INSTITUTO MINICIPAL DE CULTURA DE YUMBO

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - VIGENCIA 2024

EQUIPO COLABORADOR

GESTIÓN DE DIRECCIÓN Y PLANEACIÓN
MANTENIMIENTO Y ADMINISTRACIÓN DE BIENES

ENERO 31 DE 2024

1 CONTENIDO

1. INTRODUCCIÓN

El Instituto Municipal de Cultura de Yumbo -IMCY- (en adelante la Entidad), presenta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (en adelante PTRSPI), la cual, operará en conjunto con el Plan de Seguridad y Privacidad de la Información (PSPI) acorde a la disponibilidad de recursos y capacidad institucional de la entidad.

La Política de Gobierno Digital y Seguridad Digital son fundamentales para la transformación empresarial y digital de la Entidad, la seguridad de la información es parte esencial para el logro de los objetivos institucionales y conservar la confidencialidad, integridad y disponibilidad de sus activos de información.

En el Ciberespacio y Entornos Digitales crece la participación de los ciudadanos y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) llevando a tener una alta dependencia de Infraestructuras Digitales.

Las Infraestructuras Digitales traen consigo una serie de riesgos relacionados con la seguridad digital. Tanto así que, los incidentes de seguridad cada vez son más frecuentes debido a vulnerabilidades o amenazas con mayor complejidad y experticia por sus autores, generando graves consecuencias económicas, sociales o reputacional, conllevando hacia la desconfianza digital y desaceleración del desarrollo en el futuro digital.

El PTRSPI en mención, se enfoca en dos planteamientos; por un lado, continuar desarrollando la operación de la Entidad velando por mantener condiciones adecuadas de seguridad informática, y para la continuidad de la operación y del negocio de manera recursiva acorde con la capacidad institucional. Y por otro lado, abonando recurrentemente y de manera sostenida con la evolución metodológica de los modelos (MSPI, MGRSD) que permita mejorar la cultura de seguridad, con el gobierno y la gestión de la seguridad de la información y ciberseguridad hasta su completitud.

2. OBJETIVO GENERAL

Disminuir la probabilidad de Riesgos de Seguridad y Privacidad de la Información que puedan afectar la entidad para proporcionar mayor seguridad y confianza sobre la información utilizada en la toma de decisiones y la planificación institucional orientada a mejorar la prestación de sus servicios y generación de valor público, mediante la implementación de la metodología para la administración del riesgo puesta a disposición por el Departamento Administrativo de la Función Pública -DAFP- y fundamentada en la Política de Administración del Riesgo, Identificación y Valoración del Riesgo.

2.1 OBJETIVOS ESPECÍFICOS

1) Complementar mapa de riesgos de la seguridad de la información
2) Monitorear los controles implementados para los riesgos identificados y valorizados
3) Cerrar progresivamente brechas de seguridad de la información

3. ALCANCE

El alcance contempla continuidad del desarrollo de la operación actual del área de sistemas. Incluye la implementación de controles priorizados respecto a los siguientes dominios definidos en la norma ISO 27001:2013, con progresividad y transición a la ISO 27001:2022; según aplique, sea pertinente y acorde con la disponibilidad de recursos de la entidad

1) Políticas de seguridad.
2) Aspectos organizativos de la seguridad de la información
3) Seguridad ligada a los recursos humanos.
4) Gestión de activos.
5) Control de accesos.
6) Cifrado.
7) Seguridad física y ambiental.
8) Seguridad en la operativa.
9) Seguridad en las telecomunicaciones.
10) Adquisición, desarrollo y mantenimiento de los sistemas de información.
11) Relaciones con proveedores
12) Gestión de incidentes en la seguridad de la información.
13) Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
14) Cumplimiento

De igual manera, busca una evaluación integral de las amenazas que enfrenta la entidad y las vulnerabilidades de su entorno operativo actual en el ciberespacio con enfoque para la implementación de controles para la ciberseguridad, por lo cual se incorpora la gestión hacia controles relacionados con el ciberespacio, como son:

1) Controles a nivel de aplicación
2) Protección del servidor
3) Controles del usuario final
4) Controles contra ataques de ingeniería social

4. NORMATIVIDAD

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información -PTRSPI-, soporta su revisión de normas concordantes y complementarias en el cumplimiento normativo aplicable a:

- Plan de acción de la entidad para la misma vigencia
- Decreto 612[1] del 2018 "*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*".
- Artículo 2.2.22.3.14 del Decreto 1083 del 2015, Decreto Único Reglamentario del Sector de Función Pública que señala **Integración de los planes institucionales y estratégicos al Plan de Acción**. *"Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año".*

  (…)

  12. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

  (…)
- Artículo 74 de la Ley 1474 de 2011, *"Plan de acción de las entidades públicas".*

LEYES	
Ley 2294 del 2023	Por el cual se expide el Plan Nacional de Desarrollo 2022-2026 "Colombia Potencia Mundial de la Vida".
Ley 1955 del 2019	Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pactopor Colombia, Pacto por la Equidad".
Ley 1978 de 2019	Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea unRegulador Único y se dictan otras disposiciones.
Ley 1757 de 2015	Por la cual se dictan disposiciones en materia de promoción y protección del derecho a la participación democrática.

