IMPRETICS E.I.C.E.

2023

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

Versión 01

IMPRETICS E.I.C.E.

2023

#haciaelcentenario

Tabla de contenido

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo y su contexto, se planean acciones que mitiguen la afectación a la Entidad en caso de que se materialice, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que puedan comprometer el cumplimiento de los objetivos estratégicos trazados por IMPRETICS E.I.C.E.

Lo anterior requiere que IMPRETICS conozca su estado actual de sus activos de información, clasificarlos, priorizarlos y determinar su valor en caso de pérdida de información, y conocer los posibles riesgos que puedan afectar la seguridad y privacidad de la información y ciberseguridad de la Entidad, para de esta forma determinar las medidas orientadas a minimizar el impacto en caso de presentarse la materialización de algún riesgo.

En la medida que IMPRETICS tenga una visión de los riesgos que puedan afectar la Seguridad y Privacidad de la Información de la Entidad, se pueden establecer los controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad de su información, para lo cual, es necesario definir los lineamientos que se deben seguir para el análisis, evaluación, tratamiento de los riesgos que afectan la Seguridad y Privacidad de la Información.

El presente documento contiene entre otros aspectos, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de IMPRETICS 2023.

OBJETIVO GENERAL

Presentar el Plan de Tratamiento para los riesgos de Seguridad y Privacidad de la Información, que permita identificar, medir, tratar, controlar, monitorear y comunicar los riesgos de Seguridad y Privacidad de la Información de IMPRETICS E.I.C.E.

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

Objetivos Específicos

- Identificar los riesgos de Seguridad y Privacidad de la Información de los procesos de la Entidad.
- Calcular el nivel de riesgo.
- Establecer el plan de tratamiento de riesgos.
- Realizar el seguimiento y control a la eficacia del plan de tratamiento de riesgos.

ALCANCE

La identificación y tratamiento de los riesgos de seguridad y privacidad de la información, será de estricta aplicabilidad y cumplimiento por parte de todos los funcionarios, contratistas y terceros que presten sus servicios o que tengan algún tipo de relación con la Entidad; el tratamiento de riesgo debe involucrar a todos los procesos desarrolladas por IMPRETICS, en especial aquellos que impactan directamente la consecución de los objetivos misionales.

El Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información tendrá en cuenta los riesgos que se encuentren en los niveles Extremo, Alto y Medio, los riesgos que se encuentren en nivel Bajo serán aceptados por la Entidad, tendiendo en cuenta los lineamientos establecidos en la Política de Administración de Riesgos.

MARCO NORMATIVO

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023 de IMPRETICS es elaborado bajo el marco legal establecido:

- **Ley 87 de 1993**
  <<Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones>>.

- **Ley 1474 de 2012**
  <<Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.>> Precisa en el Art. 73 que <<cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano>>, asignando al Programa Presidencial de Modernización, Eficiencia,

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

Transparencia y Lucha contra la Corrupción señalar una metodología para diseñar y hacerle seguimiento a la estrategia. De igual forma precisa en el Art. 74 que deberá estar publicado al 31 de enero de cada año en la respectiva página web de cada entidad el Plan de Acción respectivo.

- **Decreto 1081 de 2015**
  <<Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.>> Título 4 Plan Anticorrupción y de Atención al Ciudadano.

- **Decreto 1078 de 2015**
  <<Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones>>

- **Decreto 1499 de 2017**
  <<Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015>>.

- **Política de Administración de Riesgos de IMPRETICS**

POLÍTICA DE ADMINISTRACIÓN DE RIESGO

IMPRETICS E.I.C.E. define su política de riesgos atendiendo los parámetros establecidos del Modelo Integrado de Planeación y Gestión – MIPG, así como los del Modelo Estándar de Control Interno, en lo referente a las líneas de defensa, los lineamientos de la Guía para la administración de riesgo y el diseño de controles en entidades públicas versión 4 del DAFP, articulada con las normas aplicables a la Entidad y las “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano”, como mecanismo para identificar, medir, valorar, monitorear, administrar y tratar los riesgos que pudieran afectar positivamente o negativamente el logro de los objetivos institucionales.

