

Plan de tratamiento de seguridad y privacidad de la información 2021-2024

**instituto colombiano de ballet clásico - incolballet**

**2021**

**CONTENIDO**

[**1.** **INTRODUCCIÓN** 2](#_Toc80351228)

[**2.** **MARCO CONCEPTUAL** 3](#_Toc80351229)

[**3.** **MARCO LEGAL** 3](#_Toc80351230)

[**4.** **DEFINICIONES** 4](#_Toc80351231)

[**5.** **CONTEXTO ESTRATÉGICO** 7](#_Toc80351232)

[5.1. Misión 7](#_Toc80351233)

[5.2. Visión 7](#_Toc80351234)

[5.3. Objetivos Estratégicos 8](#_Toc80351235)

[5.4. Establecimiento del contexto de Riesgos de Seguridad de la Información 8](#_Toc80351236)

[**5.4.1.** **Criterios de evaluación del riesgo de seguridad de la información:** 8](#_Toc80351237)

[**5.4.2.** **Criterios de Impacto** 9](#_Toc80351238)

[**5.4.3.** **Criterios de Aceptación** 9](#_Toc80351239)

[**5.5.** **VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** 10](#_Toc80351240)

[**5.5.1.** **Identificación del riesgo** 10](#_Toc80351241)

[5.6. Estimación del riesgo 12](#_Toc80351242)

[**5.6.1.** **Determinación del riesgo inherente y residual** 12](#_Toc80351243)

[**5.6.2.** **Evaluación de los riesgos** 13](#_Toc80351244)

[5.7. Tratamiento de los riesgos de Seguridad de la Información 13](#_Toc80351245)

[5.8. Monitoreo y seguimiento de los riesgos de Seguridad de la Información 13](#_Toc80351246)

[**5.8.1.** **CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION** 14](#_Toc80351247)

[5.9. Política de Gestión Riesgos 14](#_Toc80351248)

[5.10. Mapa de Procesos 14](#_Toc80351249)

[**6.** **ROLES Y RESPONSABILIDADES** 15](#_Toc80351260)

[**7.** **ALCANCE** 16](#_Toc80351261)

[**8.** **DESCRIPCIÓN DE PARTES INTERESADAS** 17](#_Toc80351262)

[**9.** **FORMULACIÓN DEL PLAN DE SEGURIDAD DIGITAL.** 17](#_Toc80351263)

[**9.1.** **METODOLOGÍA** 17](#_Toc80351264)

[**10.** **OBJETIVOS DEL PLAN** 23](#_Toc80351265)

[10.1. Objetivo General 23](#_Toc80351266)

[10.2. Objetivos Específicos 24](#_Toc80351267)

[**11.** **METAS** 24](#_Toc80351268)

[**12.** **PLAN DE ACCIÓN** 30](#_Toc80351269)

[**13.** **SEGUIMIENTO** 30](#_Toc80351270)

[**14.** **RENDICIÓN DE CUENTAS** 31](#_Toc80351271)

# **INTRODUCCIÓN**

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

El INCOLBALLET decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información aprobada por la Alta Dirección, y como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

* **Confidencialidad**: Propiedad que la información sea concedida únicamente a quien esté autorizado.
* **Integridad**: Propiedad que la información se mantenga exacta y completa.
* **Disponibilidad**: propiedad que la información sea accesible y utilizable en el momento que se requiera.

# **MARCO CONCEPTUAL**

# **MARCO LEGAL**

Se tendrán como línea base para la clasificación de activos de información las normas y Leyes vigentes, las cuales se listan a continuación:

|  |  |
| --- | --- |
| **Norma** | **Descripción** |
| Ley 1266 de 2008 | Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera |
| Ley 1273 de 2009 | Por la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" |
| Ley 1581 de 2012 | Por la cual se dictan disposiciones generales para la protección de datos personales |
| Decreto 1377 de 2013 | Por el cual se reglamenta parcialmente la Ley 1581 de 2012 |
| Ley 1712 de 2014 | Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones” |
| Decreto 103 de 2015 | Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones |
| Ley 1755 de 2015 | Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. |
| Decreto 1081 de 2015 | “Por medio del cual se expide el Decreto Reglamentario Único del Sector de la Presidencia de la República” |
| Resolución 3564 de 2015MinTIC | Por la cual se reglamentan los artículos 2.1.1.2.1.1, 2.1.1.2.1.11, 2.1.1.2.2.2, y el parágrafo 2o del artículo 2.1.1.3.1.1 del Decreto número 1081 de 2015. |
| Guía  | Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida en agosto de 2018. |
| CONPES 3854 del 11 de abril de 2016 - 5.1 | Política Nacional de Seguridad Digital en Colombia. La política de Seguridad Digital basa su estructura en este documento CONPES. |
| Ley 1928 de 24 de julio de 2018 | Por la cual se aprueba el convenio sobre la ciberdelincuencia. |
| Decreto 1151 de 2008 | Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Lineamientos generales de la Estrategia de Gobierno en línea. |
| Decreto 1008 del 14 de junio de 2018 | Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. |

# **DEFINICIONES**

Para la adecuada gestión de riesgos de Seguridad Digital se utilizan los siguientes términos:

* **Administración del riesgo:** Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
* **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
* **Análisis de riesgos:** Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
* **Amenaza**: Es la causa potencial de una situación de incidente y no deseada por la organización.
* **Causa**: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
* **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
* **Consecuencia**: Resultado de un evento que afecta los objetivos.
* **Criterios del riesgo:** Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
* **Control:** Medida que modifica el riesgo.
* **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
* **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
* **Evento**: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
* **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
* **Evitación del riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
* Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
* **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
* **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
* **Incidente de seguridad de la información**: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
* **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
* **Impacto:**. Cambio adverso en el nivel de los objetivos del negocio logrados.
* **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
* **Matriz de riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
* **Monitoreo**: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.
* **Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
* **Proceso**: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
* **Riesgo Inherente**: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
* **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
* **Riesgo**: Efecto de la incertidumbre sobre los objetivos.
* **Riesgo en la seguridad de la información**: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
* **Reducción del riesgo**: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
* **Retención del riesgo**: Aceptación de la pérdida o ganancia proveniente de un riesgo particular.
* **Seguimiento**: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
* **Tratamiento del Riesgo:** Proceso para modificar el riesgo” (Icontec Internacional, 2011).
* **Valoración del Riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
* **Vulnerabilidad**: Es aquella debilidad de un activo o grupo de activos de información.
* **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
* **SGSI**: Sistema de Gestión de Seguridad de la Información.

# **CONTEXTO ESTRATÉGICO**

El contexto estratégico esta soportado en los lineamientos definidos en el Plan estratégico institucional, el modelo de operación por procesos y la política integral de riesgos, que define los siguientes criterios:

## Misión

*Nuestra Misión Institucional es la de propender por el desarrollo cultural de la población infantil y juvenil preferencialmente del Valle del Cauca, mediante la elaboración y adopción de planes, programas y proyectos con criterios de responsabilidad, equidad, solidaridad y desarrollo sostenible de educación artística profesional en danza, ejecutados a través de la Escuela de Educación Formal, las compañías profesionales de Ballet Clásico y Danza Contemporánea, formación de públicos, festivales, encuentros y otros, gestionando recursos y propiciando la vinculación de organismos nacionales e internacionales, públicos y privados.*

## Visión

*En el 2024 INCOLBALLET estará posicionada en el ámbito nacional e internacional como institución líder de formación de niños y jóvenes en danza profesional en Colombia, reconocida por la excelencia de su educación formal, artística e integral, la calidad de sus producciones en Ballet clásico, Danza contemporánea y gestión cultural, contribuyendo a la consolidación de ciudadanos íntegros, con altas calidades humanas y artísticas en danza, para el bienestar y la convivencia pacífica*

## Objetivos Estratégicos

1. Fortalecer la capacidad institucional para elevar el despliegue, desarrollo e impacto de los procesos misionales del Instituto.
2. Promover el modelo artístico institucional mediante acciones de mercadeo, divulgación e imagen institucional a los grupos de valor.
3. Establecer un modelo único de educación artística INCOLBALLET; con base en la innovación y la gestión del conocimiento.
4. Articular los procesos de formación académica, mediante planes y proyectos que impulsen una gestión pública eficiente y transparente.
5. Lograr una cultura interna con enfoque a la satisfacción de la comunidad educativa y procesos internos.