[1] Fuente: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85742

Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018"TODOS POR UN NUEVO PAIS" "Por medio de la cual se crea la Leyde Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección dedatos personales.
Ley 19 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y laefectividad del control de la gestión pública
Ley 1341 de 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la informacióny de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otrasdisposiciones

DECRETOS	
Decreto 767 de 2022	Lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 338 de 2022	Lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital
Decreto 88 de 2022	Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
Decreto 1287 de 2020	Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el

	trabajo en casa, en el marco de la Emergencia Sanitaria.
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de servicios ciudadanos digitales
Decreto 2106 de 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de lasentidades del Estado
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector dela Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones y se dan Lineamientos Generales de la Estrategia de Gobierno en Línea.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictanotras disposiciones.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto 333 de 2014	Define el régimen de acreditación de las entidades de certificación, aplicable a personas jurídicas, públicas y privadas
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 1510 de 2013	Por el cual se reglamenta el sistema de compras y contratación pública
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otrasdisposiciones.
Decreto 2482 de 2012	Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión (Ley 489 de 1998, Ley 552 de1994).

DIRECTIVAS	
Directiva 26 de 2020	Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.
Directiva 03 de 2019	Lineamientos para la definición de la estrategia institucional de comunicaciones, objetivos y contenidos de las entidades de la rama ejecutiva del orden nacional
Directiva 02 de 2000	Plan de Acción de la estrategia de Gobierno en Línea.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL	
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital
CONPES 3975 de 2019	Política Nacional de Transformación Digital e Inteligencia Artificial.
CONPES 3920 de 2018	Política Nacional de Explotación de Datos (BIG DATA)
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y ciberdefensa
CONPES 3292 de 2004	Política Nacional Realización y Automatización de Tramites
CONPES 3248 de 2003	Renovación de la administración pública

RESOLUCIONES	
MINTIC, Resolución 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información (MSPI) y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
MINTIC, Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
MINTIC, Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
DAFP, Guía de 2020	Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas (Riesgos de Gestión, Corrupción y Seguridad Digital) Versión 5

5. RESPONSABILIDAD Y AUTORIDAD

La Autoridad del presente plan es el gerente de la Entidad o quién ejerza el rol de representante legal, y/o, a través de quién ejerce el rol del profesional apoyo al área de sistemas.

6. DEFINICIONES

Aplican las definiciones contenidas en el "Glosario" referido en el capítulo 4. del Modelo Nacional de Gestión de Riesgos de Seguridad Digital del Estado Colombiano –MGRSD-, páginas 17 a 31., que puede ser consultado en el siguiente enlace: https://n9.cl/sb675

7. POLITICA DE ADMINISTRACIÓN DE RIESGOS

La entidad se compromete a mantener una cultura de la gestión del riesgo asociado con la responsabilidad de diseñar, adoptar y promover política y planes regulando los riesgos de los procesos y proyectos, utilizando mecanismos y controles necesarios para la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y eficiencia a lo largo del ciclo de la vida para optimizar de manera continua y oportuna la respuesta a los riesgos de seguridad y privacidad de la información y seguridad digital de manera integra.