La Política definida por IMPRETICS E.I.C.E. como entidad operadora y proveedora de soluciones integrales de logística, comunicaciones, informática y material gráfico para el sector público y privado; coherente su compromiso de implementación del Modelo Integrado de Planeación y Gestión – MIPG, con los componentes y elementos que define el MECI, se compromete a ejercer el control efectivo de los eventos de riesgo que puedan afectar negativamente el desarrollo de sus procesos, a través de la identificación, análisis, valoración y administración del riesgo, contribuyendo de esta forma al logro de la misión y objetivos establecidos de la Entidad.

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- **EVITAR:** Eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

- **PREVENIR:** Corresponde a planear estrategias para que el evento no ocurra o que disminuya su probabilidad.

- **REDUCIR O MITIGAR:** Corresponde a la protección en el momento en que se presenta el riesgo, encontramos en estos planes de emergencia, de protección ambiental, copias de seguridad, entre otros.

- **DISPERSAR:** Dividir una actividad en diferentes componentes operativos, de manera que las actividades no se encuentran bajo un mismo proceso o bajo la responsabilidad de una sola persona.

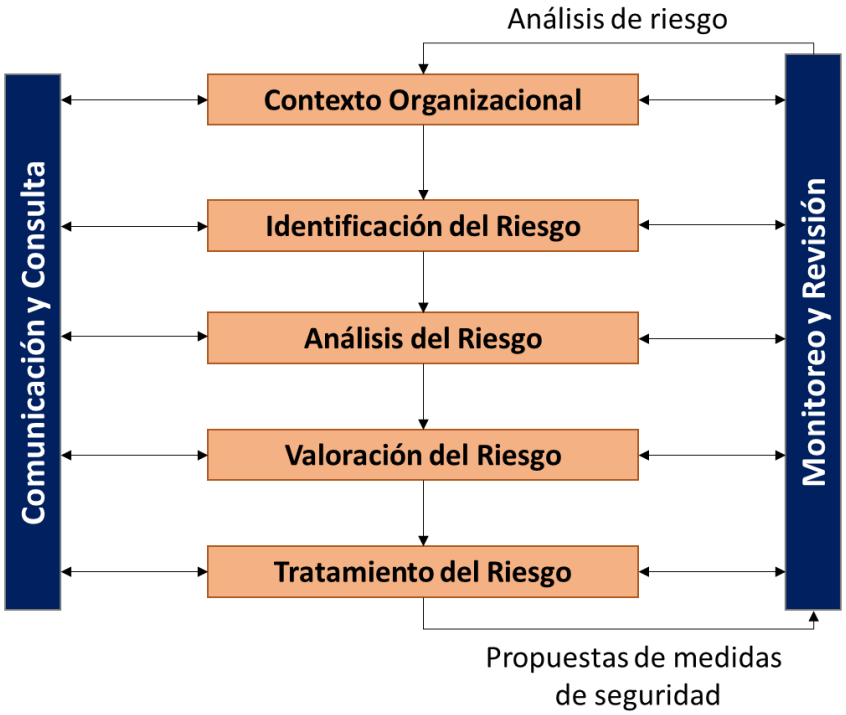
- **COMPARTIR:** Involucrar a un tercero para que responda en todo o en parte del riesgo que genera una actividad.

Teniendo en cuenta la Guía para la administración del riesgo y el diseño de controles en entidades públicas, los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, se deberá tener en cuenta al dueño del riesgo (dueño del proceso), ya que este deberá tener en cuenta la importancia del riesgo, y su impacto sobre la Entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

METODOLOGÍA DE EVALUACIÓN DE RIESGO DE SEGURIDAD DIGITAL

IMPRETICS, utiliza la metodología de Gestión de Riesgos establecida en la política adoptada por la entidad. Las actividades que hacen parte de la metodología son las siguientes:

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co



ETAPAS DE LA GESTIÓN DE RIESGOS

IMPRETICS E.I.C.E., ha definido en su Política que su gestión de riesgos consiste en la Identificación, Evaluación, Análisis, Monitoreo y Comunicación de riesgos para cada uno de los procesos entro de la organización, es decir, aquellas que se encuentren directamente ligadas con la creación de valor de la Entidad.

