PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD

2022-2023

INSTITUTO DE LA JUVENTUD EL DEPORTE Y LA RECREACION DE BUCARAMANGA

INDERBU
Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga

INTRODUCCIÓN

En el país se viene adelantando la implementación de la política de gobierno digital, como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC 1078 de 2015, como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual, se ha articulado con el Modelo Integrado de Planeación y Gestión como una herramienta para el cumplimiento de metas de las políticas de desarrollo administrativo.

El Manual de Política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

La implementación de la política de Gobierno Digital se ha definido en dos componentes: TIC para el Estado y TIC para la sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

El habilitador de seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la información –MSPI-.

El manual de las políticas de gobierno digital está amparado en el Decreto 1008 del 2018, que en su artículo 2.2.9.1.1.3 define que la política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos adoptados en Colombia, en particular, al principio de Seguridad de la Información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

La implementación del habilitador de seguridad de la información, toma como sustento los lineamientos propuestos por el Ministerio de Tecnologías de Información y de las Comunicaciones, a través del Modelo de Seguridad y Privacidad de la Información –MSPI-, quien expresa que la adopción del mismo, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

El Modelo de Seguridad y Privacidad de la Información toma como sustento el estándar NTC ISO 27001:2013 o Sistema de Gestión de Seguridad de la Información y los principios legales de la Ley 1712 de 2014; resaltando que tanto el estándar en mención, como el modelo, conciben obligatorio la identificación, valoración, tratamiento y gestión de los riesgos de seguridad, coincidiendo con los objetivos específicos de la política de Seguridad Digital, en cuanto al establecimiento de un marco institucional para la seguridad digital, consistente con un enfoque de gestión de riesgos, enfatizando en la implementación por parte del gobierno nacional a un modelode gestión de riesgos de seguridad digital.

En atención a lo anterior, el INSTITUTO DE LA JUVENTUD EL DEPORTE Y LA

RECREACION DE BUCARAMANGA -INDERBU expide la guía para riesgos de gestión, corrupción y seguridad digital; en el que se propone una metodología para la administración de riesgos y en particular, expide el modelo de gestión de riesgos de seguridad digital, como un documento anexo a la guía.

Estos referentes constituyen el fundamento para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información.

OBJETIVO

Presentar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del INSTITUTO DE LA JUVENTUD EL DEPORTE Y LA RECREACION DE BUCARAMANGA -INDERBU, en atención a lo dispuesto en el decreto 612 de 2018, como parte activa de la Política de Seguridad de la Información adoptada por la entidad; mediante el cual se definen las acciones para fortalecer las capacidades institucionales en el tratamiento de los riesgos de seguridad y privacidad de la información en la entidad.

ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto de la Juventud, el Deporte y la Recreación – INDERBU, para la vigencia 2021, está orientado a gestionar los riesgos de seguridad digital asociados a la plataforma tecnológica y servicios de tecnologías de información y comunicaciones, que apoyan el desarrollo de las diferentes actividades asociadas al modelo de operación por procesos adoptados en la entidad.

AVANCES DE LA ENTIDAD EN EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El INSTITUTO DE LA JUVENTUD EL DEPORTE Y LA RECREACION DE BUCARAMANGA - INDERBU, ha priorizado el proceso de tecnologías de información y de las comunicaciones, en atención al impacto que tiene el mismo sobre los procesos estratégicos, misionales y de apoyo; ya que actualmente, desde la secretaría de Innovación Digital se coordinan todas las actividades de adquisición, implementación y mantenimiento de tecnologías de información y de las comunicaciones para la entidad, por lo cual, una afectación a este proceso, tendrían un impacto alto para el logro de los objetivos institucionales.

Sin lugar a dudas, el valor de la seguridad informática de cualquier organización debe redundar en la protección de activos de tecnologías de información, de allí la relevancia de contar con la información que se toma como base para realizar las actividades orientadas a la identificación de riesgos y los planes de tratamiento de datos requeridos para mantener un nivel de riesgo aceptable.

ELEMENTOS DE CONFIGURACIÓN
CATEGORÍA DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN
ACCESOS
ALMACENAMIENTO
APLICACIONES
BANDA ANCHA
BASES DE DATOS MySQL
DISPOSITIVOS
PC´S

PORTATILES
PUNTOS DE ACCESO INALAMBRICO AP´S
SERVIDORES
SISTEMAS DE INFORMACIÓN
SOFTWARE
SWITCHES

Una vez se consolidó la información, se consolida el siguiente inventario que precisa información sobre el proceso, tipo de activo según la guía del Ministerio de Tecnologías de Información y de las Comunicaciones, grupo de activo y tipo de activo según la base de datos de elementos de configuración que la conforman:

N°	PROCESO	TIPO DE ACTIVO SEGÚN GUÍA MINTIC	AGRUPACIÓN DE ACTIVO	TIPO DE ACTIVO
1	TIC	HARDWARE	ESTACION DE USUARIO	PC´S
2	TIC	HARDWARE	ESTACION DE USUARIO	PORTATILES
3	TIC	HARDWARE	ESTACION DE USUARIO	ESTACIONES DE INGENIERIA
4	TIC	COMPONENTES DE RED	TELECOMUNICACIONES	PUNTOS DE ACCESO INALAMBRICO AP´S
5	TIC	COMPONENTES DE RED	TELECOMUNICACIONES	SWITCHES
6	TIC	COMPONENTES DE RED	TELECOMUNICACIONES	DISPOSITIVOS
7	TIC	COMPONENTES DE RED	TELECOMUNICACIONES	TELÉFONOS
8	TIC	SOFTWARE	SOFTWARE	SOFTWARE
9	TIC	SOFTWARE	SOFTWARE	APLICACIONES
10	TIC	INFORMACION	BASE DE DATOS	BASES DE DATOS MySQL
11	TIC	SERVICIOS	SISTEMA DE INFORMACIÓN	SISTÉMAS DE INFORMACIÓN
12	TIC	SERVICIOS	SERVIDORES	ALMACENAMIENTO
13	TIC	SERVICIOS	SERVIDORES	SERVIDORES
14	TIC	SERVICIOS	CONECTIVIDAD	ACCESOS
15	TIC	SERVICIOS	CONECTIVIDAD	BANDA ANCHA
16	TIC	SERVICIOS	CONECTIVIDAD	DEDICADOS

17	TIC	SERVICIOS	SERVICIOS	CORREO ELECTRÓNICO CORPORATIVO
18	TIC	INSTALACIONES	INSTALACIONES	CENTRO DE DATOS CORPORATIVO

El grupo de Servicios se define para incluir prioritariamente el correo electrónico corporativo, ya que sobre este servicio se utilizan un número considerable de cuentas, que se convierten en elementos importantes para la evaluación de riesgos; de igual manera, se incluye el centro de datos corporativos, por ser el lugar central donde se aloja toda la infraestructura de tecnologías de información. A partir de la identificación, se procede con la valoración de los activos de tecnologías de información, la cual se realiza a nivel de tipos de elementos frente a criterios como la confidencialidad, la integridad y la disponibilidad; tomando como referencia la criticidad del activo frente a estos criterios, los cuales, se usaron posteriormente para definir el tipo de criticidad del activo de tecnologías de información.

A continuación, se presenta la tabla de valoración de los activos de tecnologías de información definiendo, por cada categoría y la cantidad, la valoración desde los 3 criterios definidos y con base en ellos, establecer la criticidad del activo en la organización.

VALORACIÓN DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN				
CATEGORÍA DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**CRITICIDAD**
PC´S	1	1	1	BAJA

PORTATILES	1	1	1	BAJA
ESTACIONES DE INGENIERIA	1	1	1	BAJA
PUNTOS DE ACCESO INALAMBRICO AP´S	2	1	2	MEDIA
SWITCHES	1	1	2	BAJA
DISPOSITIVOS	1	1	2	BAJA
TELÉFONOS	2	2	1	ALTA
SOFTWARE	1	1	1	BAJA
APLICACIONES	3	2	2	ALTA
BASES DE DATOS MySQL	3	3	2	ALTA
SISTÉMAS DE INFORMACIÓN	3	2	2	ALTA
ALMACENAMIENTO	3	2	2	ALTA
SERVIDORES	2	2	2	MEDIA
ACCESOS	1	1	2	BAJA
BANDA ANCHA	1	1	2	BAJA
CORREO ELECTRÓNICO CORPORATIVO	3	2	3	ALTA
CENTRO DE DATOS				

CORPORATIVO	3	2	3	ALTA

La identificación y valoración de activos es una de las actividades más relevantes para la organización y se convierte en un insumo fundamental para la identificación de riesgos de seguridad informática, sin embargo, el primer factor relevante para la identificación de los mismos es el alcance, para lo cual se ha definido la evaluación de riesgos.

A partir de las agrupaciones realizadas se inició el proceso de identificación de riesgos, para lo cual se identifican amenazas y vulnerabilidades. No obstante, sobre un grupo de activos se pueden identificar diferentes riesgos, tal como se evidencia en la siguiente tabla:

RIESGOS POR GRUPOS DE CATEGORÍAS DE ACTIVOS DE TECNOLOGÍASINFORMACIÓN			
ESCENARIO DE RIESGO	**GRUPO DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN**	**AMENAZA**	**VULNERABILIDAD**
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de operadores de botnets, debido a una falta o	SERVIDORES	Operadores de Botnets	Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos

deficiencia en controles sobrela detección, prevención, recuperación para proteger contra códigos maliciosos.			
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de Spyware/Malwar e, debido a una falta o deficiencia en controles sobrela detección, prevención, recuperación para proteger contra códigos maliciosos.	SERVIDORES	Spyware/Malware	Falta o deficienciaen controles sobrela detección, prevención, recuperación para proteger contra códigos maliciosos
Compromiso de la disponibilidad,	ESTACIONES DE USUARIO	Operadores de Botnets	Falta o deficiencia en controles sobre

integridad o confidencialidad de los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería, por acción de operadores botnets, debido a una falta o deficiencia en			la detección, prevención, recuperación para proteger contra códigos maliciosos
Compromiso de la disponibilidad, integridad o confidencialidad de los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería, por acción de Spyware/Malware, debido a una falta o deficiencia en controles	ESTACIONES DE USUARIO	Spyware/Malware	Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos

sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.			
Compromiso de la disponibilidad, integridad o confidencialidad de los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería, por acción de Spyware/Malware , debido a una falta o deficiencia en controles para los medios removibles.	ESTACIONES DE USUARIO	Spyware/Malware	Falta o deficienciaen controles para los medios removibles.
Afectación de la disponibilidad, integridad o confidencialidad	SERVIDORES	Hackers	Falta o deficiencia en controles de seguridad informática en la

de los servidores, por acción hackers, debido a una falta o deficiencia en controles de seguridad informática en la gestión de las redes.			gestión de las redes
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles sobre el acceso a redes y servicios en red.	SERVIDORES	Hackers	Falta o deficiencia en controles sobre el acceso a redes y servicios en red.
Afectación de la disponibilidad, integridad o confidencialidad de los	SERVIDORES	Hackers	Falta o deficiencia en controles que garanticen el procedimiento de ingreso seguro de

servidores, por acción hackers, debido a una falta o deficiencia en controles que garanticen el procedimiento de ingreso seguro de inicio de sesión.			inicio de sesión.
Afectación de la disponibilidad, integridad o confidencialidad de lossistemas de información web,por acción de hackers, debido auna falta o deficiencia en controles que garanticen el adecuado análisisy especificaciónde requisitos de seguridad informática en los sistemas de	SISTEMAS DE INFORMACIÓN	Hackers	Falta o deficienciaen controles que garanticen el adecuado análisisy especificación de requisitos de seguridad informática en lossistemas de información.

información.			
Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de atacantes internos, debido a una falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información.	SISTEMAS DE INFORMACIÓN	Atacante interno (insider)	Falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información

afectación de la disponibilidad, integridad o confidencialidad de los sistemasde información web, por acciónde grupos criminales, debido a una faltao deficiencia encontroles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información.	SISTEMAS DE INFORMACIÓN	Grupos criminales	Falta o deficienciaen controles que garanticen el adecuado análisisy especificación de requisitos de seguridad informática en lossistemas de información.

Afectación de la confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en el establecimiento y cumplimiento de una política sobre el uso de controles criptográficos.	SISTEMAS DE INFORMACIÓN	Hackers	Falta o deficiencia en el establecimiento y cumplimiento de una política sobre el uso de controles criptográficos.
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de hackers, debido a una falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades	SERVIDORES	Hackers	Falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas.

técnicas.			
Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de atacantes internos, debido a una falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas.	SERVIDORES	Atacante interno(insider)	Falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas.
Afectación de la disponibilidad de los accesos a internet dedicados, por acción dehackers, debido a una falta o deficiencia en el mantenimiento y control de las redes, que	CONECTIVIDAD	Hackers	Falta o deficiencia en el mantenimiento y control de las redes, que dificulta la protección contra las amenazas y la gestión de seguridad de los sistemas y aplicaciones que usan la red.

dificulta la protección contralas amenazas y lagestión de seguridad de los sistemas y aplicaciones que usan la red.			
Afectación dela disponibilidadde los servidores y almacenamiento del correo electrónico, por acción de spam, debido a	SERVICIOS	Spam	Falta o deficienciaen controles sobrela detección, prevención, recuperación para proteger contra códigos maliciosos.
Afectación de la integridad de los motores de bases de datos, por acción de atacantes internos, debidoa una falta o deficiencia en controles que	INFORMACIÓN	Atacante interno (insider)	Falta o deficienciaen controles que garanticen el adecuado registrode eventos y actividad en los activos informáticos

garanticen el adecuado registro de eventos y actividad en los activos informáticos.			
Afectación de la integridad, disponibilidad y confidencialidad del servicio de correo electrónico institucional, por acción de Phishing, debido a una alta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática.	SERVICIOS	Phishing	Falta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática

A partir de la identificación de riesgos sobre los activos de tecnologías de información y de acuerdo con la versión 3.0.1 de la guía de gestión de riesgos publicada por el Ministerio de Tecnologías de Información y Comunicaciones, se realiza la valoración del riesgo inherente, para lo cual se toma como concepto base, la inexistencia de controles y la probabilidad de ocurrencia de un evento, así como

el impacto de la ocurrencia, a partir de los cuales, se define la calificación del riesgoinherente.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN POR CATEGORÍAS FRENTEA CIBERAMENAZAS

El plan describe las actividades más relevantes a realizar en el período 2022, de tal manera que orienten el que hacer de la organización para afrontar los riesgos, tal como se refleja en la siguiente tabla:

NO.	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	TIEMPO
1	Sensibilización, Socialización y Capacitación a responsables de los Activos de Tecnologías Información,sobre el proceso de identificación, valoración, tratamiento y gestión de riesgos.	Subdirección Administración y financiera (Sistemas)	01/May/2022 31/Dic/2022
2	Actualización de la valoración de Riesgos de seguridad informática.	Subdirección Administración y financiera (Sistemas).	01/Jul/2022 30/Nov/2022
3	Identificación y valoración de nuevos Riesgos asociados a cada Categoría.	Subdirección Administración y financiera (Sistemas)	01/Oct/2022 31/Nov/2022
4	Evaluación de los Controles de seguridad informática Implementados.	Subdirección Administración y financiera (Sistemas)	01/Oct/2022 31/Nov/2022

5	Actualizar el Plan de Tratamiento de Riesgos frente.	Subdirección Administración y financiera (Sistemas)	01/Nov/2022 31/Dic/2022

El desarrollo de las actividades estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; mientras que la valoración de los riesgos y sus tratamientos estará delimitada por el requerido apoyo de la alta dirección, en cuanto al apetito de riesgo corporativo que han adoptado, para afrontar el desarrollo y cumplimiento de las actividades planificadas.

CONTROL DE CAMBIOS

VERSIÓN	VIGENCIA	DESCRIPCIÓN DEL CAMBIO
01	30/01/2023	Creación del documento.

CONTROL DE DOCUMENTOS

CONTROL DE DOCUMENTOS			
ELABORÓ: Nombre: Silvia Nathalia Niño V. Cargo: Subdirector Administrativa y Financiera	**REVISÓ:** Comité Institucional de Control Interno	**APROBÓ:** Nombre: Eliana León de Ordoñez Cargo: Director General	**FECHA DE APROBACIÓN:** 30/01/2023