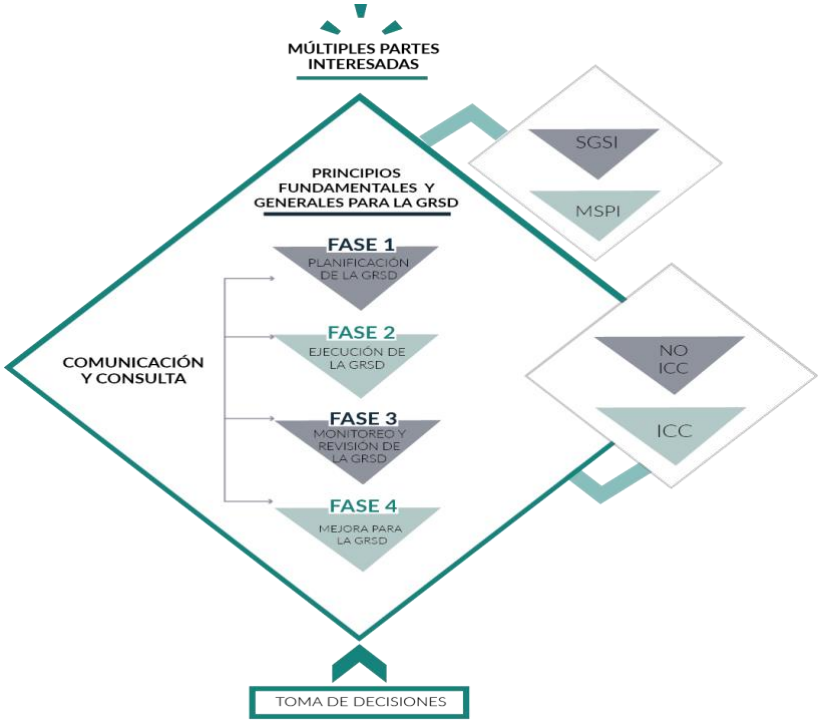
7. DESARROLLO

7.1 MARCO CONCEPTUAL DEL MGRSD

El marco conceptual del Modelo de Gestión de Riesgos de Seguridad Digital (MGSD) provee una guía para la implementación de gestión de riesgos de seguridad digital basado en principios generales y fundamentales donde se establece una interacción con los Sistemas de Gestión de la Seguridad de la Información (SGSI) o para el caso de las entidades del sector público colombiano con el Modelo de Privacidad y Seguridad de la Información (MPSI); así como la relación con los activos de información que soportan la operación de cualquier Entidad se interrelacionan con el MGRSD en todas sus fases o componentes.[2]

[2] https://mintic.gov.co/portal/715/articles-61854_documento.docx

Ilustración 1: 8.1 MARCO CONCEPTUAL DEL MGRSD



Fuente: MinTIC

7.2 SITUACION ACTUAL

El tratamiento de riesgos de seguridad digital se mantiene con las acciones concebidas por la gestión de operaciones TI en la Entidad por parte del área de sistemas.

7.3 RIESGOS

A continuación, descripción de los riesgos identificados y valorados con controles implementados y monitoreados, quedando la tarea de seguir revisando y actualizando en la presente vigencia.

7.3.1 RIESGOS DE GESTIÓN

Riesgo	Descripción del riesgo	Causa	Consecuencia	Controles existentes
Posibilidad de apagarse repentinamente los equipos de cómputo por suspensión del suministro de energía eléctrica debido a Sobretensiones Eléctricas de forma transitoria o permanente	Aumento de voltaje o elevación inusual de la tensión de la corriente eléctrica de forma transitoria o permanente con un valor superior al valor nominal de la red eléctrica	**1) Ausencia Sistemas Energía de Emergencia:** Ausencia de un sistema de energía de emergencia (UPS y/o Planta) que, garantice el suministro sin interrupciones de energía eléctrica **2) Ausencia Sistemas de Protección Eléctrica:** Ausencia de dispositivos dedicados a la protección de las instalaciones eléctricas contra cortocircuitos, sobrecargas y electrocución. **3) Descargas Atmosféricas:** Propagadas por sobretensiones conducidas (rayos) o sobretensiones inducidas (campos electromagnéticos)	1.) Interrupción funcionamiento de los equipos de cómputo, provocando fallas o daños en los equipos 2.) Interrupción de los servicios tecnológicos implementados a través del uso de los equipos de cómputo. 3.) Pérdida de información accidentalmente almacenada en los equipos de cómputo	La entidad mantendrá el suministro de energía de emergencia a los equipos de cómputo a través de un equipo UPS o Sistema de alimentación ininterrumpida

		4) Sobretensiones de Conmutación: Generadas por la conexión y desconexión de dispositivos electrónicos de gran potencia y por maniobras o defectos en el suministro eléctrico. **5) Suspensión Servicio de Energía Eléctrica:** Suspensión o daño en un componente del servicio de energía eléctrica contratado con el proveedor		

7.3.2 RIESGOS DE CORRUPCIÓN

Riesgo	Descripción del riesgo	Causa	Consecuencia	Controles existentes
Posibilidad de pérdida de información por incidentes de seguridad debido a vulnerabilidades o amenazas	Es importante distinguir entre una fuga y la pérdida de información. La fuga se lleva a cabo de forma intencional, mientras que la pérdida es accidental. Sin	1) Gobierno y gestión inadecuada de la información 2) Ausencia de roles y responsables con las competencias	1) Pérdida de disponibilidad de la información frente al logro de objetivos y la misión institucional. 2) Sobreesfuerzos	El área de sistemas realizará copias de seguridad a las bases de datos de las aplicaciones de los Sistemas de información.