A continuación, se detallan las distintas etapas de la metodología de gestión de riesgos:

Identificación de Riesgo

El objetivo de esta etapa es identificar los principales riesgos críticos a los cuales se encuentran expuestos los procesos de la Entidad. Los encargados de los riesgos identificarán, para los procesos de su responsabilidad, los riesgos que puedan afectar los objetivos y/o estrategias definidas por el área.

Esta identificación puede ser realizada a través de:

- Reuniones con el equipo de trabajo.
- Encuestas con los diferentes colabores y personal que se relacione con el equipo de trabajo.

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

- Bases de datos o matrices de riesgo de ejercicios previos.

Una vez identificados los riesgos críticos, estos se deben documentar en una matriz de riesgos, clasificándolos por tipo de riesgo de acuerdo a lo siguiente:

- **Riesgos estratégicos:** posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
- **Riesgos gerenciales:** posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
- **Riesgos operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
- **Riesgos financieros:** posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, costos, etc.
- **Riesgos tecnológicos:** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- **Riesgos de cumplimiento:** posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
- **Riesgo de imagen o reputacional:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de seguridad digital:** posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Valoración de los Riesgos

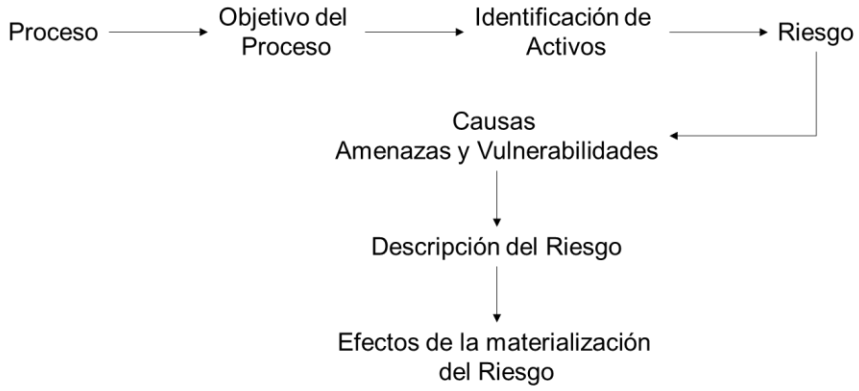
El objetivo de este paso es generar una lista completa de los riesgos sobre la base de los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos de la Entidad.

Las debilidades de los procesos en cuanto a seguridad de la información, los riesgos a los cuales se encuentran expuestos y las causas que podrían comprometer la confidencialidad, integridad y disponibilidad de los procesos de IMPRETICS deben

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

ser identificadas y evaluadas teniendo en cuenta los criterios de evaluación definidos. En este proceso se deben realizar las siguientes actividades:

- Identificar el flujo de información de cada uno de los procesos.
- Identificar las vulnerabilidades que existen en el proceso.
- Identificar los riesgos que podrían materializarse, dadas las vulnerabilidades existentes.
- Definir las escalas a utilizar.



De acuerdo con los lineamientos para la gestión de riesgos digital en entidades públicas emitida por el Departamento Administrativo de la Función Pública – DAFP, se podrán identificar los siguientes tres riesgos inherentes de seguridad digital:

- Pérdida de confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles **amenazas** y **vulnerabilidades** que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres riesgos previamente mencionados:

Identificación de amenazas

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

Deliberadas (D), Fortuito (F), Ambientales (A)

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

Tipo	Amenaza	Origen
Daño físico	Fuego	D, F, A
	Agua	D, F, A
Eventos naturales	Fenómenos climáticos	F
	Fenómenos sísmicos	F
Pérdida de los servicios esenciales	Fallas en el suministro de agua	D, F, A
	Fallas en el suministro de aire acondicionado	D, F, A
Perturbación debida a la radiación	Radiación electromagnética	D, F, A
	Radiación térmica	D, F, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D
Dirigidas por el hombre	Pirata informático, intruso ilegal	D
	Criminal de la computación	D
	Terrorismo	D
	Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	D
	Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despidos)	D

Identificación de las vulnerabilidades

Se deben identificar debilidades de acuerdo con los siguientes tipos:

Tipo	Vulnerabilidad
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura, polvo y suciedad.
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envió o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia de personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso de supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Análisis de Riesgo de Seguridad Digital

El objetivo del Análisis de Riesgos es identificar y valorar los riesgos a los cuales están expuestos los procesos y los flujos de información, para identificar y seleccionar los controles apropiados de seguridad. El análisis está basado en los flujos de información de cada uno de los procesos de IMPRETICS y los requerimientos de seguridad, tomando en cuenta los controles existentes.

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

En esta etapa se definen los criterios que se deben utilizar para evaluar la importancia del riesgo. Los criterios reflejarán los valores de la Entidad, los objetivos y recursos existentes. Estos criterios deberán revisarse contantemente, dado los cambios que puedan ocurrir en la Entidad.

Al definir los criterios de riesgo, se tendrá en cuenta:

- La naturaleza, los tipos de causas y consecuencias que puedan ocurrir y como se van a medir.
- La manera de definir la probabilidad de ocurrencia de un evento.
- La forma de determinar el nivel de riesgo.
- Niveles de riesgo aceptable para la organización.

Las actividades realizadas para ejecutar el análisis de riesgos se realizan de acuerdo con el siguiente esquema:

- Definición de las áreas de IMPRETICS que se incluirán dentro del alcance del proceso de gestión de riesgos de seguridad y privacidad de la información.
- Levantamiento de información relacionada con el proceso seleccionado.
- Entrevistas con personal clave dentro del proceso para conocer su percepción del riesgo al cual se encuentra expuesta la información.
- Ejecución de la evaluación de riesgos a los que se encuentra expuesto el proceso, por medio de la valoración de hallazgos y evaluación de probabilidad de ocurrencia de amenazas y vulnerabilidades.
- Análisis y diagnóstico del nivel de riesgos para el proceso definido. Se deberá elaborar un informe con los resultados.

Para la identificación de amenazas, vulnerabilidades y riesgos, se tienen en cuenta los resultados de las entrevistas con los dueños y/o responsables de los procesos del negocio y los análisis de riesgos existentes. Con el fin de establecer los niveles de riesgos a los cuales se encuentran expuestos los procesos, se mide la probabilidad de ocurrencia de las amenazas y el impacto que tendría las consecuencias de su materialización.

Se determina la probabilidad de ocurrencia para cada riesgo de acuerdo con la siguiente escala:

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

Probabilidad	Valor	Descripción
Insignificante	1	Ha ocurrido una vez en los últimos tres a cinco años
Bajo	2	Ha ocurrido una vez entre los últimos tres y cinco años
Moderado	3	Ha ocurrido una vez entre el ultimo año y tres años
Mayor	4	Ha ocurrido entre una y tres veces en el último año
Catastrófico	5	Ha ocurrido más de tres veces en el último año

Se determina el impacto de cada riesgo de acuerdo con la siguiente tabla:

IMPACTO	VALOR ASIGNADO	CONSECUENCIAS CUANTITATIVAS	CONSECUENCIAS CUALITATIVAS
Insignificante	1	• Impacto que afecte la ejecución presupuestal en un valor ≥0,5% • Pérdida en la prestación de los productos y servicios ofertados por la entidad ≥1% • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	• No hay interrupción de las operaciones de la entidad. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional de forma significativa. • Sin afectación de la confidencialidad
Menor	2	• Impacto que afecte la ejecución presupuestal en un valor ≥1% • Perdida en la prestación de los productos y servicios ofertados por la entidad ≥5% • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1% • Pago de sanciones económicas por incumplimiento en la normatividad aplicables ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	• Interrupción de las operaciones de la entidad por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del producto o servicio a los usuarios o clientes. • Afectación leve de la confidencialidad
Moderado	3	• Impacto que afecte la ejecución presupuestal en un valor ≥5% • Perdida en la prestación de los productos y servicios ofertados por la entidad ≥10%	• Interrupción de las operaciones en la entidad entre uno (1) o dos (2) días. • Reclamaciones o quejas de los usuarios que podrían implicar

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

		• Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, los cuales afectan en un valor ≥5% del presupuesto general de la entidad.	una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Inoportunidad en la información ocasionando retrasos en la prestación de los servicios a los usuarios. • Reproceso de actividades y aumento de carga operativa. • Imagen institucional afectada por retrasos en la prestación del servicio a los usuarios o clientes. • Investigaciones penales, fiscales o disciplinarias. • Afectación moderada de la confidencialidad de la información.
Mayor	4	• Impacto que afecte la ejecución presupuestal en un valor ≥20% • Pérdida de cobertura en la prestación de los productos y servicios ofertados por la entidad ≥20% • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	• Interrupción de las operaciones de la entidad por más de dos (2) días. • Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. • Sanción por parte del ente de control u otro ente regulador. • Incumplimiento en las metas y objetivos estratégicos institucionales establecidos, afectando el cumplimiento en las metas de la gobernación. • Imagen institucional afectada por el incumplimiento en la prestación de servicio a los usuarios y clientes. • Afectación grave de la confidencialidad de la información.
Catastrófico	5	• Impacto que afecte la ejecución presupuestal en un valor ≥50% • Pérdida en la prestación de los servicios de la entidad ≥50% • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	• Interrupción de las operaciones de la entidad por más de cinco (5) días. • Intervención por parte de un ente de control u otro ente regulador. • Pérdida de la información crítica para la entidad que no se puede recuperar. • Incumplimiento en las metas y objetivos estratégicos institucionales afectando de forma grave la ejecución presupuestal.

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

			• Imagen institucional afectada por actos o hechos de corrupción comprobados. • Afectación muy grave de la confidencialidad de la información.

La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Evaluación de los Controles Establecidos para la Mitigación de los Riesgos.

La Evaluación de los controles se realiza cuando se ha establecido el riesgo inherente para los procesos y el impacto y probabilidad de ocurrencia de cada uno de los riesgos establecidos. La evaluación de controles se realiza identificando los criterios relacionados a cada uno de los riesgos establecidos.

Variables:

CARACTERISTICA	DESCRIPCIÓN
Naturaleza del Control	Determina si el control es manual, mixto o automático
Documentación	Establece si el control está documentado
Evidencia	Si el control está divulgado o no divulgado
Tipo de control	Detectivo, preventivo o correctivo.

Para cada tipo de control se tienen en cuenta los siguientes pesos para determinar su eficacia:

TIPO DE CONTROL	PESO
Manual, mixto o automático	25%
Documentado (si) o (no)	25%
Divulgado (si) o (no)	25%
Detecto, preventivo o correctivo	25%

Cobertura efectiva: Con este análisis se identifica en que porcentaje se está mitigando el control teniendo en cuenta los siguientes determinadores:

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

NIVEL DE COBERTURA	PESO
Más del 90%	10
Entre 80 y 90%	9
Entre 70 y 80%	8
Entre 60 y 70%	7
Entre 50 y 60%	6
Entre 40 y 50%	5
Entre 30 y 40%	4
Entre 20 y 30%	3
Entre 10 y 20%	2
Menos del 10%	1

Niveles de Riesgo

Con base en el resultado del análisis de riesgo y con el fin de tratar el riesgo residual se proponen acciones de mejora que propenden por conservar las características de confidencialidad, integridad y disponibilidad de la información.

NIVELES DE RIESGOS			
Nivel	Valor asignado	Acción requerida	Gestión requerida
Extremo	Mayor a 9	Requiere acciones rápidas por parte de la Alta Dirección para disminuir el riesgo	Evitar
Alto	>7 y <=9	Requiere acciones rápidas por parte de la Alta Dirección para disminuir el riesgo	Evitar
Medio	>4 y <=7	Se requiere seguir ejecutando los controles definidos para el riesgo y revisar eficacia de estos.	Reducir
Bajo	>=2 y <=4	El riesgo se mitiga con actividades propias y por medio de acciones detectivas y preventivas.	Acepta
Insignificante	1	El riesgo no representa impacto significativo para la Entidad	Acepta

Las opciones de tratamiento de riesgos no son excluyentes entre sí. Estas pueden incluir una o varias de las siguientes acciones:

- Eliminar el riesgo prescindiendo del proceso, la actividad o las circunstancias que lo generan.

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

- Asumir el riesgo, aún aumentándolo, con el fin de incrementar una posible oportunidad.
- Tomar acciones para disminuir la probabilidad del riesgo.
- Implementar acciones que disminuyan el impacto negativo del riesgo.
- Compartir el riesgo.
- Retener el riesgo con base en información confiable.

Se debe tener en cuenta los siguientes factores en el establecimiento del tratamiento del riesgo:

- Si se encuentra en una zona de aceptación de riesgo.
- Recibirán tratamiento todos los riesgos que tengan un nivel Alto y Extremo.
- Si es susceptible de ser tratado a través de la implantación de un nuevo control o fortalecimiento de los ya existentes.
- Si la decisión es aceptarlo, independiente de donde se encuentra ubicado y la afectación que pueda tener para Confidencialidad, Integridad y Disponibilidad de la información.
- Si se decide ignorar el riesgo se reinicia el análisis.

Seguimiento y Revisión del Proceso de Gestión de Riesgos de Seguridad y Privacidad

El seguimiento y revisión del proceso de Gestión de Riesgos es una de las partes más importantes, donde las responsabilidades de seguimiento, monitoreo y evaluación debe estar claramente definidas y deben abarcar todos los aspectos del proceso de gestión.

No obstante, en la Política de Administración de Riesgos de IMPRETCS, se encuentran definidas las líneas de defensa, responsables de cada línea y sus responsabilidades frente al riesgo.

Adicional se recomiendan las siguientes actividades a ejecutar en esta fase:

- Analizar los cambios, tendencias, éxitos y fracasos dentro del proceso de gestión de riesgos de seguridad de la información.
- Detectar cambios en el contexto interno o externo, incluyendo los cambios que se presenten en los criterios de riesgos de seguridad y privacidad de la información.

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co

- Revisar la implementación de los planes de tratamiento de riesgo de seguridad de la información y las prioridades de implementación de estos.
- Identificación de nuevos riesgos de seguridad de la información.

CRONOGRAMA 2023

Actividad	Responsable Acción	1	2	3	4	5	6	7	8	9	10	11	12
Elaboración Plan de tratamiento de Riesgos de Seguridad y Privacidad	Planeación	E	F	M	A	M	J	J	A	S	O	N	D
Identificación de Riesgos	G. Sistemas	E	F	M	A	M	J	J	A	S	O	N	D
Medición de Riesgos	G. Sistemas/ Planeación	E	F	M	A	M	J	J	A	S	O	N	D
Control de Riesgos	G. Sistemas	E	F	M	A	M	J	J	A	S	O	N	D
Monitoreo de Riesgos	G. Sistemas	E	F	M	A	M	J	J	A	S	O	N	D
Elaborar informe semestral gestión	G. Sistemas/ Planeación	E	F	M	A	M	J	J	A	S	O	N	D
Ejecutar análisis de vulnerabilidades	G. Sistemas	E	F	M	A	M	J	J	A	S	O	N	D
Seguimiento y Control	G. Sistemas/ Planeación	E	F	M	A	M	J	J	A	S	O	N	D

APROBACIÓN, SOCIALIZACIÓN Y PUBLICACIÓN DEL PLAN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023 fue aprobado por unanimidad en el Comité Institucional de Gestión y Desempeño tal como reposa en el Acta No 001 de reunión del Comité realizada el 23 de enero del 2023. IMPRETICS E.I.C.E. divulgará y publicará el presente plan para conocimiento de todas las dependencias de la entidad y demás usuarios interesados.

Proyecto	**Reviso**	**Aprobó**
Genaro Peña Retallakc Gestión de Sistemas **Armando Rodríguez Cuellar** Planeación y Gestión MIPG	**Jairo García Londoño** Subgerente Administrativo y Financiero	**Comité Institucional de Gestión y Desempeño** **Dr. Fernando Céspedes Martínez** Presidente

Carrera 6 - Calles 9 y 10; Edificio de la Gobernación del Valle, Gerencia Tel: 889 6477- Planta Sótano -
Mercadeo y Ventas: 885 5253 - Administrativo: 885 5255 Celular: 318 - 889 55 68
Email: ventas@impretics.gov.co - comercialcali@impretics.gov.co, gerencia@impretics.gov.co