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

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

# INTRODUCCIÓN

El Instituto Departamental de Deporte y Recreación del Quindio "INDEPORTES QUINDIO ", entendiendo la importancia de una adecuada gestión de la información,
Se ha comprometido con la implementación de un plan de tratamientos de riesgos de seguridad y privacidad de la información que permita tener un control para proteger y de ser necesario reducir los daños en caso de una fuga de la información en el instituto

# DEFINICIONES

Riesgo: Evento adverso e incierto (externo o interno) que derivado de la combinación de su probabilidad de ocurrencia y el posible impacto pudiera obstaculizar o impedir el logro de los objetivos y metas institucionales,

Administración del Riesgo: Comportamiento de los riesgos a que están expuestas en el desarrollo de sus actividades mediante el análisis de los distintos factores que pueden provocarlos, con la finalidad de definir las estrategias y acciones que permitan controlarlos y asegurar el logro de los objetivos y metas de una manera razonable.

Factores de Riesgo: Circunstancia o situación interna y/o externa que aumenta la probabilidad de que un riesgo se materialice.

Impacto: Consecuencias negativas que se generarían en la institución, en el supuesto de materializarse el riesgo

**Activo**
En relación con la seguridad de la información, se refiere a cualquier información
O elemento relacionado con el tratamiento de la misma (sistemas, soportes,
Edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

**Amenazas**
Causa potencial de un incidente no deseado, que puede provocar daños a un
Sistema o a la organización. (ISO/IEC 27000).

**Análisis de Riesgo**
Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

**Auditoría**
Proceso sistemático, independiente y documentado para obtener evidencias de
Auditoria y obviamente para determinar el grado en el que se cumplen los
Criterios de auditoría. (ISO/IEC 27000).

**Ciberseguridad**
Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

**Ciberespacio**
Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en
La civilización electrónica, la informática y la cibernética. (CONPES 37
01, Tomado de la Academia de la lengua Española).

**Control**
Las políticas, los procedimientos, las prácticas y las estructuras organizativas
Concebidas para mantener los riesgos de seguridad de la información por debajo
Del nivel de riesgo asumido. Control es también utilizado como sinónimo de
Salvaguarda o contramedida. En una definición más simple, es una medida que

Modifica el riesgo.

**Declaración de aplicabilidad**
Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información –SGSI, de la organización
Tras el resultado de los procesos de evaluación y tratamiento de riesgos
Y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

**Gestión de incidentes de seguridad de la información**
Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los Incidentes de seguridad de la información. (ISO/IEC 27000).

**Riesgo**
Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

**Seguridad de la información**
Preservación de la confidencialidad, integridad, y disponibilidad de la Información. (ISO/IEC 27000)

**Sistema de Gestión de Seguridad de la Información SGSI**

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

**Trazabilidad**

Cualidad que permite que todas las acciones realizadas sobre la información o Un sistema de tratamiento de la información sean asociadas de modo inequívoco A un individuo o entidad. (ISO/IEC 27000)

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

**Parte interesada (Stakeholder)**

Persona u organización que puede afectar a, ser afectada por o percibirse a sí Misma como afectada por una decisión o actividad.

# OBJETIVOS

El plan busca controlar y reducir los riesgos que puedan poner en peligro la información en el instituto departamental de deporte y recreación como son:

Mejorar la trasparencia en la gestión pública del instituto departamental de deporte y recreación del quindio Indeportes quindio

