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

INSTITUTO COLOMBIANO DE ANROPOLOGÍA E HISTORIA

Instituto Colombiano de Antropología e Historia

ICANH

Tabla de contenido

1. OBJETIVO

Generar un plan de seguridad y privacidad alineado con el propósito misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

2. DEFINICIONES

- **Aceptación del Riesgo:** Análisis de consecuencias que surgen después de analizar un riesgo y decide afrontarlo.
- **Acción correctiva:** Acción para remediar una no conformidad, para que esta no se vuelva a repetir.
- **Acción preventiva:** Proceso que se implementa o se realiza para evitar que se ejecute o se implemente una no conformidad.
- **Administración de riesgos:** Serie de etapas que se deben desarrollar para el adecuado tratamiento de los riesgos
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis del riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Causa**: agentes internos o externos que generan riesgos.
- **Confidencialidad:** Nivel de seguridad, donde la información solo puede ser accedida por personal autorizado.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona jurídica o natural.
- **Integridad:** Propiedad de la información, donde la información no ha sido modificada
- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Conjunto de lineamientos, políticas, procesos de una institución.
- **Riesgo:** Posibilidad que una amenaza pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. ISO Guía 73:2002.
- **Riesgo Inherente:** Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. Este riesgo surge de la exposición que se tenga de la información y de la

probabilidad que una amenaza se concrete y afecte los activos de información

- **Vulnerabilidad:** Es un falla, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes
- **SGSI Sistema de Gestión de la Seguridad de la Información:** Según [ISO/IEC 27001: 20005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).

3. ETAPAS

Un Plan Estratégico de Seguridad informática está basado en un conjunto de políticas de seguridad elaboradas a partir de una evaluación de los riesgos a los que están expuestos los activos de información, que indicará el nivel de seguridad en el que se encuentre la institución. Con el fin de identificar, medir, controlar y monitorear los riesgos existentes, el ICANH va a desarrollar el Tratamiento de Riesgos de Seguridad y Privacidad de la Información y se proponen las siguientes fases:

A. IDENTIFICACIÓN DE LA INFORMACIÓN

Identificación de los activos más relevantes que inciden directamente en los productos y servicios del ICANH que reflejan la misionalidad de la entidad, ponderando su impacto a nivel de confidencialidad, integridad, y disponibilidad.

B. IDENTIFICACION DE LOS RIESGOS

Debemos tener en cuenta las siguientes definiciones para poder identificar el riesgo de seguridad y poder aplicarlos.

- **Confidencialidad de la información:** Comprende los riesgos a la pérdida o revelación de la misma. Cuando se habla de información reservada institucional se hace alusión a aquella que por la razón de ser de la entidad solo puede ser conocida y difundida al interior de la misma; así mismo, la sensibilidad de la información depende de la importancia que esta tenga para el desarrollo de la misión de la entidad.

- **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- **Riesgos Operativos:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias. En esta parte entran todos aquellos procesos clasificados como apoyo.

- **Riesgos Legales:** Se refiere con el incumplimiento en su función administrativa, ejecución presupuestal y normatividad aplicable.

- **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión**.**

C. ESTIMACIÓN EL IMPACTO

Cuando se hayan identificados los riesgos miramos el daño sobre los activos, teniendo en cuenta los impactos sobre (Confidencialidad, Integridad y Disponibilidad).

TABLA DE IMPACTO			
TIPO	**NIVEL**	**DESCRIPTOR**	**DESCRIPCIÓN** En caso que el riesgo se materialice el impacto y afectación sería…
CONFIDENCIALIDAD EN LA INFORMACIÓN	**1**	**INSIGNIFICANTE**	Se afecta a una persona en particular.
	2	**MENOR**	Se afecta a un grupo de trabajo interno del proceso.
	3	**MODERADO**	Se afecta a todo el proceso.
	4	**MAYOR**	La afectación se da a nivel estratégico.
	5	**CATASTRÓFICO**	La afectación se da a nivel institucional.
CREDIBILIDAD O IMAGEN	**1**	**INSIGNIFICANTE**	Se afecta al grupo de funcionarios y contratistas del proceso.
	2	**MENOR**	Se afecta a todos los funcionarios y contratistas de la entidad.
	3	**MODERADO**	Se afecta a los usuarios de la Sede Central de la entidad.
	4	**MAYOR**	Se afecta a los usuarios de las Direcciones Territoriales.
	5	**CATASTRÓFICO**	Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales.
LEGAL	**1**	**INSIGNIFICANTE**	Se producen multas para la entidad.
	2	**MENOR**	Se producen demandas para la entidad.
	3	**MODERADO**	Se producen investigaciones disciplinarias.
	4	**MAYOR**	Se producen investigaciones fiscales.
	5	**CATASTRÓFICO**	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.
OPERATIVO	**1**	**INSIGNIFICANTE**	Se tendrían que realizar ajustes a una actividad concreta del proceso.
	2	**MENOR**	Se tendrían que realizar ajustes en los procedimientos del proceso.
	3	**MODERADO**	Se tendrían que realizar ajustes en la interacción de procesos.
	4	**MAYOR**	Se presentan intermitencias o dificultades en la operación del proceso
	5	**CATASTRÓFICO**	Se presentaría paro o no operación del proceso.

Valor	Nivel	Descripción del impacto
1	INSIGNIFICANTE	Se afecta a un funcionario al interior del instituto, no afecta la imagen del instituto ni la de ningún proceso por lo cual no se presentan riesgos operativos
2	MENOR	Impacta la imagen del Instituto, se afecta a un grupo de usuarios de un proceso y por ende el funcionamiento, pueden existir demandas legales, Se tendrían que realizar ajustes en los procedimientos del proceso.
3	MODERADO	Se afecta la imagen de la institución, afecta a terceros, se producen investigaciones disciplinarias y se tendrían que realizar ajustes en la interacción de procesos.
4	MAYOR	Existe afectación a nivel de confidencialidad de la información a nivel estratégico, afecta la imagen de toda la institución, se pueden producir investigaciones a nivel fiscal y a nivel operativo se presentan intermitencia en los procesos.
5	CATASTRÓFICO	La confidencialidad afectara toda la institución, la imagen se ve afectada a nivel nacional, se producen sanciones por los entes de control a la entidad por parte de los entes de control, se puede presentar paro a nivel de los procesos.

En conclusión, la escala que se utilizara es la siguiente

Escala	Valor
INSIGNIFICANTE	1
MENOR	2
MODERADO	3
MAYOR	4
CATASTRÓFIC O	5

D. ESTIMACIÓN DE LA PROBABILIDAD EN EL RIESGO

Se estima el impacto ponderando con la probabilidad de ocurrencia de la amenaza. Y el impacto que puede causar la materialización del riesgo. La primera se refiere a la magnitud de sus efectos y la segunda representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse.

Debemos tener en cuenta lo siguiente: RIESGO = IMPACTO*PROBABILIDAD

TABLA DE PROBABILIDAD			
Valor	**DESCRIPTOR**	**DESCRIPCIÓN (FACTIBILIDAD)**	**FRECUENCIA**
1	**RARO**	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años.
2	**IMPROBABLE**	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
3	**POSIBLE**	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
4	**PROBABLE**	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
5	**CASI SEGURO**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Impacto: son las consecuencias que puede ocasionar la materialización del riesgo, referido a la magnitud y sus efectos.

CONCEPTO		IMPACTO				
PROBABILIDAD		INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
	VALOR	1	2	3	4	5
RARO (1)	1	1	2	3	4	5
IMPROBABLE (2)	2	2	4	6	8	10
POSIBLE (3)	3	3	6	9	12	15
PROBABLE (4)	4	4	8	12	16	20
CASI SEGURO (5)	5	5	10	15	20	25

Una vez identificados los riesgos a los que se refiere la etapa D de este documento será necesario llevar a cabo la determinación del Impacto de tales Riesgos en la Gestión Institucional del ICANH. Para lograrlo, se pretende tener en cuenta la escala que se muestra en la tabla expuesta a continuación.
Luego de la calificación del riesgo se mide la zona de impacto.

ZONA	VALOR
ZONA DE RIESGO BAJA	Mayor de 0 y menor de 5
ZONA DE RIESGO MODERADA	Mayor o igual a 5 y menor de 10
ZONA DE RIESGO ALTA	Mayor o igual a 10 menor de 20
ZONA DE RIESGO EXTREMA	Mayor o igual a 20

Teniendo en cuenta con los niveles de riesgos, las acciones requeridas se complementan en la siguiente tabla:

Zona	Acción requerida
ZONA DE RIESGO EXTREMA	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
ZONA DE RIESGO ALTA	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo
ZONA DE RIESGO MODERADA	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
ZONA DE RIESGO BAJA	Mitigar el riesgo mediante medidas momentáneas y efectivas del proceso que permitan prevenirlo o llevarlo a la zona de riesgo bajo. Asumir el riesgo.

4. MATRIZ DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

La valoración de los activos de información, serán plasmados en una matriz teniendo en cuenta las dimensiones de confidencialidad, integridad, disponibilidad y el análisis de riesgos de seguridad y privacidad de la información.
Elementos que componen la matriz de riesgo:

A. IDENTIFICACIÓN DEL RIESGO

- **Tipo de Activo de Información**:
  - **Información y datos de la entidad:** Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros
  - **Sistemas de información y aplicaciones de Software**: Software de

aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.

- **Dispositivos de Tecnologías de información- Hardware:** Equipos de cómputo que por su criticidad son considerados activos de información, no sólo activos fijos.
- **Soporte para almacenamiento de información**: Equipo para almacenamiento de información como USB, Discos Duros, CDs, SAN, NAS.
- **Servicios**: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.

- **Activo de Información**: Es cualquier elemento que contenga, genere, gestione y/o procese información, que tiene valor para la organización y por tanto debe protegerse.
  Ejemplos de activo de información: Base de datos personales, página web institucional, correo electrónico, unidades de backup, servidor de archivos, software antivirus, firewall perimetral, enlace de datos principal, enlace de datos de backup, VPN

  - **Propiedad que afecta el Riesgo**: Los riesgos de seguridad digital se basan en la afectación de uno o los tres criterios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”.
  - **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
  - **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
  - **Integridad:** Propiedad de exactitud y completitud.

- **Descripción del Riesgo**: Esta descripción se refiere a las características generales las formas en que se manifiesta y observa el riesgo identificado.

- **Responsable de determinar la materialización del riesgo**: Responsable de proceso; Gestor de TI o supervisor de la Entidad.

- **Amenazas**: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización [ISO/IEC 27000:2018]

- **Vulnerabilidades**: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos

B. ANÁLISIS DEL RIESGO INHERENTE

- **Probabilidad**: Es la medida para estimar la ocurrencia del riesgo y se mide con criterios de Frecuencia, si se ha materializado cierto número de veces en un tiempo determinado) o de factibilidad; teniendo en cuenta la presencia de factores internos y externos, que pueden propiciar el riesgo, aunque este no se haya materializado.

- **Impacto**: Son las consecuencias potenciales que genera el hecho que se materialice el riesgo
  - **INSIGNIFICANTE:** Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
  - **MENOR:** Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad
  - **MODERADO:** Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
  - **MAYOR:** Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
  - **CATASTRÓFICO:** Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.
- **Zona de Riesgo**: Representa la zona en la que se encuentra el riesgo, a la que se enfrenta inicialmente un proceso o la entidad, en ausencia de controles.

Zona de Riesgo Baja
Zona de Riesgo Moderado
Zona de Riesgo Alta
Zona de Riesgo Extrema

C. IDENTIFICACIÓN DE CONTROLES

- **Opciones de manejo del riesgo**: Las opciones de manejo del riesgo, representan las posibilidades que se tienen para administrar el riesgo, a través de controles, luego de determinar la probabilidad e impacto del riesgo inherente.

o **ACEPTAR EL RIESGO:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

o **REDUCIR EL RIESGO:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

o **EVITAR EL RIESGO:** Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

o **COMPARTIR EL RIESGO:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.

- **Zonas de riesgo y opciones de riesgo**: Para nuestro caso las se aplicaran las siguientes opciones de manejo de las zonas de riesgo.

Zona	Acción
Zona de Riesgo Baja	Reducir el Riesgo
Zona de Riesgo Moderado	Reducir el Riesgo
Zona de Riesgo Alta	Compartir el Riesgo
Zona de Riesgo Extrema	Compartir el Riesgo

- **Descripción del control**: Cual(es) es (son) los controles que actualmente realiza el proceso para mitigar el riesgo inherente.
- **Responsable de ejecutar el control**: La persona que es responsable de la ejecución de los controles

D. RIESGO RESIDUAL:

Es aquel que persiste después de haber aplicado controles para la disminución del riesgo

- **Probabilidad**: Representa la probabilidad residual, de materialización del riesgo, una vez evaluados los controles establecidos en el proceso, que contrarrestan la probabilidad de materialización del riesgo inherente.
- **Impacto**: Representa el impacto residual, de materialización del riesgo, una vez evaluados los controles establecidos en el proceso; que contrarrestan el impacto de la materialización del riesgo inherente.
- **Zona de riesgo residual**: Es la nueva zona de riesgo, después de evaluar los controles establecidos por el proceso para mitigar el riesgo inherente.

4. FORMULACIÓN DEL PLAN DE TRATAMIENTOS RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

La formulación de las diferentes actividades de tratamiento de riesgos de seguridad de la información implicara la definición e identificación de los controles existentes y la implementación de nuevos controles, acorde al nivel de riesgo y a la disponibilidad de recursos.

Es importante además definir el tipo de control se va a implementar:

- **Preventivo:** Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
- **Correctivo:** Aquellos que permiten el restablecimiento de la actividad, después de ser identificado un evento no deseable, también la modificación de las acciones que propiciaron su ocurrencia.
- **Detectivo:** Aquellos que detectan un evento no deseable cuando se están ejecutando y por tal razón impiden la materialización del riesgo

A. SEGUIMIENTO Y EVALUACIÓN

Es importante llevar el registro de acciones de seguimiento para cada uno de los controles implementados en el Plan de tratamiento, con el fin de evaluar la eficacia en su implementación, adelantando verificaciones como mínimo semestralmente o cuando se considere necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo semestral debe estar a cargo de los responsables de los procesos, la Oficina de Control Interno y del área de TI y/o Sistemas, aplicando y haciendo los ajustes necesarios para tener un control del manejo del riesgo de seguridad y privacidad de la información.

B. MATRIZ DE SEGUIMIENTO Y EVALUACIÓN

TAREAS 2022	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Revisión y ajustes de los activos de información						
Sistema de gestión de seguridad de la información – SGSI -						
Declaración de aplicabilidad						
Ajuste de la Matriz de Riesgo						
Plan de tratamiento de Riesgo						