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

INSTITUTO DISTRITAL DE DEPORTE Y RECREACION - IDER

GINA VIVIANA LONDOÑO
DIRECTORA IDER

Cartagena de Indias D T y C
Departamento de Bolívar
2020

Versión 1.0

TABLA DE CONTENIDO

INTRODUCCIÓN....3

1. OBJETIVO....4
1.1. OBJETIVO GENERAL....4
1.2. OBJETIVOS ESPECIFICOS....4
2. JUSTIFICACIÓN....5
3. MARCO NORMATIVO....6
4. RESPONSABLES....8
5. ALCANCE....9
6. TERMINOS Y DEFINICIONES....10
7. PROCESO DE GESTION DE RIESGO DE SEGURIDAD DE LA INFORMACION....14
8. CONTEXTO ESTRATEGICO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 15
8.1. IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN....16
8.1.1. Análisis de los objetivos estratégicos....16
8.1.2. Análisis de los objetivos de proceso....16
9. IDENTIFICACIÓN DE RIESGOS....18
9.1. TIPOS DE RIESGOS....18
9.2. TÉCNICAS PARA LA IDENTIFICACIÓN DE RIESGOS.....19
10. VALORACIÓN DE RIESGOS....21
10.1. ANALISIS DE IMPACTO....21
10.2. EVALUACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN....23
10.2.1. Análisis Preliminar Riesgo Inherente....23
10.2.2. Valoración de los Controles....24
10.2.3. Nivel de riesgo (Riesgo residual)....24
10.3. MONITOREO Y REVISIÓN....25
10.3.1. Línea Estratégica....26
10.3.1.1. Primera Línea de Defensa....26
10.3.1.2. Segunda Línea de Defensa....26
10.3.1.3. Tercera Línea de Defensa....27
10.3.2. Matriz de Responsabilidad....28
10.4. SEGUIMIENTO AL RIESGO....29
10.4.1. Reportes Periódicos....30
11. COMUNICACIÓN Y CONSULTA....31

INTRODUCCIÓN

La gestión del riesgo es el proceso por el cual se controlan, minimizan o eliminan los riesgos que afectan los activos de información de una Organización. La norma ISO 27005:2011 y la NTC ISO 31000 son estándares internacionales diseñados para la gestión del riesgo en la seguridad de la información que permiten reaccionar ante una posible materialización del riesgo.

El no contar con una adecuada gestión del riesgo de seguridad de la información, en el instituto distrital de deporte y recreación puede traer consecuencias graves, como fuga o perdida de información, alteración de documentos, negación de servicios entre otras, este plan tiene como fin la seguridad de la información bajo los pilares de Integridad, Disponibilidad y Confidencialidad de la información.

1. OBJETIVO

1.1. OBJETIVO GENERAL

Definir el conjunto de actividades, procedimientos, roles y responsabilidades que permitan el sostenimiento de la continuidad en la plataforma tecnológica de la entidad, en caso de ocurrencia de cualquier evento de amenaza o materialización del riesgo.

1.2. OBJETIVOS ESPECIFICOS

- Brindar lineamientos y principios que propendan por la unificación de criterios para la administración de los riesgos de seguridad de la información del instituto distrital de deporte y recreación.
- Continuar con la operación del área con procedimientos informáticos alternos, con miras a que se disponga de los respaldos de información, en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental de las operaciones necesarias, para reconstruir los archivos dañados en una eventual materialización del riesgo.
- Contar con un instructivo de operación para la detección de posibles fallas, a fin de que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Disponer de un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Proyectar el mapa de riesgos informáticos de del instituto distrital de deporte y recreación, donde se establece el contexto.
- Mantener revisiones del plan, con miras a que se efectúen las actualizaciones respectivas.

2. JUSTIFICACIÓN

El Gobierno Nacional a través del Ministerio de las Tecnologías de la Información y Comunicaciones (MINTIC) dentro del marco del Modelo de Seguridad y Privacidad de la Información – MSPI y en virtud a las Políticas de Gobierno Digital, profirió el Decreto N° 612 de 2018, “Por el cual se fijan directrices para la Integración de los planes Institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, estableció la obligatoriedad para las entidades públicas de adoptar y publicar en su página web el “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información”; con miras a viabilizar la integración de los planes institucionales y estratégicos al Plan de Acción de las entidades. Por tal razón, las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos, dentro de los cuales está el aludido, y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año.

En consideración a lo anterior, el instituto distrital de deporte y recreación ha diseñado su “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información”. Con el cual, se propende que la entidad se beneficie con la construcción e implementación de dicho plan, para que se garantice una adecuada gestión del riesgo en esta entidad.

3. MARCO NORMATIVO

Norma	Tema
Política de Gobierno Digital	Para la implementación de la Política de Gobierno Digital, se han definido varios elementos que brindan orientaciones generales y específicas que deben ser acogidas por las entidades, a fin de alcanzar los propósitos de la política. Estos elementos son los siguientes: * Los dos componentes TIC para el Estado y TIC para la Sociedad son líneas de acción que orientan el desarrollo y la implementación de la política. * Los tres habilitadores transversales Arquitectura, Seguridad y privacidad y Servicios Ciudadanos Digitales, son elementos de base que permiten el desarrollo de los componentes de la política.
Decreto 1008 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.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Modelo de Gestión IT4+, versión 02 de 2016	IT4+® es el modelo de gestión sobre el que se construyó la Estrategia TI para Colombia, el cual es un modelo resultado de la experiencia, de las mejores prácticas y lecciones aprendidas durante la implementación de la estrategia de gestión TIC en los últimos 12 años en las entidades del Estado colombiano. IT4+® es un modelo integral que está alineado con la estrategia

	empresarial u organizacional y permite desarrollar una gestión de TI que genere valor estratégico para la organización y sus clientes. Está conformado por los siguientes componentes: Estrategia de TI, Gobierno de TI, Análisis de información, Sistemas de información, Gestión de servicios tecnológicos, Apropiación y uso.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 1078 de 2015	Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014, el cual establece los lineamientos generales de la Estrategia de Gobierno en Línea.
Conpes 3854 de 2016	Política Nacional de seguridad Digital
Ley 1581 de 2012	Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales.
ISO 27005:2011	Estándar internacional diseñado para la gestión del riesgo en la seguridad de la información.
NTC ISO 31000	Norma Técnica Colombiana para la Gestión del riesgo.

4. RESPONSABLES

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del instituto distrital de deporte y recreación, tendrá como responsables de su implementación, a los siguientes:

- Alta dirección de la entidad (Director o su delegado)
- Líder de Seguridad y Sistemas de la Información o quien haga sus veces en la entidad.
- Comité Institucional de Coordinación de Control Interno o quien haga sus veces en la entidad.

5. ALCANCE

En este documento se enmarca la gestión del riesgo para la protección de los sistemas y plataformas tecnológicas descritos a continuación y que soportan los distintos procesos que se surten al interior de la entidad, a la vez que representan el contexto informático del instituto distrital de deporte y recreación.

6. TERMINOS Y DEFINICIONES

OST: Oficina de Sistemas y Tecnología

BCP: Sigla en inglés (Business Continuity Plan) que hace referencia al Plan de Continuidad de Negocio, el cual integra el DRP, planes de contingencia y recuperación de procesos de la entidad, planes de emergencia, y plan de comunicación y administración de crisis.

BIA: Sigla en inglés (Business Impact Analisys), y hace referencia a un documento que identifica la disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la entidad, con el fin de garantizar la continuidad en la prestación del servicio a los usuarios internos y externos.

DRP: Sigla en inglés (Disaster Recovery Plan), que hace referencia al Plan de Recuperación ante Desastres de Tecnología, el cual define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

ERA: Sigla en inglés (Environment Risk Analisys), Análisis de Riesgos Ambientales en español, y hace referencia a un documento que relaciona los riesgos que pueden afectar la continuidad de la plataforma tecnológica de la entidad.

RAS: Sigla en inglés (Response Alternative and Solutions), y hace referencia a un documento que relaciona las diferentes alternativas y estrategias potenciales para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

RPO: Sigla en inglés (Recovery Point Objetive), que corresponde a la cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio.

RTO: Sigla en inglés (Recovery Time Objetive), que corresponde al tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.

PLATAFORMA TECNOLÓGICA CRÍTICA: Hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo,

ider.gov.co
Tel: 6567702 - 6567677. - Fax: 6567708 / 6567709.
Cartagena de Indias, Colombia - Pie de la Popa, Cra.30 No.18A-253.

equipos y enlaces de comunicación que son críticos para soportar los procesos y servicios de la entidad.

DVD. Es un formato de almacenamiento óptico que puede ser usado para guardar datos, incluyendo películas con alta calidad de vídeo y audio. Se asemeja a los discos compactos en cuanto a sus dimensiones físicas (diámetro de 12 u 8 centímetros), pero están codificados en un formato distinto y a una densidad mucho mayor. A diferencia de los CD, todos los DVD deben guardar los datos utilizando un sistema de archivos denominado UDF (Universal Disk Format), el cual es una extensión del estándar ISO 9660, usado para CD de datos.

CD. El disco compacto (conocido popularmente como CD, por las siglas en inglés de Compact Disc) es un soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, vídeo, documentos y otros datos).

DISCO DURO. Elemento de almacenamiento de datos en forma magnética u óptica, constituido por una lámina delgada con forma circular.

UNIDAD DE RED. Es un directorio compartido desde otro equipo por medio de la red y que se ancla a la sesión de un usuario o computadora como una unidad adicional. Su presencia lógica y física está alojada en un equipo físico completamente diferente, el cual puede estar en un lugar geográfico diferente.

ALMACENAMIENTO CONECTADO A LA RED (NAS). Network Attached Storage (NAS), es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

COBIAN BACKUP. Es un programa multitarea capaz de crear copias de seguridad en un equipo, en una red local o incluso en/desde un servidor FTP. También soporta SSL.

RESPALDO COMPLETO. El método básico es el de copia completa o "Full Copy" que realiza una copia directa de los archivos y directorios. Este proceso puede durar horas dependiendo del tamaño de los archivos o directorios a copiar, por lo que este proceso normalmente se ejecuta la primera vez o cada cierto tiempo.

ider.gov.co
Tel: 6567702 - 6567677. - Fax: 6567708 / 6567709.
Cartagena de Indias, Colombia - Pie de la Popa, Cra.30 No.18A-253.

Existen dos métodos más avanzados respecto a la copia completa que son la copia diferencial y la copia incremental. Dichas copias lo que realizan es un proceso de copia más avanzado permitiendo ahorrar tiempo, debido a que no se considera necesario realizar una copia completa cada día si no todos los archivos han sido modificados.

RESPALDO INCREMENTAL. La copia incremental (o diferencial incremental) es la más avanzada al respecto, ya que únicamente copia los ficheros creados o modificados desde el último backup realizado, ya sea de una copia completa o incremental, reduciendo de este modo los archivos a copiar y el tiempo empleado en el proceso de backup.

CONFIDENCIALIDAD: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

INTEGRIDAD: Propiedad de exactitud y completitud.

DISPONIBILIDAD: Propiedad de ser accesible y utilizable a demanda por una entidad.

AMENAZAS: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

MAPA DE RIESGOS: Documento con la información resultante de la gestión del riesgo.

ACTIVO: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

RIESGO DE SEGURIDAD DIGITAL: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como 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.

PROBABILIDAD: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

IMPACTO: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

CAUSA: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

CONSECUENCIA: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

RIESGO INHERENTE: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

RIESGO RESIDUAL: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

GESTIÓN DEL RIESGO: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

RESPALDO DIFERENCIAL. La copia diferencial únicamente copia los archivos y directorios que han sido creados y/o modificados desde la última copia completa. Esto viene a suponer que si el lunes hemos realizado una copia completa y el martes ejecutamos una copia diferencial, únicamente se copiaran los ficheros creados o modificados durante el martes. Este mismo comportamiento se efectuará si la lanzamos el miércoles, tomando la copia completa del lunes como base.

Normalmente las copias diferenciales ocupan más espacio que las incrementales debido a que parten de la base de un único punto fijo en el tiempo (la copia completa inicial).

7. PROCESO DE GESTION DE RIESGO DE SEGURIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información basada en las normas ISO/IEC 31000 e ISO 27005, tomadas como referencia para la adecuada administración de riesgos en la seguridad digital del instituto distrital de deporte y recreación.

8. CONTEXTO ESTRATEGICO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Este contexto de gestión de riesgos de seguridad digital define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de del instituto distrital de deporte y recreación y obtener los resultados esperados, basándose en la identificación de las fuentes que pueden dar origen a la materialización de los riesgos y a las oportunidades en los procesos de esta entidad, en el análisis de las debilidades y las amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para dicha entidad, así como en la probabilidad de su ocurrencia, al igual que en la construcción de acciones que mitiguen los riesgos, en beneficio de que éstos se logren mantener niveles aceptables.

Tipo de Componente	Descripción	Tiempo Tolerable de Interrupción RTO
Aplicaciones	Sistema de Gestión Financiera (SAFE)	24 Horas
	Aplicaciones Ofimáticas	24 Horas
Mensajería	OpenFire	24 Horas
	Correo Institucional	24 Horas
Comunicaciones	Router (ISP)	8 Horas
	Red Interna	4 Horas
Servicios	Dominio Local DNS	24 Horas
	Servidores	24 Horas

	Página Web Institucional	24 Horas
Infraestructura	UPS	24 Horas
	Aires Acondicionados	8 Horas

Contexto de riesgos de seguridad de la información en IDER.

8.1. IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

8.1.1. Análisis de los objetivos estratégicos

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

8.1.2. Análisis de los objetivos de proceso

De esta manera se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, unos archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios). Así la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Elemento / Sitio	Amenazas	Criticidad
Centro de Cómputo	Atentado Terrorista Incendio Inundación Daño Aires Acondicionados Daño Sistema Eléctrico	Alta
Infraestructura Comunicaciones	Switch Core Fibras ópticas de conexión con Centros de Cableado Router Core Router AP Switch Zonal Enlace ISP Otros enlaces Firewall	Media
Infraestructura Servidores	HP SERVER1 (Dominio) HP SERVER2 (Base de Datos) HP SERVER3 (Linux-Endian-Squid My SQL) Proveedor HTTP (Hosting)	Alta
Infraestructura Base de Datos, Almacenamiento y Respaldo	Corrupción de la base de datos Borrado o pérdida de datos Falla total o parcial del HP SERVER2 Falla en Switch LAN Falla total o parcial del servidor de respaldo (VBX)	Alta

Activos de seguridad de la información

9. IDENTIFICACIÓN DE RIESGOS

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

9.1. TIPOS DE RIESGOS

- **Estratégico:** Se asocia con la forma en que se administra la Entidad. Se enfoca a 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 dirección.
- **Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la entidad.
- **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.
- **De 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.
- **De Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
- **De Corrupción:** Se asocian a uso del poder para desviar la gestión de lo público hacia el beneficio privado.
- **Seguridad Digital:** Refiere a la combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de los objetivos institucionales y afectar la autonomía, principios e integridad de la entidad. Incluye aspectos como el ambiente físico y digital, como temas de seguridad de la información.

9.2. TÉCNICAS PARA LA IDENTIFICACIÓN DE RIESGOS.

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

Los responsables de los procesos realizan la identificación de:

- Las causas o factores generadores de riesgos, tanto internos como externos y del proceso, a partir de las debilidades y amenazas identificadas en el contexto estratégico, con preguntas como: ¿Qué puede suceder?, ¿Cómo puede suceder? ¿Cuándo puede suceder?
- Los riesgos que pueden afectar el desempeño de los procesos, para lo cual además de tener en cuenta el contexto estratégico, también se podrán identificar a través de lluvia de ideas y de acuerdo con experiencias anteriores en la entidad.
- Las consecuencias o efectos que se generarían en caso de materializarse los riesgos identificados. ¿Qué consecuencias tendría su materialización?

RIESGO	CAUSAS	TIPO DE RIESGO	CONSECUENCIAS
Pérdida de la información de la entidad	* Falta de planes contingencia que permitan la recuperación en caso de desastres. * Desconocimiento e incumplimiento de las políticas de Seguridad de la Información. * Deficiencias en la Infraestructura Tecnológica para respaldo de Información.	**ESTRATÉGICO**	* Legales, Disciplinarias, Imagen institucional
Imposibilidad de prestar tramites y servicios en línea de cara al ciudadano.	* Indisponibilidad del canal de internet * Indisponibilidad de los servidores. * Fallas eléctricas en el Data Center * Ciberataques a los servicios en línea	**ESTRATÉGICO**	* Información institucional no disponible * Retraso en los resultados * Afectación de la imagen

Ejemplo de Identificación de Riesgos en el IDER.

10. VALORACIÓN DE RIESGOS

Además de la identificación, se realiza la clasificación de cada uno de los riesgos, de acuerdo a los siguientes conceptos:

10.1. ANALISIS DE IMPACTO

Se realiza el análisis de riesgos, a través de la estimación de la probabilidad de su ocurrencia y el impacto o consecuencias que puede causar su materialización, realizando la calificación y evaluación con el fin de estimar la zona de riesgo inicial – Riesgo inherente. Por impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

PROBABILIDAD	IMPACTO				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrofico(5)
Raro(1)	B	B	M	A	A
improbable(2)	B	B	M	A	E
posible(3)	B	M	A	E	E
probable(4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E
B:Zona de Riesgo Baja:Asumir el riesgo					
M:Zona de Riesgo Moderada:Asumir el riesgo,Reducir el riesgo					
A:Zona de Riesgo Alta:Reducir ,Evitar,Compartir o Transferir					
E:Zona de Riesgo extrema:Reducir el riesgo,evitar compartir o transferir					

Matriz de probabilidad de Impacto

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Valores Impacto para riesgos institucionales

La probabilidad de ocurrencia representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede llegar a presentarse y el impacto hace referencia a la magnitud de sus efectos.

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Criterios parar calificar la probabilidad

10.2. EVALUACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

10.2.1. Análisis Preliminar Riesgo Inherente

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

VALORACION DEL RIESGO	
NIVEL DE RIESGO INHERENTE	**CALIFICACION**
EXTREMO	41 A 75
ALTO	21 A 40
MODERADO	11 A 20
BAJO	1 A 10

Tabla valoración del Riesgo

RIESGO	CAUSAS	TIPO DE RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	EVALUACION DEL RIESGO	NIVEL DE RIESGO INHERENTE
Pérdida de la información de la entidad	* Falta de planes contingencia que permitan la recuperación en caso de desastres. * Desconocimiento e incumplimiento de las políticas de Seguridad de la Información. * Deficiencias en la Infraestructura Tecnológica para respaldo de Información.	ESTRATÉGICO	* Legales, Disciplinarias, Imagen institucional	4	15	60	EXTREMO

Ejemplo de Calificación del Riesgo

10.2.2. Valoración de los Controles

CONTROLES EXISTENTES		TIPO DE CONTROL	PERIODICIDAD DEL CONTROL	PRODUCTO (TIPO x PERIODICIDAD)	EFICACIA CONTROL	VALORACION DEL CONTROL	GRADO DE EXPOSICION (RESIDUAL)	NIVEL DE RIESGO RESIDUAL	RESPONSABLE
* Copias de Seguridad * Contar con un Datacenter Alterno que garantice la continuidad del Servicio. * Políticas de Seguridad de la Información.	3	4	3	12	ALTO	4	15	MODERADO	• Líder de Seguridad y Sistemas de la Información o quien haga sus veces en la entidad

Ejemplo de Valoración de Controles

La valoración de controles, evalúa los controles existentes en la organización y la efectividad para mitigar la exposición al riesgo.

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

- Debe tener definido el responsable de llevar a cabo la actividad de control.
- Debe indicar cuál es el propósito del control.
- Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
- Debe tener una periodicidad definida para su ejecución.
- Debe establecer el cómo se realiza la actividad de control.
- Debe dejar evidencia de la ejecución del control.

Estos controles se basan en la gestión operativa y de aseguramiento, de zonas físicas, accesos, manipulación de hardware, software, accesos a sitios web, manejo de la información, entre otros.

10.2.3. Nivel de riesgo (Riesgo residual)

Esta etapa busca establecer tanto la probabilidad de ocurrencia del riesgo como la consecuencia o impacto final, teniendo en cuenta la calificación realizada a los controles existentes para gestionarlos. El propósito de estimar la zona de riesgo

ider.gov.co
Tel: 6567702 - 6567677. - Fax: 6567708 / 6567709.
Cartagena de Indias, Colombia - Pie de la Popa, Cra.30 No.18A-253.

después de la identificación de los controles, los cual nos permite conocer el riesgo residual.

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

VALORACION DEL RIESGO (residual)	
NIVEL DE RIESGO RESIDUAL	**CALIFICACION**
EXTREMO	> 37
ALTO	23 a 36
MODERADO	9 a 22
BAJO	<8

VALORACION DEL RIESGO (residual)

10.3. MONITOREO Y REVISIÓN

El Instituto distrital de deporte y recreación, debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad. El modelo integrado de plantación y gestión (MIPG) en la dimensión 7 “Control interno” desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control. Este modelo de control establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

El monitoreo y revisión de la gestión de riesgos está alineado con la dimensión del MIPG de “Control interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y

roles, el cual se distribuye en diversos servidores de la entidad a través de su línea estratégica así:

10.3.1. Línea Estratégica

Es el marco general para la gestión del riesgo y el control y supervisión de su cumplimiento, está a cargo de la alta dirección y el comité institucional de coordinación de control interno o quien haga sus veces en la entidad, enmarcadas en una operatividad con tres líneas de defensas.

10.3.1.1. Primera Línea de Defensa

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.

Rol principal: diseñar, implementar y monitorear los controles, además de gestionar de manera directa en el día a día los riesgos de la entidad. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.

10.3.1.2. Segunda Línea de Defensa

Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende. A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros.

Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

10.3.1.3. Tercera Línea de Defensa

Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. A cargo de la oficina de control interno, auditoría interna o quien haga sus veces.

El rol principal: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I.

El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I.

10.3.2. Matriz de Responsabilidad

Es el reporte de la gestión del riesgo de seguridad digital, para este caso se reporta el mapa de riesgo y planes de tratamiento.

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	**Pérdida de la integridad**	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	**Probable**	**Menor**	**Moderado**	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018	
					"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

Ejemplo de Formato mapa y plan de tratamiento de riesgos de seguridad digital

El tratamiento del riesgo se basa en la ejecución de las tareas definidas como acciones para mitigar, determinadas en las matrices de identificación de riesgos y validadas según se describió anteriormente; para tal fin, deben establecerse los responsables de éstas y fijar fechas para su implementación sin olvidar que también deben velar por el cumplimiento en el desarrollo e implementación de dichas tareas.

El responsable de seguridad digital o quien haga sus veces en la entidad apoyará y acompañará a las diferentes líneas de defensa tanto para el reporte como para la gestión y el tratamiento de estos riesgos.

En los riesgos de seguridad digital se genera indicadores para medir la gestión realizada en cuanto a la eficacia y la efectividad de los planes de tratamiento implementados.

La entidad debería definir como mínimo 2 indicadores por proceso de la siguiente manera:

- 1 indicador de eficacia que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.
- 1 indicador de efectividad para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

10.4. SEGUIMIENTO AL RIESGO

Una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

Es importante que el instituto distrital de deporte y recreación cuente con el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar. El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

10.4.1. Reportes Periódicos

El responsable de seguridad digital se reportara periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

- Mapa de Riesgo y Plan de tratamiento de Riesgo
- Listado de Activos Críticos TI/TO y Listado de ICC.
- Reporte de criticidad/Impacto de la entidad.
- Reporte de la evolución del riesgos y modificación del apetito del riesgo.
- Impacto económico que podría presentarse frente a la materialización de los riesgos.

11. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas, tanto internas como externas, tendrán lugar durante todas las etapas del proceso para la gestión del riesgo, ya que constituye un elemento transversal a todo el proceso al involucrar a todos los funcionarios para el levantamiento de los mapas de riesgos. El instituto distrital de deporte y recreación determina las siguientes acciones:

- Los líderes y responsables de cada proceso deben divulgar y sensibilizar al interior de sus dependencias el mapa de riesgos junto con el plan de tratamiento y políticas de operación que se derivan.
- La Oficina Asesora de Planeación y la Oficina de Control Interno, impulsarán a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos.
- Las acciones de tratamiento de los riesgos priorizados que involucren partes interesadas o terceros, serán dadas a conocer, por parte de los líderes y responsables de cada proceso.

12. CONTROL DE CAMBIOS

FECHA	AUTOR	VERSIÓN	CAMBIOS
24 de Enero 2020	Oficina de sistemas	1.0	Versión Inicial

MAPA DE RIESGOS TIC 2020																											
Identificación del riesgo							Calificación del riesgo				Valoración del riesgo								Plan de tratamiento del riesgo							
Nº DE RIESGO	PROCESO, PRODUCTO O LINEAMIENTO	OBJETIVO DEL PROCESO O DEFINICIÓN DEL PRODUCTO O LINEAMEINTO	RIESGO	CAUSAS	TIPO DE RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	EVALUACION DEL RIESGO	NIVEL DE RIESGO INHERENTE	CONTROLES EXISTENTES		TIPO DE CONTROL	PERIODICIDAD DEL CONTROL	PRODUCTO (TIPO x PERIODICIDAD)	EFICACIA CONTROL	VALORACION DEL CONTROL	GRADO DE EXPOSICION (RESIDUAL)	NIVEL DE RIESGO RESIDUAL	ACCIONES	RESPONSABLE	CRONOGRAMA	INDICADOR	% AVANCE	DESCRIPCION DE LA ACCION EJECUTADA	% AVANCE	DESCRIPCION DE LA ACCION EJECUTADA
1	Gestión de Información y Tecnología	Garantizar la disponibilidad y uso de las tecnologías necesarias en las operaciones y procesos de la Alcaldía de Santa Rosa de Lima y la conservación del conocimiento institucional	Pérdida de la información de la entidad	* Falta de planes contingencia que permitan la recuperación en caso de desastres. * Desconocimiento e incumplimiento de las políticas de Seguridad de la Información. * Deficiencias en la Infraestructura Tecnológica para respaldo de Información.	**ESTRATÉGICO**	* Legales, Disciplinarias, Imagen institucional	4	15	**60**	**EXTREMO**	* Copias de Seguridad * Contar con un Datacenter Alterno que garantice la continuidad del Servicio. * Políticas de Seguridad de la Información.	3	4	3	12	**ALTO**	4	**15**	MODERADO	* Apertura de Cuentas SYNC para respaldo de archivos y documentos * Contar con un Datacenter Alterno que garantice la continuidad del Servicio. * Programar de forma periódica capacitaciones e inducciones en Políticas de Seguridad de la Información.	**• Líder de Seguridad y Sistemas de la Información o quien haga sus veces en la entidad**	**Agosto de 2020**	Ejecutado Parcialmente Ejecutado			60%	* Cuentas SYNC creadas para los Jefes de Sistemas. * Servicio recurrente de respaldos instalado y configurado con Cobian Backup en los equipos de Jefes de División. * Se mantiene una máquina virtual en un equipo alterno para contingencia en caso de que el principal falle. * Se entregará un Cronograma de Capacitación e Inducción a Políticas de Seguridad de la Información.