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

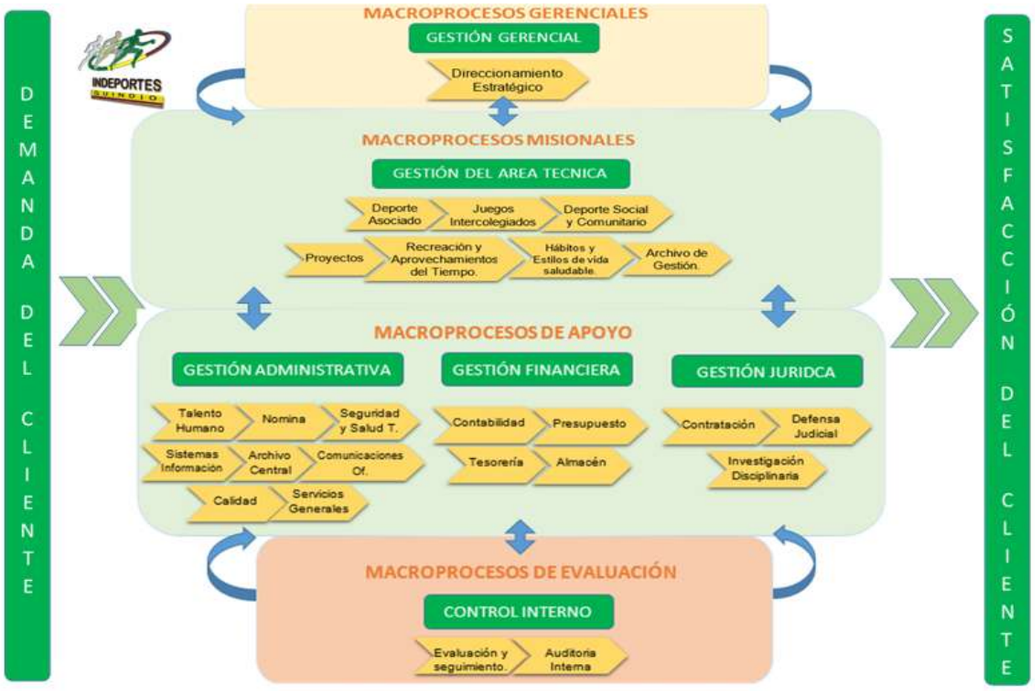
Contar con un monitoreo en tiempo real sobre eventos que puedan suceder en los equipos de computo de la entidad

Generar un informe de las fallas de seguridad que cuenta en el instituto departamental de deporte y recreación del quindio y de ser así subsanarlas para minimizar los riesgos

# ALCANCE

Este plan está dirigido a todos los funcionarios de planta y contratistas que son parte en los riesgos que cuenta el Instituto Departamental de Deporte y Recreación del quindio "INDEPORTES QUINDIO"

# RESPONSABLES DE PROCESOS




# DESCRIPCION DEL PLAN

## IDENTIFICACION DEL RIESGO

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

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

**Causas:**

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

**Consecuencias Potenciales:**

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

# RIESGOS DE SEGURIDAD DE LA INFORMACION

Los riesgos en la seguridad de la información del Departamental de Deporte y Recreación del Quindio se pueden clasificar en tres grupos: Actos originados por la criminalidad común, Riesgos por sucesos de origen físico y riesgos por sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales

| Actos originados por criminalidad común: | Riesgos por sucesos de origen físico: | Negligencia de usuarios y decisiones institucionales |
|---|---|---|
| • Sabotaje (ataque físico y electrónico)<br>• Daños por vandalismo<br>• Fraude /Estafa<br>• Robo/hurto (físico)<br>• Robo / Hurto información electrónica<br>• Virus /ejecución no autorizada de programas<br>• Violación a derechos de autor | • Incendio<br>• Sismo<br>• Polvo<br>• Sobrecarga eléctrica<br>• Falla de corriente (apagones)<br>• Falla de sistema /daño disco duro | • Falta de inducción, capacitación y sensibilización sobre riesgos<br>• Mal manejo de sistemas y herramientas<br>• Utilización de programas no autorizados /software ilegal<br>• Falta de pruebas de software nuevo con datos productivos<br>• Pérdida de Datos<br>• Infección de sistemas a través de unidades portables sin escaneo<br>• Manejo inadecuado de datos críticos (codificar, borrar, etc.)<br>• Manejo inadecuado de contraseñas (inseguras, no cambiar ,compartidas)<br>• Compartir contraseñas o permisos a terceros no autorizados<br>• Trasmisión de contraseñas por teléfono<br>• Acceso electrónico no autorizado a sistemas externos |

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

## TIPO DE RIESGOS

**Financieros:** Bajo presupuesto de funcionamiento que impide el desarrollo de los procesos, demoras en apropiación y ejecución de recursos, demoras para la trasferencia de recursos a municipios y apoyo a ligas deportivas.

**Tecnológico:** sistemas operativos ineficientes, falta de optimización de software, falta de coordinación de necesidades de tecnología, capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión

**Estratégicos:** Falta de lineamientos y demoras en la Planeación, , estructura organizacional no acordes con procesos, indicadores mal formulados que no aportan a la gestión para toma de decisiones, Falta de objetivos estratégicos y operacionales en el instituto

**Operativo:** 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.

**Confianza e imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

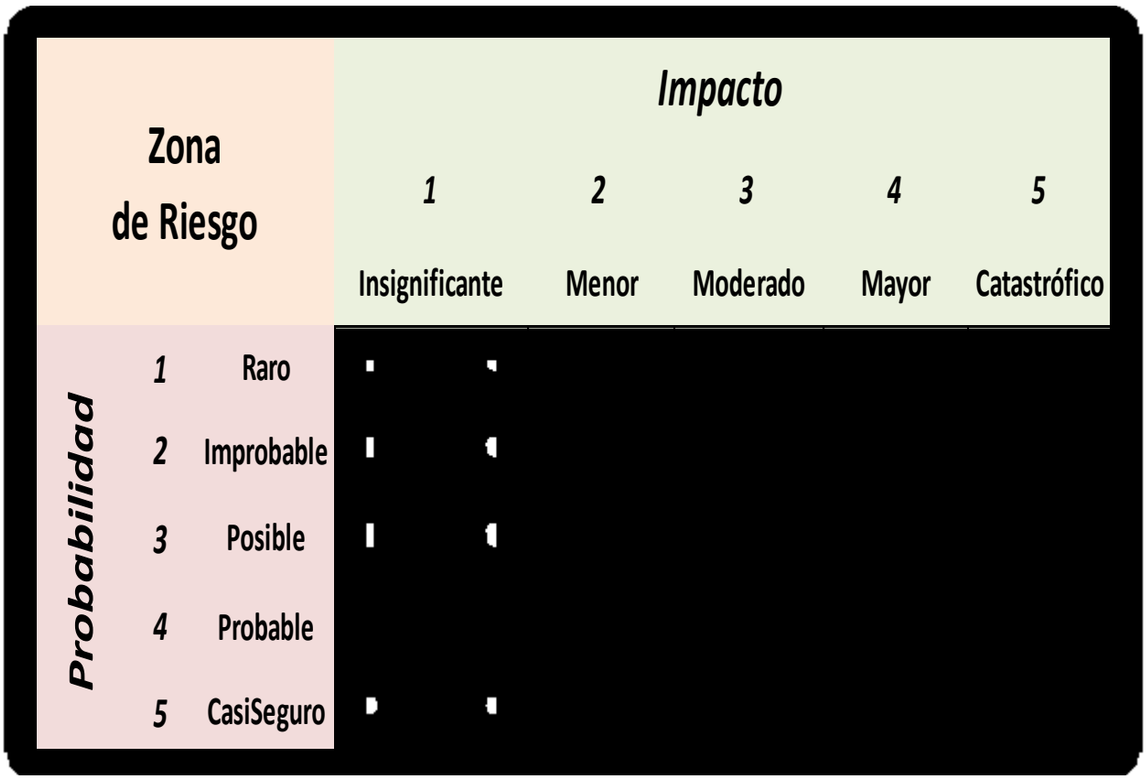
**Cumplimiento:** Se asocian con la capacidad del Instituto para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

## 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 a la actividad en particular y de la probabilidad que un choque negativo afecte la rentabilidad y el capital de la compañía.

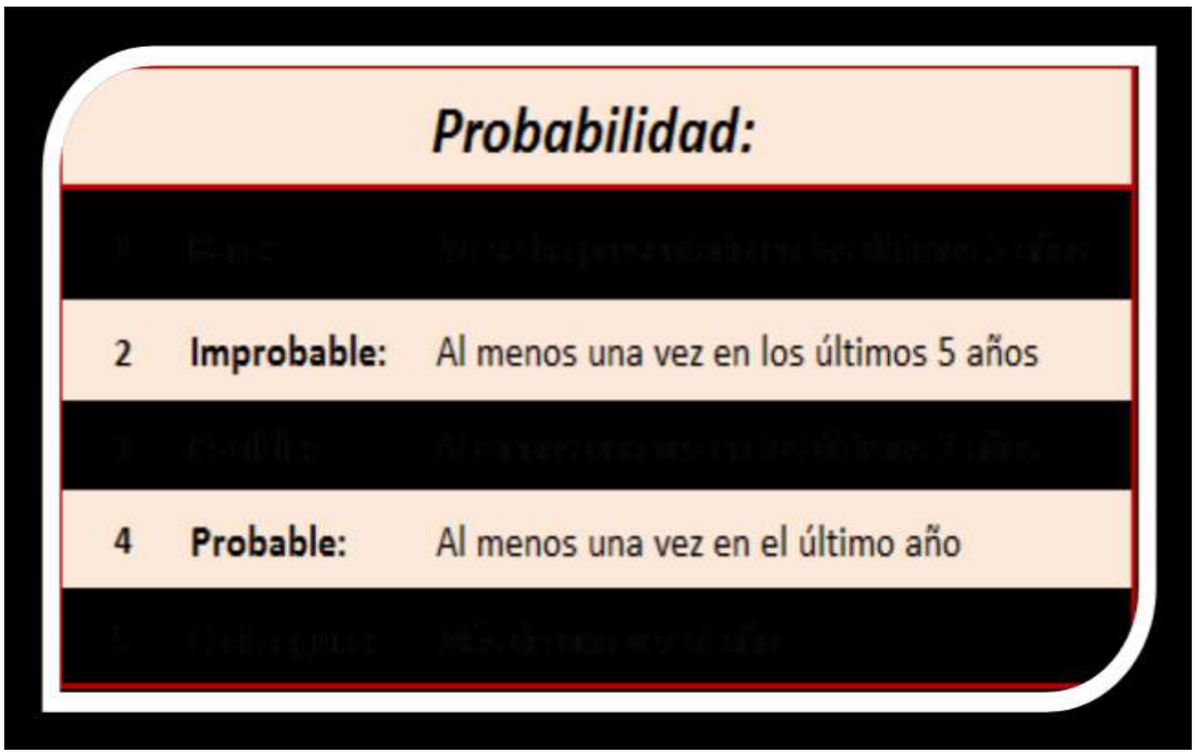

Zona de Riesgos - Probabilidad Vs Impacto

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

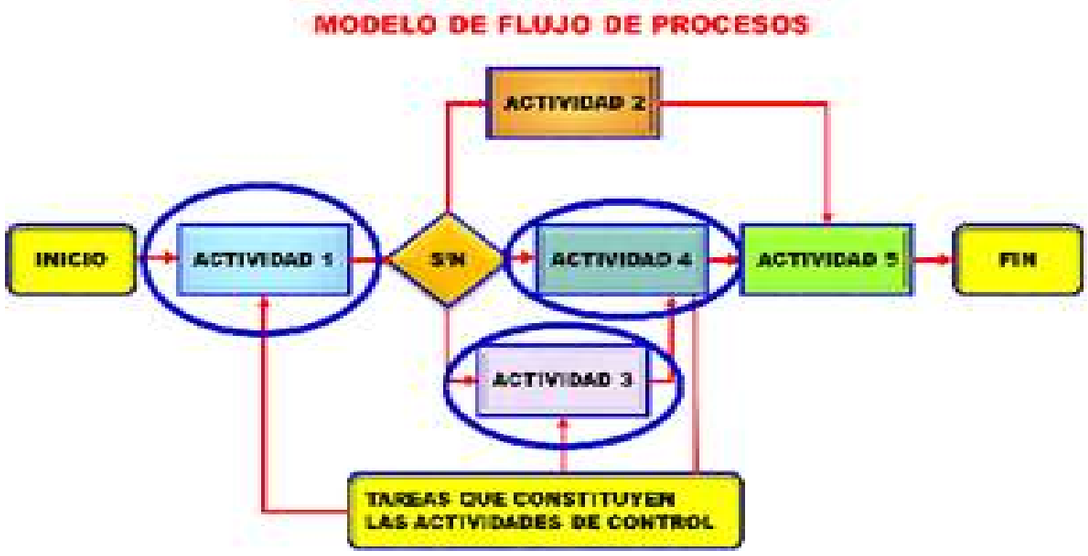



**Probabilidad:** Habla de una vez identificado el riesgo se analiza diciendo que probabilidad en la escala 1 a 5 hay de que se materialice el riesgo.

**Impacto:** Habla si el riesgo se materializa cual es la resultado en la escala de 1 a 5 al ocurrir dicho evento.



## ACTIVIDADES DE CONTROL




Se Define como **CONTROL** toda medida tomada para mitigar o gestionar el riesgo, y para que la probabilidad de que un proceso logres sus metas y sus objetivos sean mayor.

Los controles son actividades incorporadas al proceso que ayudan a prevenir o detectar la ocurrencia de un evento de riesgo, a fin de cumplir los objetivos generales del proceso:

## TIPOS DE CONTROLES

Preventivo: Cuando el punto de control se ubica al inicio del proceso, y las adecuaciones se enfocan a evitar los errores, antes de que afecten al proceso. Corresponden a esfuerzos de prevención y difusión. Anticipan eventos no deseados antes de que sucedan.

Defectivo: Cuando el punto de control se ubica dentro del proceso, y las adecuaciones se enfocan a detectar y compensar los errores o desviaciones, antes de que se elabore el resultado, corresponde a esfuerzos de contención. Identifican los eventos en el momento en que se presentan.

Correctivo: Cuando el punto de control se ubica al final del flujo de proceso, las adecuaciones se enfocan a corregir los errores sobre el resultado obtenido. Corresponden a esfuerzos de restauración, recuperación, rescate o reversión. Aseguran que las acciones correctivas sean tomadas para revertir un evento no deseado.

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

| Significado | | |
|---|---|---|
| | ***Evitar el riesgo*** | **Prevenir su materialización: Cambios sustanciales al interior de los procesos.** |
| | ***Reducir el riesgo*** | **Tomar medidas encaminadas a disminuir Probabilidad e Impacto: Optimización de Procedimientos; implementación de Controles.** |
| | ***Transferir el riesg*** | **Reducir su efecto a través del traspaso de las pérdidas a otras organizaciones: Seguros, Tercerización.** |
| | ***Asumir el riesgo*** | **Aceptar la pérdida residual probable => Planes de Contingencia.** |

| | Opciones de Manejo: | |
|---|---|---|
| Zona | BAJA: | Asumir el riesgo |
| | MODERADA: | Asumir, Reducir el riesgo |
| | ALTA: | Reducir, Evitar, Compartir o Tranferir |
| | EXTREMA: | Reducir, Evitar, Compartir o Tranferir |

**Acciones:**

Son las actividades que vamos a usar para mitigar el riesgo y reducir su probabilidad Además de dar un tiempo de periocidad con su indicador de cumplimiento

Para conocer si se está realizando la reducción del riesgo con las acciones planteadas

Se describen los controles o barreras a ser implementadas que fortalezcan las existes, con lo cual aportar y evitar la materialización del riesgo desde la reducción de la probabilidad y/o del impacto. Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referencias realizas, fortalecimiento de buenas prácticas de seguridad del paciente, asesorías con expertos, entre otras.

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

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

INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACION DEL QUINDIO "INDEPORTES QUINDIO".

MAPA DE RIESGOS INSTITUCIONAL

| Proceso: | SISTEMAS | Año: | 2018 |
|---|---|---|---|
| Objetivo del Proceso: | | | |