## Establecimiento del contexto de Riesgos de Seguridad de la Información

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la el INCOLBALLET y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos del INCOLBALLET, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

# **Criterios de evaluación del riesgo de seguridad de la información:**

La evaluación de los riesgos de seguridad de la información se enfocará en:

* El valor estratégico del proceso de información en el INCOLBALLET.
* 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 del INCOLBALLET
* Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la el INCOLBALLET.

# **Criterios de Impacto**

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

* Nivel de clasificación de los activos de información impactados
* Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
* Operaciones deterioradas (afectación a partes internas o terceras partes)
* 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

Los niveles de clasificación de los impactos establecidos se podrán tomar del documento - Política integral de gestión del Riesgo

# **Criterios de Aceptación**

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la el INCOLBALLET y de las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información se podrán tomar del documento – Política integral de gestión del Riesgo

# **VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la el INCOLBALLET, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

* Análisis del riesgo
	+ Identificación de los riesgos
	+ Estimación del riesgo
* Evaluación del riesgo

# **Identificación del riesgo**

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los **activos de información** se clasifican en dos tipos:

1. **Primarios**: Procesos o subprocesos y actividades del Negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización;procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
* **Información:** información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
* **Actividades y procesos de negocio**: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.
1. **De Soporte**
* **Hardware**: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
* **Software**: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
* **Redes**: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
* **Personal**: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
* **Sitio**: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
* **Estructura organizativa**: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las **amenazas** que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las **vulnerabilidades** que podrían aprovechar las amenazas y causar daños a los activos de información del INCOLBALLET. Existen distintos métodos para analizar amenazas, por ejemplo:

* Entrevistas con líderes de procesos y usuarios
* Inspección física
* Uso de las herramientas para el escaneo automatizado

Para cada una de las **amenazas** analizaremos las **vulnerabilidades** (debilidades) que podrían ser explotadas.

Finalmente se identificarán las **consecuencias**, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

## Estimación del riesgo

La estimación del riesgo busca 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. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

* **Probabilidad**: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.
* **Impacto**: Hace referencia a las consecuencias que puede ocasionar a la el INCOLBALLET la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

# **Determinación del riesgo inherente y residual**

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

# **Evaluación de los riesgos**

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto a la Alta Entidad.

## 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.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

**Nota:** Será conveniente que para la selección de los controles se consideren posibles restricciones o limitantes que impidan su elección: restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal o las restricciones para la integración de controles nuevos y existentes.

## 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 iterativa de los riesgos de seguridad de la información.

Los riesgos podrán cambiar de forma o manera radical, es por ello es necesario una supervisión continua que detecte:

* Nuevos activos o modificaciones en el valor de los activos.
* Nuevas amenazas.
* Cambios o aparición de nuevas vulnerabilidades.
* Aumento de las consecuencias o impactos.
* Incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

# **CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION**

La Entidad define el cronograma anexo que contiene las actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la organización, basado con su criticidad y su valor para el cumplimiento de la misionalidad del INCOLBALLET.

Hacen parte como anexo de este plan la matriz y el cronograma de valoración y tratamiento de riesgos de Seguridad de la Información.

## Política de Gestión Riesgos

La Política de gestión de riesgos de Seguridad Digital PGRSD definida para la entidad, se encuentra integrada en el documento titulado “Política Integral de Riesgos”.

## Mapa de Procesos





1.
2.
3.
4.
5. 1.
	2.
	3.
	4.
	5.

# **ROLES Y RESPONSABILIDADES**

|  |  |  |
| --- | --- | --- |
| **DENOMINACIÓN** | **ROL** | **RESPONSABILIDADES** |
| Dirección administrativa y financiera-TIC | Líder del proceso de apoyo | Realizar propuestas ante el comité de seguridad de la información para proteger y preservar los activos de información de la entidad.Realizar el seguimiento al cumplimiento de las políticas de seguridad de la información de la entidad. Ejecutar el plan de tratamiento de seguridad de la información. |
| Comité de seguridad de la información | Coordinador del SGSI | Aprobar las políticas y propuestas para la seguridad de la información.Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean con las metas y objetivos de INCOLBALLET.Realizar revisiones del SGSI. |
|  |  |  |

# **ALCANCE**

La gestión de riesgos de seguridad de la información y su tratamiento, será aplicada sobre cualquier proceso del INCOLBALLET, a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación, contenidos en la política integral de gestión del riesgos.

# **DESCRIPCIÓN DE PARTES INTERESADAS**

|  |  |  |
| --- | --- | --- |
| **Parte involucrada** | **Descripción** | **Tipo de impacto** |
| Funcionarios propios y personal de apoyo interno | Todos los que participan en los procedimientos de la entidad y producen información para y en el desarrollo de sus actividades diarias. | ALTO |
| Escuela | La escuela produce, administra y gestiona información de si proceso, de menores de edad, padres y/o acudientes y docentes, adicional- | ALTO |
| Ciudadanía en general | Con la implementación de recursos tecnológicos en las diferentes actividades de la entidad, se genera un impacto de cara al ciudadano que consume los diferentes productos y servicios de INCOLBALLET. | ALTO |

# **FORMULACIÓN DEL PLAN DE SEGURIDAD DIGITAL.**

# **METODOLOGÍA**

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñada basada tanta en la norma ISO/IEC 31000 como en la ISO 27005 adoptada por el INCOLBALLET para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:



La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.

* + 1. **POLÍTICA DE ADMINISTRACIÓN DE RIESGOS**

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores de INCOLBALLET:

|  |
| --- |
| **POLÍTICA DE ADMINISTRACIÓN** |
|   |
| Cuando se mide la probabilidad e impacto de un riesgo residual de proceso y éste queda catalogado en nivel **BAJO,** se **ASUMIRÁ** el riesgo y se administrará por medio de las actividades propias del proceso, se administrará mediante un seguimiento semestral, su control y registro de avance se realizará en el reporte **MENSUAL** de su desempeño. |
| Cuando el nivel del riesgo queda en **MODERADO,** se establecerán acciones de Control Preventivas que permitan **ASUMIR O REDUCIR** la probabilidad de ocurrencia del riesgo, se administrarán mediante seguimiento **BIMESTRAL** y se registrarán sus avances en el Mapa de riesgos por proceso. |
| Cuando el nivel del riesgo residual queda ubicado en la zona de riesgo **ALTA,** se deberá incluir el riesgo, tanto en el Mapa de riesgo del proceso como en el Mapa de riesgo institucional y se establecerán acciones de control preventivas que permitan **REDUCIR, EVITAR, COMPARTIR O TRANSFERIR** la materialización del riesgo. La Administración de estos riesgos será con periodicidad sugerida al menos **MENSUAL** |
| Si el nivel del riesgo residual se ubica en la zona de riesgo **EXTREMA,** se incluirá el riesgo en el Mapa de riesgo del Proceso y en el Mapa de Riesgo Institucional, se establecerán acciones de control preventivas y correctivas que permitan **REDUCIR, EVITAR, COMPARTIR O TRANSFERIR** la materialización del riesgo. La Administración de estos riesgos será con periodicidad mínima **MENSUAL.** Adicionalmente se deberán documentar al interior del proceso, planes de contingencia para tratar el riesgo materializado, con criterios de oportunidad, evitando el menor daño en la prestación del servicio; estos planes estarán documentados en las políticas de operación de cada proceso.  |
| **TODOS** los riesgos tipificados como **“CORRUPCIÓN”** harán parte del Mapa de riesgo Institucional y, aunque queden en la zona de riesgo **BAJA** se establecerán acciones preventivas con periodicidad **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos. |

|  |
| --- |
| **CLASIFICACIÓN DE RIESGO ( Muestra las clases de riesgos que se pueden presentar)** |
| **ESTRATÉGICO** | Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia. |
| **IMAGEN** | Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución. |
| **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, de la articulación entre dependencias. |
| **FINANCIEROS** | Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes. |
| **CUMPLIMIENTO** | Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad. |
| **TECNOLOGÍA** | Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión. |
| **CORRUPCIÓN** | Posibilidad de que por acción u omisión se use el poder para poder desviar la gestión de lo público hacia un beneficio privado. **ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.** |

