PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2022

INSTITUTO MUNICIPAL DE LA REFORMA URBANA Y VIVIENDA DE PASTO

SANDRA PATRICIA BRAVO LARRAÑAGA
Directora Ejecutiva

Historial de revisión

Fecha	Versión	Descripción	Autor
31/01/2022	1.0	Creación del documento	Ing. Fabio Vallejo

Elaboró:	Reviso´:	Aprobó:
FABIO VALLEJO ING DE SISTEMAS		

Contenido

1. INTRODUCCIÓN

INVIPASTO, en busca de la mejora continua de la mano de la estrategia de gobierno digital, implementa el modelo de seguridad y privacidad de la información propuesto por el MINTIC que permitirá identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados en cuanto al manejo de la información institucional, con el fin de que no afecten los diferentes procesos del instituto y pueden continuar su operación.

Centro Administrativo Municipal – CAM Anganoy Barrio los Rosales II Tel. 7222330 – 3207262361
Correo Electrónico: secretariaejecutiva@invipasto.gov.co
contactenos@invipasto.gov.co

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Implementar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, que permita la guía para el control y minimización de los de los riesgos y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas directa e indirectamente con la información del Instituto.

2.2. OBJETIVOS ESPECÍFICOS

- Identificar un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información
- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y MINTIC para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Optimización de los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

3. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos del Instituto los cuales manejen, procesen o interactúen con información institucional.

4. MARCO CONCEPTUAL

- 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).
- 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.

- 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).

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

- Ciberespacio: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española). 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.

- 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).

- 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).

- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- 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 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).

- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

5. MARCO NORMATIVO

- Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública

- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública

- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública

- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales

- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad

- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.

- Decreto 1008 de 2018 Por el cual se establecen los lineamientos generales de a 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.

- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información
- Modelo de Seguridad y privacidad de la información – MSPI

6. DESCRIPCIÓN DEL PLAN

Identificación del riesgo:

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas recolectan datos de entrada para esta actividad.

Categorías de riesgos:

ET: Estratégicos: Relacionados a lineamientos, políticas, estrategias o directrices no adecuadas o no convenientes para el instituto.

OP: Operativo: Relacionado a procesos, conductas o actividades inapropiadas, contrarias al deber ser o que presente una posible brecha frente a la calidad esperada.

FA: Financiero: Relacionado con la asignación, suficiencia o recaudo de recursos económicos que puedan afectar a corto, mediano o largo plazo financieramente a los procesos o el instituto.

TEC: Tecnológico: Relacionado al uso, manejo o disposición de equipos de cómputo y periféricos.

Identificación de riesgos:

Normalmente se identifican los riesgos como eventos o situaciones no deseadas que se pretenden evitar, por tal razón la identificación de riesgos inicia con términos como: Ausencia, No adherencia, Inadecuada, No suficiencia, entre otros.

Una vez se identifique el riesgo, debe complementarse para obtener el contexto del riesgo, ya que éste puede presentarse en un área, en un horario, por parte de un grupo de colaboradores, o en unas circunstancias específicas que ayudarán más adelante a determinar las acciones a tomar. Estos son algunos ejemplos de preposiciones a utilizar: al, durante, en, sobre, con, hacia, de, mediante, entre otros.

Descripción de Causas:

Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso.

Consecuencias:

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Perdidas económicas, Perjuicio de la imagen, Sanciones legales, Demoras, Insatisfacción, entre otras.

Barreras de Seguridad Existentes:

Se describen los controles implementados o barreras que existen actualmente para evitar la materialización del riesgo, se pueden encontrar en los protocolos o procedimientos documentados, en las guías de reacción inmediata o en los documentos de buenas prácticas de seguridad.

Valoración del Riesgo:

Se mide en cuanto a probabilidad e impacto para obtener un dato cuantitativo que permita su comparación y priorización.

Tratamiento y Seguimiento del Riesgo:

Se describen los controles o barreras a ser implementadas para fortalecer las existentes, con lo cual aportar y evitar la materialización del riesgo desde la reducción

de la probabilidad y/o del impacto. Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones realizadas, fortalecimiento de buenas prácticas de seguridad, asesorías con expertos, entre otras.

Un aspecto de gran importancia es la definición de indicadores para determinar el impacto de las acciones realizadas, ya que no es suficiente cumplir las actividades propuestas sino también valorar como estas acciones permiten disminuir la probabilidad de ocurrencia o nivel de impacto del riesgo; con el fin de medir la efectividad de las acciones para la mitigación del riesgo.

7. IDENTIFICACION, VALORACION Y SEGUIMIENTO DE RIESGO POR PROCESOS.

				ANALISIS DEL RIESGO			VALORACION INICIAL DEL RIESGO				TRATAMIENTO Y SEGUIMIENTO DEL RIESGO						
	N°	IDENTIFICACION DE RIESGOS	FECHA DE IDENTIFICACION DE RIESGO	CAUSAS	CONSECUENCIAS	BARRERAS DE SEGURIDAD EXISTENTES	VALOR DE PROBABILIDAD	VALOR DE IMPACTO	NIVEL DEL RIESGO	BARRERAS DE SEGURIDAD A IMPLEMENTAR	RESPONSABLE DEL SEGUIMIENTO	INDICADOR	LINEA BASE	META	RESULTADOS DE EFECTIVIDAD DE LAS ACCIONES (Planeación)	VALORACION DEL RIESGO DESPUES DE CONTROLES (Control Interno)
TEC	1	Perdida de información por alteraciones en el sistema o inconvenientes en equipos de cómputo o servidores, fluido eléctrico	01/2022	Daño en hardware y software especializado redes: daño en swicth daño físico y lógico de los equipos de computo. Intrusión Malware (virus informáticos, gusanos, troyanos, spyware, hardware) Caídas y variaciones en el fluido eléctrico obsolescencia tecnológica	Perdida de información administrativa y asistencial física o magnética Perdidas económicas -Sanciónales Legales - Afectación de las operaciones en los procesos de entidad	-Realizar copias de seguridad a los computadores que necesiten guardar la información -Procesos de custodia de documentos de archivo de gestión central se dispone de una persona encargada del manejo de las TICS Antivirus instalado en cada equipo de computo	3 moderado	4 Mayor	Extremo	-Aplicación permanente de los controles existentes para la gestión Seguridad y privacidad de la información - Cronograma de mantenimiento preventivo y correctivo de computadores y equipo de redes de datos. - Adquirir sistema de regulación y resguardo de fluido eléctrico -Adquirir equipos o hardware nuevos y actualizados	Proceso de gestión de la información, control interno,	(# de controles ejecutados / # de controles existentes) x 100				

CATEGORIA	Nº	IDENTIFICACION DE RIESGOS	FECHA DE IDENTIFICACION DE RIESGO	ANALISIS DEL RIESGO			VALORACION INICIAL DEL RIESGO				TRATAMIENTO Y SEGUIMIENTO DEL RIESGO					
				CAUSAS	CONSECUENCIAS	BARRERAS DE SEGURIDAD EXISTENTES	VALOR DE PROBABILIDAD	VALOR DE IMPACTO	NIVEL DEL RIESGO	BARRERAS DE SEGURIDAD A IMPLEMENTAR	RESPONSABLE DEL SEGUIMIENTO	INDICADOR	LINEA BASE	META	RESULTADOS DE EFECTIVIDAD DE LAS ACCIONES (Planeación)	VALORACION DEL RIESGO DESPUES DECONTROLES (Control Interno)
TEC	2	Vulnerabilidad, adulteración o uso indebido de la información	01/2022	Desconocimiento de política de confidencialidad y seguridad de la información Falta de procesos y procedimientos que regule, controle y mejore el acceso a la información Accesos no autorizados a las instalaciones	-Perdidas económicas - Daños a funcionarios, -Perdidas económicas, -Perjuicio de la imagen, -Sanciones legales	Políticas se seguridad y confidencialidad de la información --Procesos de custodia de documentos de archivo -Se dispone de backup	3 moderado	4 Mayor	Moderado	.Actualizar las Políticas se seguridad y confidencialidad de la información Seguimiento constante los controles existentes para que nunca se dejen de realizar	Proceso de gestión de la información, control interno, encargado de sistemas	(# de controles ejecutados / # de controles existentes) x 100 Informes desegui miento				

TEC	3	No disponibilidad del servicio de internet	01/2022	Debido a fallas técnicas en la prestación del servicio por parte del proveedor. Debido a daños físicos en la infraestructura de la red de datos.	Afectación a las operaciones en los procesos de la entidad. Reclamos de los ciudadanos. Perdida de acceso a los servicios tecnológicos.	.- Se tiene contrato de un servicio de internet con otro operador como respaldo. La alcaldía de Pasto tiene contacto directo con el proveedor de internet -La alcaldía de Pasto brinda soporte en caso de fallas	3 moderado	4 Mayor	Extremo	Aplicación permanente de los controles existentes.	Encargado de sistemas	# de controles ejecutados / # de controles existentes) x 100				
TEC	4	No de la disponibilidad del software Sysman	01/2022	falta de mantenimiento y actualización del mismo Perdida de conexión con el servidor Daño del servidor donde esta alojado el software	. detención en los procesos financieros y contables Quejas de los usuarios internos y externos del instituto	Se realizan copias de seguridad constantes Existe la persona idónea para dar solución en caso de fallas	3 moderado	4 Mayor	Extremo	. Adquirir contratación de actualización y mantenimiento Realizar procedimiento de copias de seguridad	Direccion Subdirección administrativa Funcionario encargado de Sysman	# de controles ejecutados / # de controles existentes) x 100 # de backups ejecutados / # de backups programadas x 100				

TEC	5	No disponibilidad de la información de copias de seguridad	01/2022	contaminación o deterioro de los contenedores de las copias errores humanos en la manipulación física de los contenedores o lógica de la información	Perdida de la confidencialidad, integridad o disponibilidad de la información contenida en copias de seguridad	- Disco duro externo donde se almacenan las copias de seguridad - Se tienen registros físicos de la información importante - Se realizan copias de seguridad en la nube de correo electronico	3 moderado	4 Mayor	Extremo	- Adquirir métodos automáticos para realizar copias de seguridad. - dar a conocer la política de seguridad de la informacion	Todos los funcionarios	# de backups ejecutados / # de backups programadas x 100				
TEC	**6**	**Publicación de información clasificada o reservada en el sitio web institucional o sin el debido proceso para solicitar publicar informacion**	**01/2022**	**-inadecuado nivel de conocimiento sobre la confidencialidad de la información por parte del personal que realiza la publicación o de quien autoriza la publicación** **- falta del uso de formatos y para solicitar publicaciones**	**- Demandas legales** **- Sanciones**	- **Se cuenta con asesores jurídicos** -	**1 moderado**	**3 Mayor**	**Moderado**	**. Utilizar los debidos procesos y formatos para solicitud de publicaciones** **-Implementar políticas de tratamiento de datos personales**	**Asesores jurídicos** **sistemas**					