	embargo, es importante mencionar que también podrían existir pérdidas de información intencionales (Un empleado que borra una base de datos) y fugas accidentales (si se envía un correo electrónico con información sensible a un destinatario erróneo). Quizá la diferencia radica en que una fuga implica que la información pueda ser accedida por personas o entidades sin los privilegios para hacerlo (divulgación), mientras que la pérdida de información no necesariamente se puede relacionar con la fuga o filtración, ya que esta puede dañarse (modificación, destrucción o interrupción) sin necesidad de que un agente interno o externo pueda	en seguridad informática 3) Altos volúmenes de información con operación manual 4) Acceso no autorizado a la información sensible y crítica de la entidad	para el tratamiento de la información que permita mayores posibilidades a la Entidad para la estrategia, la operación y la entrega de valor de manera oportuna. 3) Pérdida de control de la información con acceso indiscriminado generando amenazas de demanda para la entidad y ante terceros	La entidad contratará Soporte y Actualizaciones a las aplicaciones de los Sistemas de información

	acceder a ella. También es relevante identificar al actor que materializa un riesgo sobre la información, sobre todo porque ya sea una pérdida, fuga o filtración de información puede ser debida a un agente interno o externo. A decir verdad, existen un sin número de escenarios posibles en los cuales se pueden presentar los incidentes de seguridad, debidos a amenazas o vulnerabilidades que, podrían interrumpir el uso de los servicios tecnológicos desde un usuario hasta toda la entidad			

7.3.3 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Código	Riesgo	Activo	Tipo Activo	Amenazas	Descripción del riesgo	Causa	Consecuencia	Controles existentes

R-GT-01	Pérdida de la Integridad	Bases de datos de los Sistemas de Información	Información	Bases de datos sin copias de respaldo	Pérdida de información de las bases de datos de los sistemas de información debido a no realizar copias de respaldo	Realizar copias de respaldo guardándolas en un solo sitio, quedando dependiendo de un solo dispositivo de almacenamiento y/o alternativa de recuperación cuando sea requerido, pudiendo presentar averías o anomalías Ausencia de un sistema automático que, realice y almacene copias de respaldo en diferentes sitios	Parada de las operaciones del negocio Manualmente desarrollar los procesos de información retrasando las operaciones del negocio	El área de sistemas realizará copias de seguridad de las bases de datos de los sistemas de información
R-GT-02	Pérdida de la Disponibilidad	Aplicaciones de los Sistemas de Información	Software	Aplicaciones sin soporte y actualizaciones	Pérdida de disponibilidad de las aplicaciones debido a falta de soporte y actualizaciones que se requieran para el buen funcionamiento de las mismas	Demora en el desarrollo o aprobación proceso de contratación de soporte y actualizaciones para las aplicaciones de los sistemas de información	Retraso en el desarrollo de los procesos de información Parada de las operaciones del negocio	La entidad contratará Soporte y Actualizaciones a las aplicaciones de los Sistemas de información

8. ACTIVIDADES DEL PLAN

A continuación, las actividades definidas para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

El avance estará supeditado al apalancamiento y la capacidad institucional, ante lo cual se revisará la priorización y su implementación procederá acorde con las necesidades institucionales bajo principios de gradualidad, proporcionalidad y disponibilidad de recursos específicos.

ID	Actividad	Responsables	Fecha
01	Respaldar copias de seguridad de la información en un dispositivo de almacenamiento interno y externo de la entidad.	Área de sistemas.	2024
02	Realizar mantenimiento Preventivo a equipo UPS del IMCY, encargado de suministrar energía regulada a los equipos de cómputo	Líderes de procesos, Área de sistemas.	2024
03	Contratar asistencia técnica y actualizaciones a las aplicaciones de los sistemas de información	Líderes de procesos, Área de sistemas.	2024

9. PLAN DE COMUNICACIONES

El presente plan será socializado a la comunidad e interesados, mediante publicación en el sitio web de la entidad: www.imcy.gov.co

10. EVALUACIÓN

La evaluación del presente plan se realizará de acuerdo a las acciones establecidas dentro del mismo y con base en ellas se realizarán las mejoras necesarias para cumplir con el ciclo PHVA.

JOHN SEBASTIÁN ECHEVERRI COLLAZOS
GERENTE

Reviso y aprobó: Comité de Gestión y Desempeño
Elaboró: Equipo de trabajo Planeación y Mantenimiento y Administración de Bienes.