|  |  |
| --- | --- |
| **TIPOS DE CONTROLES** | **DISMINUYE** |
| **PREVENTIVOS** | Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización. | **PROBABILIDAD** |
| **CORRECTIVOS** | Aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia. | **IMPACTO** |
| **DETECTIVO** | Aquellos que registran un evento después presentado; sirve para descubrir resultados no previstos y alertar sobre la presencia de un riesgo. | **DEPENDE DEL CONTROL IDENTIFICADO** |

|  |  |
| --- | --- |
| **ZONA DE RIESGO** | **OPCIONES DE MANEJO DEL RIESGO** |
| **BAJA** | \* Asumir el riesgo | Se asume el riesgo. **Nota:** Si el riesgo inherente se ubica en la zona baja, se debe revisar si éste riesgo amerita o no, que se incluya en el mapa de riesgos, para su administración. Se exceptuan los riesgos de **CORRUPCIÓN** |
| **MODERADA** | \* Asumir el riesgo\* Reducir el riesgo | Se asume el riesgo.Se implementan ***controles*** *y*sus ***acciones de manejo del riesgo*** orientadas a **disminuir** la probabilidad de materialización del riesgo Y/O ***controles*** y sus ***acciones de manejo del riesgo*** , orientadas a **disminuir** el impacto de la materialización del riesgo. Lo anterior con el propósito de llevar el riesgo a la zona baja.  |
| **ALTA** | \* Reducir el riesgo\* Evitar el riesgo\* Compartir o transferir el riesgo | Se implementan ***controles*** *y*sus ***acciones de manejo del riesgo,*** orientadas *a* **disminuir**o **evitar**la materialización del riesgo Y/O ***controles*** y sus ***acciones de manejo del riesgo*** orientadas*a* **disminuir o**  **evitar** el impacto de la materialización del riesgo. Lo anterior con el propósito de llevar el riesgo a zona moderada. En lo relacionado con compartir o transferir el riesgo, se podría establecer el mantenimiento de pólizas (contratos de seguros), tercerización, entre otras; como controles o acciones de manejo del riesgo enfocadas a la protección. Esta opción de manejo se deberá tener en cuenta, con base en la capacidad del proceso y/o la entidad, para asumir las consecuencias del impacto producido por la materialización del riesgo.  |
| **EXTREMA** | \* Reducir el riesgo\* Evitar el riesgo\* Compartir o transferir el riesgo | Se implementan ***controles***y sus ***acciones de manejo del riesgo***, orientadas a **disminuir** o **evitar** la materialización del riesgo Y/O **c*ontroles*** y sus ***acciones de manejo del riesgo***  orientadas a **disminuir** o **evitar** el impacto de la materialización del riesgo. En lo relacionado con **Compartir o transferir el riesgo**, teniendo en cuenta que en esta zona de riesgo se pueden producir pérdidas considerables para el proceso y/o la entidad, se hace necesario que se implementen **controles** de proteccióny sus **acciones de manejo del riesgo,** en los cuales se involucren **pólizas, tercerizaciones,** entre otras medidas que protejan el proceso y/o la entidad.  |

* + 1. **Fase 1: Análisis de información**
* Aplicar o construir políticas de tratamiento de riesgos.
* Determinar los controles aplicados en INCOLBALLET.
* Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de riesgos.
	+ 1. **Fase 2: Consolidación del Comité de Seguridad de la información.**

Se debe instaurar el comité vía resolución; el Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

El comité debe decidir en su primera reunión la estructura funcional del mismo acorde a los roles y responsabilidades establecidos en la resolución.

* + 1. **Fase 3: Identificación de activos de seguridad digital**

De acuerdo a lo establecido en el Plan de seguridad y privacidad de la información de INCOLBALLET.

* + 1. **Fase 4: Elaborar políticas de acceso y manejo de la información**

El líder operativo deberá proponer políticas de acuerdo a las condiciones, necesidades y objetivos de la entidad, teniendo en cuenta la matriz de activos de información y la matriz de riesgos con el fin de proteger y preservar la información de la entidad.

Estas políticas, manuales e instructivos deberán ser presentadas ante el comité de seguridad de la entidad para que se apruebe o se recomiende cambios según se requiera.

* + 1. **Fase 5: Realizar propuestas de adquisición o actualización de infraestructura tecnológica.**

Se encuentra alineado en el plan de acción el PETIC, si se requiere algo por fuera de ese plan de acción, se deberá realizar la propuesta al comité de seguridad para que esta sea aprobada en sesión y por acta.

* + 1. **Ciclo de vida del tratamiento de riesgos.**

**Planear:** Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 y 2 de la metodología de tratamiento de riesgos.

**Hacer:** En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 3, 4 y 5 de la metodología del

tratamiento de riesgos.

**Verificar:** En esta etapa se desarrollarán las actividades que permiten al comité hacer seguimiento a cada una de las medidas.

**Actuar:** Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

# **OBJETIVOS DEL PLAN**

## Objetivo General

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información en INCOLBALLET, permitiendo a la entidad alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad,

confidencialidad, disponibilidad y autenticidad de la información.

## Objetivos Específicos

* Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Entidad.
* Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas
* Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.
* Reducir toda posibilidad que un evento produzca un impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.

# **METAS**

Articuladas con el plan de seguridad y privacidad de la información.

| **PLAN DE TRABAJO MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** |
| --- |
| **FASE** | **OBJETIVO** | **ACTIVIDAD** | **2021** | **2022** | **2023** | **2024** |
| **TRIMESTRE 1** | **TRIMESTRE 2** | **TRIMESTRE 3** | **TRIMESTRE 4** | **TRIMESTRE 1** | **TRIMESTRE 2** | **TRIMESTRE 3** | **TRIMESTRE 4** | **TRIMESTRE 1** | **TRIMESTRE 2** | **TRIMESTRE 3** | **TRIMESTRE 4** | **TRIMESTRE 1** | **TRIMESTRE 2** | **TRIMESTRE 3** | **TRIMESTRE 4** |
| PLANIFICACIÓN | Establecer las actividades y procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información establecidos en el MSPI | Establecer (Actualizar) Política de Seguridad de la Información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Establecer manual de gestión de Seguridad de la Información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Actualizar el manual de seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Actualizar la política de seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Validar seguridad en aplicaciones de la Entidad |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Establecer roles y responsabilidades al interior de INCOLBALLET |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Definir guía e instrumento para el levantamiento y clasificación de activos de información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Realizar levantamiento y clasificación de activos de información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Establecer contexto de los riesgos de seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Identificar riesgos de seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Realizar análisis de riesgos de seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Realizar evaluación de los riesgos de seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Establecer declaración de aplicabilidad |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Diseñar el programa de sensibilización y capacitación |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Diseñar el plan de sensibilización y capacitación de sensibilización y capacitación en seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Definir herramientas para el programa de sensibilización y capacitación en seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Implementar el programa de sensibilización y capacitación en seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Establecer y documentar procedimientos de seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Definir guía para la gestión de eventos e incidentes de seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| IMPLEMENTACIÓN | Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información | Implementar plan de tratamiento de riesgos de seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Establecer el plan de contingencias de los sistemas de información y servicios de TI |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Definir componentes para la continuidad del negocio |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Realizar análisis de impacto del negocio |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| EVALUACIÓN DE DESEMPEÑO | Hacer seguimiento y medición a la implementación del MSPI. | Realizar plan de seguimiento y revisión de la efectividad de la implementación del MSPI. |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Ejecución de auditorías |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Medir la efectividad de los controles y políticas definidas |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Revisar los niveles de riesgos. |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Actualizar los planes entorno a la seguridad de la información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| MEJORA CONTINUA | Determinar los factores y/o aspectos a mejorar que hacen parte del MSPI | Desarrollar plan de mejora continua |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Gestionar las comunicaciones |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

# **PLAN DE ACCIÓN**

Ver anexo plan de acción.

# **SEGUIMIENTO**

Matriz de seguimiento.

# **RENDICIÓN DE CUENTAS**

|  |  |  |
| --- | --- | --- |
| Versión | Fecha | Cambios realizados |
| 2 | 30/12/2021 | Actualización |

Para su publicación se realiza revisión y aprobación por parte de las directivas de Incolballet.

|  |
| --- |
| PLAN de Tratamiento de Seguridad y Privacidad de la Información |
| Elaboró | Aprobó | Aprobó |
| JAMES GUTIERREZ  | BEATRIZ DELGADO |  |
|  |  |  |