto 612 de 2018 – Departamento Administrativo de la Función Pública - DAFP
- **Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública - DAFP - Riesgos de gestión, corrupción y seguridad digital** - Versión 4 –

INFOGRAFÍAS:

- Modelo de Gestión de Riesgos de Seguridad Digital Mintic: https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b?version=1.0
- Herramienta de Autodiagnóstico del MSPI Modelo de Seguridad y privacidad de la Información: https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx