



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

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

INSTITUTO MUNICIPAL DE DEPORTE Y RECREACIÓN DE CAJICÁ

ANA KATHERINE ARTUNDUAGA MENDOZA
Director Instituto Municipal de Deportes y Recreación de Cajicá

CAJICÁ 2022



INDEPORTES
CAJICÁ
Unidos con toda seguridad



ALCALDÍA MUNICIPAL
DE CAJICÁ



CAJICÁ
TEJIENDO FUTURO
UNIDOS CON TODA SEGURIDAD

FABIO RAMÍREZ
ALCALDE 2020-2023

Calle 1 Sur No. 7-56 Coliseo Fortaleza de Piedra
E-Mail: ventanillaunica@insdeportescajica.gov.co
Teléfonos: (57+1) 8898746 / Página: www.insdeportescajica.gov.co



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

TABLA DE CONTENIDO

| | |
|---|----|
| 1. INTRODUCCIÓN | 3 |
| 2. MARCO NORMATIVO | 3 |
| 3. OBJETIVOS | 3 |
| 4. ALCANCE | 4 |
| 5. DEFINICIONES | 4 |
| 6. DESCRIPCIÓN DEL PLAN | 5 |
| 7. RIESGOS DE SEGURIDAD DE LA INFORMACION | 5 |
| 8. TIPOS DE RIESGOS | 6 |
| 9. ACTIVIDADES..... | 7 |
| 10. CRONOGRAMA DE ACTIVIDADES | 8 |
| 11. SEGUIMIENTO..... | 14 |
| 12. COMUNICACIÓN..... | 15 |



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

1. INTRODUCCIÓN

El Instituto Municipal de Deporte y Recreación de Cajicá, entendiendo la importancia que es el llevar una adecuada gestión de la información, se desarrolla el plan de tratamiento de riesgos de seguridad y privacidad de la información, el cual permita tener un control para proteger y si es necesario reducir los daños en caso perdidas y daños en la información que tiene el instituto.

2. MARCO NORMATIVO

Cabe mencionar que el presente plan cumple con lo establecido en:

La 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.

El 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".

El 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.

El Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.

La Norma ISO 27001: Sistemas de gestión de la información, es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que se procesan.

3. OBJETIVOS

- Este plan de tratamiento de riesgos de seguridad y privacidad de la información busca el control y la reducción de los riesgos que puedan poner en riesgo la información en el Instituto Municipal de Deporte y Recreación de Cajicá.
- Gestionar los riesgos de Seguridad y Privacidad de la información, de acuerdo con los contextos establecidos en el Instituto Municipal de Deporte y Recreación de Cajicá.
- Hacer el fortalecimiento de la transparencia en la gestión pública del Instituto Municipal de Deporte y Recreación de Cajicá.
- Contar con el monitoreo en tiempo real sobre eventos que puedan suceder



INSDEPORTES
CAJICÁ
Unidos con toda seguridad



ALCALDÍA MUNICIPAL
DE CAJICÁ



CAJICÁ
TEJIENDO FUTURO
UNIDOS CON TODA SEGURIDAD

FABIO RAMÍREZ
ALCALDE 2020-2023

Calle 1 Sur No. 7-56 Coliseo Fortaleza de Piedra
E-Mail: ventanillaunica@insdeportescajica.gov.co
Teléfonos: (57+1) 8898746 / Página: www.insdeportescajica.gov.co

en los equipos de cómputo de la entidad.



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

4. ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información, está dirigido a todos los funcionarios de planta y contratistas los cuales, son parte integral de los riesgos a los que está expuesto el Instituto Municipal de Deporte y Recreación de Cajicá, para así de manera eficiente realizar la gestión de riesgos de seguridad y privacidad de la información, para que se permita integrar en los procesos del Instituto, las buenas prácticas, las cuales contribuyan a la toma de decisiones y se prevengan los incidentes que puedan afectar el logro de los objetivos.

5. DEFINICIONES

Activo de Información: toda aquella información que reside en medio electrónico o físico, que tiene un significado y valor para Colombia Compra Eficiente y, por ende, necesita ser protegida.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Confidencialidad: principio de la Seguridad de la Información que busca asegurar que la información de Colombia Compra Eficiente sea accedida únicamente por personal autorizado (tanto interno como externo a Colombia Compra Eficiente), para suplir una necesidad legítima para la realización de sus funciones, con el fin de prevenir el uso o divulgación de esta en forma no autorizada.

Contenedor de la Información: cualquier plataforma tecnológica o lugar físico que almacena, procesa, transmite un Activo de Información por cualquier lapso o propósito.

Disponibilidad: principio de la Seguridad de la Información que busca asegurar que la información esté disponible cuando sea requerido por los procesos, servicios, ciudadanos y en general partícipes de los procesos de contratación alojados en las plataformas bajo responsabilidad de Colombia Compra Eficiente.

Integridad: principio de Seguridad de la Información que busca asegurar que la información esté protegida contra modificaciones no autorizadas para garantizar su consistencia, exactitud y completitud. Se debe garantizar la trazabilidad de la información.

Proceso: grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de Colombia Compra Eficiente para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio.

Propietario del Activo (o de la Información): funcionario encargado de identificar y establecer el alcance y valor o criticidad de un Activo de Información, los requerimientos de seguridad de este y la comunicación de éstos a los custodios del Activo de Información.



INSDEPORTES
CAJICÁ
Unidos con toda seguridad



ALCALDÍA MUNICIPAL
DE CAJICÁ



CAJICÁ
TEJIENDO FUTURO
UNIDOS CON TODA SEGURIDAD

FABIO RAMÍREZ
ALCALDE 2020-2023

Calle 1 Sur No. 7-56 Coliseo Fortaleza de Piedra
E-Mail: ventanillaunica@insdeportescajica.gov.co
Teléfonos: (57+1) 8898746 / Página: www.insdeportescajica.gov.co



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

Riesgo Residual: Riesgo restante después de aplicar el tratamiento al Riesgo.
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.

Riesgos de seguridad digital: Posibilidad 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.

Seguridad de la Información: Preservación de la Confidencialidad, Integridad y Disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.

Vulnerabilidad: debilidad asociada al Contenedor de un Activo de Información y que puede ser explotada para materializar un Riesgo, causando incidentes no deseados que pueden dar lugar a la pérdida de Confidencialidad, Integridad o Disponibilidad de los Activos de Información.

6. DESCRIPCIÓN DEL PLAN

Identificación del riesgo

El propósito de la identificación del riesgo es determinar las causas de lo que pueda hacer que se materialice una pérdida potencial de la información, y así mismo llegar a comprender el cómo, el dónde, y por qué podría ocurrir esta pérdida.

Causas

Se describe las causas asociadas al riesgo que sea identificado, las cuales pueden ser intrínsecas: atribuidas a personas, métodos, equipos, instalaciones directamente involucradas en el proceso. O Externas: dadas por el entorno en el que se realice el proceso.

Consecuencias:

Se describen los efectos asociados a la materialización del riesgo, los cuales incidan en el objetivo del proceso o de la Entidad. Pueden agruparse en: daños a deportistas, funcionarios o contratistas, pérdidas económicas, perjuicio a la imagen corporativa, sanciones legales, demoras en los tiempos de los procesos, insatisfacción, entre otras.

7. RIESGOS DE SEGURIDAD DE LA INFORMACION

Los riesgos en la seguridad de la información del Instituto Municipal de Deporte y Recreación de Cajicá se pueden clasificar en tres grupos: Actos originados por la criminalidad común, Riesgos por sucesos de origen físico, negligencia de usuarios y decisiones institucionales.



| Actos originados por criminalidad común: | Riesgos por sucesos de origen físico: | Negligencia de usuarios y decisiones institucionales |
|---|---|---|
| <ul style="list-style-type: none"> - Sabotaje (ataque físico y ataque electrónico). - Daños por vandalismo. - Fraude / Estafa. - Robo al bien físico. - Robo al bien electrónico. - Virus digital/ejecución de un programa no autorizado. - Violación a los derechos de autor. | <ul style="list-style-type: none"> - Incendio. - Sismo. - Polvo. - Sobrecarga eléctrica. - Falta de energía (apagones). - Fallas de sistema/Daño de disco duro. | <ul style="list-style-type: none"> - Falta de inducción, capacitación y sensibilización sobre riesgos. - Mal manejo de sistemas y herramientas. - Uso de programas no autorizados/Software ilegal. - Pérdidas de Datos. - Infección de sistema a través de unidades portables sin escaneo. - Manejo inadecuado de datos importantes. - Manejo inadecuado de contraseñas. - Compartir contraseñas personales a terceros no autorizados. - Acceso electrónico no autorizado a sistemas externos. |

8. TIPOS DE RIESGOS

Financieros: Bajo presupuesto el cual puede impedir el desarrollo de los procesos, demoras en apropiación y ejecución de recursos.

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.

Estratégicos: Falta de lineamientos y demoras en la Planeación, estructura organizacional no acordes con los 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.

Confianza e imagen: esto en relación con la percepción de la ciudadanía y la confianza que la ciudadanía le tenga al Instituto.

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.





9. ACTIVIDADES

Las actividades planteadas en la siguiente tabla se presentan con el fin de fortalecer la gestión de los riesgos de la privacidad y seguridad de la información en el Instituto Municipal de Deporte y Recreación de Cajicá.

Para la vigencia 2022 se plantea realizar las siguientes actividades por parte del área encargada.

| Actividades | Descripción |
|---|--|
| 1. Realizar diagnósticos de riesgos de seguridad y privacidad de la información. | Se realizará el diagnóstico del estado de la gestión de riesgos de Seguridad y Privacidad de la Información, a través de los procesos misionales, estratégicos y de evaluación en el Instituto Municipal de Deporte y Recreación de Cajicá. |
| 2. Elaborar el alcance del Plan del Tratamiento de Riesgos de Seguridad y Privacidad de la Información. | Teniendo ya determinado el estado de la estrategia de gestión y tratamiento de riesgos de Seguridad y Privacidad de la Información, se planteará el alcance del Plan del Tratamiento de Riesgos de Seguridad y Privacidad de la Información. |
| 3. Realizar la identificación de los riesgos con los líderes de los procesos | En reuniones y mesas de y trabajo con los líderes, responsables de los procesos, se realizará la identificación de los riesgos de seguridad de la información asociados a cada proceso y la posibilidad de ocurrencia. |
| 4. Valoración de riesgo y del riesgo residual. | Con los resultados de la actividad anterior, se revisará el impacto de la materialización del riesgo, la aceptación del riesgo en la entidad y la identificación del riesgo residual. |
| 5. Plantear el plan de tratamiento de riesgo. | Con la información recolectada en las actividades anteriores y con la participación de los líderes de los procesos, se planteará la estrategia para el tratamiento de los riesgos. |



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

10. CRONOGRAMA DE ACTIVIDADES

| Cronograma de actividades Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información | | | | | | | | | | | | | | | | | | | | |
|---|--------|----|----|----|------------|----|----|----|---------|----|----|----|-----------|----|----|----|-----------|----|----|----|
| ACTIVIDADES | Agosto | | | | Septiembre | | | | Octubre | | | | Noviembre | | | | Diciembre | | | |
| | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 |
| 1. Realizar diagnósticos de riesgos de seguridad y privacidad de la información. | | | x | x | | | | | | | | | | | | | | | | |
| 2. Elaborar el alcance del Plan del Tratamiento de Riesgos de Seguridad y Privacidad de la Información. | | | | | x | x | x | x | | | | | | | | | | | | |
| 3. Realizar la identificación de los riesgos con los líderes de los procesos. | | | | | | | | | x | x | x | x | | | | | | | | |
| 4. Valoración de riesgo y del riesgo residual. | | | | | | | | | | | | | x | x | x | x | | | | |
| 5. Plantear el plan de tratamiento de riesgo. | | | | | | | | | | | | | | | | | x | x | x | x |



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

- Dependencia de partes externas.

En la tabla que aparece en Identificación de amenazas, se pueden ver algunos de los ejemplos de vulnerabilidad y amenazas que sirven de guía, para la de identificar las vulnerabilidades que se puedan presentar.

Definir actividades de control

De deben definir las acciones que hagan que se reduzca, se evite y se transfiera el riesgo, según sea el caso que se presente. También, se debe especificar en esta etapa:

- El alcance de la acción.
- La prioridad con la que se ejecuta.
- Asignar el responsable de la ejecución de acciones.
- El Propósito del control
- Establecer como se realiza la acción
- Hay que indicar que acciones se deben tomar, si llegan a existir observaciones o derivaciones resultantes de la ejecución de control.
- La documentación que soporte la ejecución del control

Las actividades de control son identificadas dentro del contexto que pueden ser preventivas o detectivas, dado que las preventivas, se diseñan para evitar la materialización de un evento no deseado, llevando a la presión de la ocurrencia de algún riesgo que afecte la integridad, la disponibilidad y la confidencialidad de la información; y los controles detectivos, son dirigidos a los eventos que ya se materializaron con el fin de corregir la situación. Es importante que los controles lleven a tratar las Causas/Vulnerabilidades que generan los riesgos, estos controles pueden tratar varias o simplemente una, lo importante es que, sean tratadas de forma efectiva.

11. SEGUIMIENTO

Los Riesgos y sus factores (el Valor de los activos, los impactos, las amenazas, las vulnerabilidades y la probabilidad de su ocurrencia) deberían ser monitoreados para identificar los cambios con los líderes de las áreas del Instituto en una etapa temprana, y para mantener una visión general de la perspectiva del Riesgo.

Para lo anterior, de debe llevar el control documental de las revisiones por el área encargada, la fecha para la implementación de los tratamientos, la frecuencia y un auto seguimiento que los responsables de los tratamientos del Riesgos deben realizar sobre la implementación de los controles, los cuales se realizaran mes tras



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

| | |
|--|---------------------------------------|
| Ausencia de procedimientos para el manejo de información clasificada | Error en el uso |
| Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos | Error en el uso |
| Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información | Hurto de equipo |
| Ausencia de política formal sobre la utilización de computadores portátiles | Hurto de equipo |
| Ausencia de control de los Activos que se encuentran fuera de las instalaciones | Hurto de equipo |
| Ausencia de autorización de los recursos de procesamiento de información | Hurto de medios o documentos |
| Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad | Hurto de medios o documentos |
| Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad | Uso no autorizado de equipo |
| Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales. | Uso de software falsificado o copiado |

Identificación de Vulnerabilidades

En esta etapa se necesita identificar las debilidades que puedan ser explotadas por las amenazas identificadas y que puedan comprometer la confidencialidad, integridad y la disponibilidad de la información.

Se puede llegar a identificar las vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración de los sistemas de información.
- Hardware, software y equipos de comunicaciones.



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

| | | |
|---------------------|---|---|
| | Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería | Uso no autorizado del equipo |
| Organización | Ausencia de procedimiento formal para el registro y retiro de usuarios | Abuso de los derechos |
| | Ausencia de proceso formal para la revisión de los derechos de acceso | Abuso de los derechos |
| | Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad) | Abuso de los derechos |
| | Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información | Abuso de los derechos |
| | Ausencia de procedimientos de identificación y valoración de Riesgos | Abuso de los derechos |
| | Ausencia de reportes de fallas en los registros de administradores y operadores | Abuso de los derechos |
| | Respuesta inadecuada de mantenimiento del servicio | Incumplimiento en el mantenimiento del sistema de información |
| | Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos | Incumplimiento en el mantenimiento del sistema de información |
| | Ausencia de procedimientos de control de cambios | Incumplimiento en el mantenimiento del sistema de información |
| | Ausencia de procedimiento formal para la autorización de la información disponible al público | Datos provenientes de fuentes no confiables |
| | Ausencia de asignación adecuada de responsabilidades en seguridad de la información | Error en el uso |
| | Ausencia de políticas sobre el uso de correo electrónico | Error en el uso |
| | Ausencia de procedimientos para introducción del software en los sistemas operativos | Error en el uso |



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

| | | |
|-----------------|--|--|
| | Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento | Incumplimiento en el mantenimiento del sistema de información. |
| | Ausencia de esquemas de reemplazo periódico | Destrucción de equipos o medios. |
| | Susceptibilidad a la humedad, el polvo y la suciedad | Polvo, corrosión y congelamiento |
| | Sensibilidad a la radiación electromagnética | Radiación electromagnética |
| | Falta de cuidado en la disposición final | Hurtos medios o documentos |
| | Copia no controlada | Hurtos medios o documentos. |
| Red | Ausencia de pruebas de envío o recepción de mensajes | Negación de acciones |
| | Líneas de comunicación sin protección | Escucha encubierta |
| | Tráfico sensible sin protección | Escucha encubierta |
| | Conexión deficiente de los cables | Fallas del equipo de telecomunicaciones |
| | Punto único de fallas | Fallas del equipo de telecomunicaciones |
| | Ausencia de identificación y autenticación de emisor y receptor | Falsificación de derechos |
| | Arquitectura insegura de la red | Espionaje remoto |
| | Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento) | Saturación del sistema de información |
| | Conexiones de red pública sin protección | Uso no autorizado |
| Personal | Ausencia del personal | Incumplimiento en la Disponibilidad del personal |
| | Procedimientos inadecuados de contratación | Destrucción de equipos y medios |
| | Entrenamiento insuficiente en seguridad | Error en el uso |
| | Uso incorrecto de software y hardware | Error en el uso |
| | Falta de conciencia acerca de la seguridad | Error en el uso |
| | Ausencia de mecanismos de monitoreo | Procesamiento ilegal de los datos |
| | Trabajo no supervisado del personal externo o de limpieza | Hurto de medios o documentos. |



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

| | | |
|-----------------|--|---------------------------------|
| | Susceptibilidad a las variaciones de temperatura | Fenómenos meteorológicos. |
| | Almacenamiento sin protección | Hurtos medios o documentos |
| | Falta de cuidado en la disposición final | Hurtos medios o documentos. |
| | Copia no controlada | Hurtos medios o documentos. |
| Software | Asignación errada de los derechos de acceso | Abuso de los derechos |
| | Software ampliamente distribuido | Corrupción de datos |
| | En términos de tiempo utilización de datos errados en los programas de aplicación | Corrupción de datos |
| | Interfaz de usuario compleja | Error en el uso |
| | Ausencia de documentación | Error en el uso |
| | Configuración incorrecta de parámetros | Error en el uso |
| | Fechas incorrectas | Error en el uso |
| | Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario | Falsificación de derechos |
| | Tablas de contraseñas sin protección | Falsificación de derechos |
| | Gestión deficiente de las contraseñas | Falsificación de derechos |
| | Habilitación de servicios innecesarios | Procesamiento ilegal de datos |
| | Software nuevo o inmaduro | Mal funcionamiento del software |
| | Especificaciones incompletas o no claras para los desarrolladores | Mal funcionamiento del software |
| | Ausencia de control de cambios eficaz | Mal funcionamiento del software |
| | Ausencia de copias de respaldo | Manipulación con software |
| | Ausencia de protección física de la edificación, puertas y ventanas | Hurto de medios o documentos |
| | Ausencia o insuficiencia de pruebas de software | Abuso de los derechos |
| | Defectos bien conocidos en el software | Abuso de los derechos |
| | Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo | Abuso de los derechos |
| | Disposición o reutilización de los medios de almacenamiento sin borrado adecuado | Abuso de los derechos |



Identificación De Los Contenedores o Activos De Información

En esta etapa se debe realizar la identificación de los contenedores y activos de la información, los cuales se podrían ver afectados por los riesgos que se puedan presentar, tomando la matriz de identificación de activos, la cual contiene la siguiente información:

- Proceso en el que se encuentra la custodia y tratamiento del activo de la información.
- Clasificación documental (Serie – Subserie).
- Descripción del activo de información.
- Propietario del activo.
- Medio.
- Físico/Electrónico.
- Lugar de almacenamiento Físico / Lugar de almacenamiento Electrónico.

Esta información se deberá actualizar semestralmente y se le deberá hacer el respectivo seguimiento, con el fin de contar con un inventario de los activos de información vigente.

Identificación de amenazas

En esta etapa se realiza la identificación de las amenazas que pueden tener los contenedores o activos de información. Las amenazas tienen el potencial de divulgar, dólar, modificar o hasta eliminar la información. Para lo anterior mencionado se puede usar la siguiente tabla:

| Tipo | Vulnerabilidad | Amenazas |
|----------|--|--|
| Hardware | Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento | Incumplimiento en el mantenimiento del sistema de información. |
| | Ausencia de esquemas de reemplazo periódico | Destrucción de equipos o medios. |
| | Sensibilidad a la radiación electromagnética | Radiación electromagnética |
| | Ausencia de un eficiente control de cambios en la configuración | Error en el uso |
| | Susceptibilidad a las variaciones de voltaje | Pérdida del suministro de energía |



ALCALDÍA MUNICIPAL
DE CAJICÁ
Instituto Municipal de Deporte y Recreación

mes para así llevar un buen control y reducción de las amenazas que se puedan llegar a presentar para la información.

12. COMUNICACIÓN

Todas las novedades sobre los Riesgos de Seguridad de la Información de deberán comunicar al Encargado de Seguridad de la Información y se debe dejar la respectiva documentación asociada la cual puede ser por correo electrónico.

| Responsable | Nombre(s) y apellidos | Firma | Area |
|-------------------------|-------------------------------------|-------|-----------------------|
| Proyectó: | Catherine Nieto Martínez | | Contratista Dirección |
| Revisó y Aprobó: | Ana Katherine Artunduaga Mendoza | | Directora |

Los firmantes, manifestamos expresamente que hemos estudiado y revisado el presente documento, y por encontrarlo ajustado a las disposiciones constitucionales, legales y reglamentarias vigentes, lo presentamos para su firma bajo nuestra responsabilidad.