INSTITUTO MUNICIPAL DE REFORMA URBANA Y DE VIVIENDA DE INTERES SOCIAL DE YUMBO - IMVIYUMBO

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

2023

Dirección Administrativa y Financiera
23-1-2023

CONTENIDO

1. PRESENTACIÓN

Se adopta en el Instituto el presente Plan, como un instrumento de Gerencia Pública, para fortalecer la gestión del componente de Gobierno Digital, La seguridad digital y un uso acertado de la información, que permita prevalecer la Estrategia en seguridad y privacidad de la información; en tanto que se constituye como un patrimonio de la gestión pública del Instituto y del ente territorial en su conjunto.

El Instituto, durante la presente vigencia ha continuado con el proceso de integración de sus modelos de gestión y de control, en el marco del Modelo MIPG. Con ese propósito se adoptó por la Gerencia la Resolución No 115 de 2018, por medio la Cual se conformó el Comité Institucional de Gestión y Desempeño. Esa Instancia colegiada ha adoptado un cronograma propio para armonizar progresivamente los diferentes elementos de la gestión municipal. El presente plan, como herramienta de la gestión Pública del Instituto municipal, hace parte del proceso de implementación del Modelo Integrado de Planeación y Gestión MIPG, por lo que progresivamente se incorporará – en lo que corresponde – a las políticas de riesgos institucionales propios del Sistema de Control Interno (15), Transparencia y acceso a la información (5) y a las políticas de Gobierno digital (11) y seguridad digital (12).

Adicionalmente, en los términos de lo señalado en el artículo 133 de la ley 1753 de 2015, el Instituto fortalecerá el proceso de formulación de un manual Institucional de riesgos de la Entidad, que incorpore el presente Plan a la política institucional de prevención de otros riesgos propios de la gestión Pública, tales como los riesgos asociados a la gestión por procesos, los riesgos asociados con la corrupción, los que correspondan a los procesos de gestión contractual, los que se presenten en la gestión del talento humano del Instituto, los que amenacen la consumación de riesgos anti jurídicos en la Entidad, los que resultaren del uso de la información y las tecnologías, e incluso los propios de la prevención de riesgos de desastres en el entorno de la labores administrativas o misionales de la Entidad.

Con el desarrollo de este plan se permitirá la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos, dando a conocer aquellas situaciones que puedan comprometer en cumplimiento de los objetivos trazados por la entidad y de esta manera reducir la afectación o impacto de su materialización.

2. MARCO TEÓRICO

Sin perjuicio de otras definiciones o referentes conceptuales, técnicos o normativos que El Instituto adopte en otros instrumentos similares de gestión; el marco teórico que sirve de referencia para el presente plan es el siguiente, con carácter interpretativo para los destinatarios, usuarios y líderes que los procesos a que se hace referencia:

- 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. (Ley 1712 de 2014, art 4).
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.
- 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. (Ley 594 de 2000, art 3)
- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701)
- Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas

concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- Datos Abiertos: Todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6
- Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- 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 ISO 27001. (ISO/IEC 27000).
- 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 (Jurisprudencia Corte Constitucional).
- 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. (Ley 1581 de 2012, art 3)

- Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular, privado o mixto de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- Plan de continuidad de Gestión: Plan orientado a permitir la continuación de las principales funciones misionales o de la actividad pública del Instituto, en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- 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.
- 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. (Ley 1581 de 2012, art 3).
- Riesgo: 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. (ISO/IEC 27000).
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos

interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- 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. (ISO/IEC 27000).

3. OBJETIVOS

3.1. Objetivo General:

Implementar acciones de gestión Pública que le permitan a la Alta Dirección del Instituto Identificar, evaluar, priorizar, controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en IMVIYUMBO con el fin de salvaguardar los activos de información, el manejo de medios, el control de acceso y la gestión de los diferentes usuarios internos y externos de la Entidad.

3.2. Objetivos Específicos:

a. Conformar un equipo, liderado por la Alta Dirección del Instituto, que formule, adopte y desarrolle el presente Plan.
b. Optimizar los recursos con los que se cuentan actualmente en IMVIYUMBO para implementar el plan de tratamiento de riesgo de seguridad y privacidad de la información.
c. Aplicar los instructivos del DAFP y las metodologías ISO, respectivamente, en seguridad y riesgo de la información en la gestión Pública de la Entidad.
d. Incorporar progresivamente las actividades del presente instrumento de gestión al Plan Institucional de riesgos de la Entidad descentralizada del orden territorial y de la entidad municipio de Yumbo en general.

4. RECURSOS INSTITUCIONAL PARA LA IMPLEMENTACIÓN DEL PLAN

- Humano: Gerente, Líderes del Proceso, Profesionales contratistas.
- Tecnología: Servidores y software para salvaguardar la información.
- Físico: Firewall, equipos de cómputo y de comunicación.
- Financieros: Recursos financieros para la implementación.

5. RESPONSABLES DE LA IMPLEMENTACIÓN INTEGRAL DEL PLAN

En los términos de la resolución Interna No 115 de 2018, la Gerencia del Instituto, en su calidad de Líder del Comité Institucional de Gestión y Desempeño - MIPG designará mediante actas y cronograma las labores y competencias para el cumplimiento de los propósitos del presente Plan.

Corresponde a la dependencia asesora de Control Interno diseñar e implementar acciones de seguimiento y control al plan de trabajo que se adopte, formulando las recomendaciones, advertencias o planes correctivos a que hubiere lugar.

6. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en IMVIYUMBO la gestión de riesgos de seguridad de la información deberá ser interactiva para las actividades de valoración de riesgos y/o tratamiento de estos y se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitido De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

7. ACTIVIDADES

1. Realizar Diagnóstico.
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
3. Realizar la Identificación de los Riesgos con los líderes del Proceso.
3.1. Entrevistar con los líderes del Proceso.
4. Valorar del riesgo y del riesgo residual.
5. Realizar Mapas donde se ubican los riesgos.
6. Formular concertadamente el plan de tratamiento de riesgos.

8. CRITERIOS DE EVALUACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Se desarrollarán criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización teniendo en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información en la Entidad
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de IMVIYUMBO.

8.1 CRITERIOS DE IMPACTO

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para IMVIYUMBO, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados.
- Vulnerabilidad en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a usuario del sistema)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

8.2 CRITERIOS DE ACEPTACIÓN

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos del IMVIYUMBO y de las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información son directamente proporcionales al daño o afectación que le pueda ocurrir a la información.

8.3 IDENTIFICACIÓN DE RIESGOS

Para la evaluación de riesgos de seguridad de la información es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos.

Clasificación de activos:

1. Primarios:
a. Procesos y actividades del Negocio
b. Información

2. Soporte:
a. Hardware
b. Software
c. Redes
d. Personal
e. Sitio
f. Estructura organizativa

8.4 ANÁLISIS DE RIESGOS

IMVIYUMBO documentará y especificará cada una de las etapas surtidas para el proceso de Gestión de Riesgos, así tener una guía para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria.

8.5 ESTIMACIÓN DEL RIESGO

Establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- Probabilidad
- Impacto

PROBABILIDAD DEL RIESGO			
Concepto	**Nivel**	**Criterios de factibilidad**	Criterios de frecuencia
Raro	1	El evento puede ocurrir sólo en circunstancias Excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Pudo ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
Posible	3	Podría ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos 1 vez en el año
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias	Más de una vez al año

IMPACTO DEL RIESGO			
Nivel	**Descriptor**	**Descripción**	**Criterios de frecuencia**
5	Insignificante	Si se presenta tendría consecuencias mínimas sobre la entidad	Más de una vez al año
10	Menor	Si se presenta tendría bajo impacto sobre la entidad	Al menos 1 vez en el año
15	Moderado	Si se presenta tendría mediana consecuencia sobre la entidad	Al menos 1 vez en los últimos 2 años
20	Mayor	Si se presenta tendría una alta consecuencia sobre la entidad	Al menos 1 vez en los últimos 5 años
25	Catastrófico	Si se presenta tendría desastrosa consecuencia sobre la entidad	No se ha presentado en los últimos 5 años

8.6 EVALUACIÓN DEL RIESGO

Esta se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”, con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente tabla:

PROBABILIBAD	IMPACTO				
	Insignificante (5)	Menor (10)	Moderado (15)	Mayor (20)	Catastrófico (25)
Raro (1)	5	10	15	20	25
Improbable (2)	10	20	30	40	50
Posible (3)	15	30	45	60	75
Probable (4)	20	40	60	80	100
Casi Seguro (5)	25	50	75	100	125

Zona de riesgo baja: Asumir el riego
Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo
Zona de riesgo alta: Reducir el riesgo, evitar, compartir o trasferir
Zona de riesgo extremo: Reducir el riesgo, evitar, compartir o trasferir

8.7 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

COSTO - BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o aceptar** el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

8.8 MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración interactiva de los riesgos de seguridad de la información.

9. CUMPLIMIENTO DE IMPLEMENTACIÓN

En los términos de las etapas antes precisadas; señalamos los componentes describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por IMVIYUMBO.

a. Revisión y actualización de la actual Política de Seguridad.
b. Actualizar componentes organizativos de la seguridad de la información
c. Evaluar la seguridad que está ligada a los recursos humanos.
d. Revisión del Control de acceso.
e. Implementación del componente de seguridad operativa.
f. Implementación de componente de seguridad en las telecomunicaciones.
g. Evaluación, registro y seguimiento de gestión de Incidentes de Seguridad de la Información.
h. Implementación progresiva del plan operativo para fortalecer la seguridad de la información en la gestión de labores de IMVIYUMBO.

10. CRONOGRAMA PARA DESARROLLAR EL PLAN DE ACCIÓN

Actividades	Mes1	Mes2	Mes 3	Mes4	Mes5	Mes6	Mes7	Mes8	Mes9	Mes10	Mes11	Mes12
Realizar Diagnóstico												
Formular Alcance del Plan												
Identificación de riesgos												
Valoración concertada de riesgos												
Valoración riesgo residual												
Mapa de tratamiento de riesgos												
Seguimiento y control												

11. SEGUIMIENTO Y EVALUACIÓN

En cumplimiento de las funciones propias del sistema de Control Interno, la Gerencia de la Entidad incluirá en el plan anual de auditorías los seguimientos propios al correspondiente Plan. En los términos de la resolución Interna No 115 de 2018, se realizará un cronograma propio para revisar los diferentes mapas de riesgos y los planes de gestión que pretender mitigarlos o controlarlos, en lo que corresponda.

12. INTEGRACIÓN CON OTROS INSTRUMENTOS DE GESTIÓN

El presente plan hace parte del proceso de implementación del Modelo Integrado de Planeación y Gestión MIPG, por lo que progresivamente se incorporará – en lo que corresponde – a las políticas de riesgos institucionales propios del Sistema de Control Interno (15), Transparencia y acceso a la información (5) y a las políticas de Gobierno digital (11) y seguridad digital (12).
Adicionalmente, en los términos de lo señalado en el artículo 133 de la ley 1753 de 2015, el Instituto fortalecerá el proceso de formulación de un manual Institucional de riesgos de la Entidad, que incorpore el presente Plan a la política institucional de prevención de otros riesgos propios de la gestión Pública.

13. ENTREGABLES DEL PROCESO

- Plan anual de acción para la implementación.
- Informe de avance o resumen ejecutivo del líder del proceso.
- Acta de Reunión.
- Plan de tratamiento de riesgo aprobado por los líderes
- Política de Seguridad
- Productos de cada etapa
- Plan anual de auditoria que incluye el presente instrumento de gestión.

FIN DE DOCUMENTO

RUTA DE APROBACIÓN VERSION 4					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Milton Marino Pulido Dávila	Nombre	José Arles Narváez Álvarez	Nombre	Uriel Urbano Urbano
Cargo	Profesional de apoyo gestión de tecnologías (contratista)	Cargo	Director Administrativo y Financiero	Cargo	Gerente

ANEXO

a). Control de Cambios: *Nota: Los documentos obsoletos se les da de baja del Sistema Integrado de Gestión Institucional.*

Versión	Fecha (dd/mm/aa)	Aprobado por:	Descripción de la actualización
1	29/06/2018	Gilma Mancilla Angulo (Gerente)	Creación del Documento.
2	02/03/2020	Uriel Urbano Urbano (Gerente)	Actualización de logo e imagen corporativa.
3	04/05/2021	Uriel Urbano Urbano (Gerente)	Cambio de código en el Sistema Integrado de Gestión Institucional, a causa de la creación del Proceso Gestión de Tecnologías.
4	23/01/2023	Uriel Urbano Urbano (Gerente)	Actualización vigencia 2023.