| CAUSAS | RIESGO | CONSECUENCIAS POTENCIALES | Tipo de Riesgo | Riesgo Inherente | | Zona de Riesgo | CONTROLES | Tipo de Control | | Evaluación del Control | Riesgo Residual | | Zona de Riesgo | OPCIÓN DE MANEJO | ACCIONES | PERIODICIDAD | RESPONSABLE | REGISTROS | INDICADOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Probabilidad | Impacto | | | A | | | Probabilidad | Impacto | | | | | | | |
| Exposición a redes de datos, dispositivos externos, acceso a páginas diferentes a las institucionales | Equipos de computo existentes infectados con virus informatico | Sobrecostos y parálisis en los procesos ejecutados y el posible robo de información. | Tecnológico | 3 | 4 | EXTREMA | Implementar la política de seguridad y privacidad de información. - Actualizar parches de seguridad- - Restringuir el acceso a paginas que no sean de uso institucional. -Mantener todos los equipos con software de deteccion de archivos dañinos. - Implementacion de software anti ramssoware. | Preventivo | Probabilidad | 45 | 3 | 4 | EXTREMA | Evitar el Riesgo | Implementar en su totalidad la política de seguridad y privacidad de la informacion. -Generar backups diarios para la base de datos de red, -actualizar permanentemente el antivirus institucional | Permanente | Lider Sistemas de información 1 | Acta de socializacion de la política de seguridad y privacidad. -Registro de eventos que sucedan en cada equipo. - | # de equipos de computo con las implementaciones necesarias para su seguridad / # total de equipos del instituto |
| Falta de presupuesto. - Falta de conocimietno de funcionarios de sistemas. | Sistemas operativos en funcionamiento sin licencias | Sanciones por parte de los entes de control | Cumplimiento | 1 | 4 | ALTA | Hojas de vidas de los equipos de computo. -Software libre y open sourse | Preventivo | Probabilidad | 70 | 1 | 4 | ALTA | Reducir el Riesgo | Realizar el inventario de las licencias de los equipos de la entidad. - Diligenciamiento de hojas de vida para detectar incosistencias. | Semestral | Lider Sistemas de información 1 | Hojas de vida de los equipos de computo. | # de equipos con licenciamiento / # total de equipos con que cuenta la entidad. |
| Insuficiente inversión en Sistemas de Información<br><br>Eventos ajenos a la institución (fallas eléctricos) | Softwares en funcionamiento con perdida de la informacion. | Parálisis en los procesos. -informacion suministrada errada por perdida de la informacion. | Tecnológico | 3 | 5 | EXTREMA | Backups de la información Sistemas de alimentacion auxiliar (UPS) | Preventivo | Probabilidad | 70 | 2 | 4 | ALTA | Evitar el Riesgo | Generacion de Backups de la informacion. | Mensual | Lider Sistemas de información 2 | Registro de copias de seguridad firmadas por el funcionario responsable del equipo. | #Backups realizados en cada equipo / # total de equipos en el instituto. |
| Falta de capacitacion de induccion y reinduccion del uso de los sistemas de informacion. | Usuarios realizan de manera deficiente el manejo de los equipos | Parálisis de los servicios. -Retrazo en los procesos. -sobrecostos para la entidad. | Cumplimiento | 3 | 3 | ALTA | Socializacion de politica de seguridad y privacidad de la informacion. -Socializacion de cuidados basicos delos equipos. | Correctivo | Probabilidad | 30 | 3 | 3 | ALTA | Evitar el Riesgo | Realizar la socializacion de la politicada de seguridad y privacidad de la informacion y delos cuidados basico de los equipos de computo. | Semestral | Lider Sistemas de información 1 | Acta de socializacion de la política de seguridad y privacidad. -folleto de cuidados basicos de computo | # de funcionarios capacitados / # total de funcionarios de la entidad. |

# MARCO NORMATIVO

Elaboración de la política general de seguridad y privacidad de la información. Ministerio de las Tic

Ley 1450 de 2011, por el cual se expide el Plan Nacional de Desarrollo 2010

Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad De la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras Disposiciones en el artículo 38 sobre Masificación del uso de las TIC y cierre de la Brecha digital

Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamentan Parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras Disposiciones

Capítulo IV referente a la Gestión de Documentos Electrónicos de Archivo del Decreto 2609 de 2012, por el cual se reglamenta el Título V de la Ley 594 de 2000, Parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras Disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, por la Cual se dictan disposiciones generales para la protección de datos personales.

# REFERENCIAS

https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual

http://www.normas-iso.com/iso-27001/

https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf