

INDERBU Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

PROCEDIMIENTO GESTION DE INCIDENTES


INSTITUTO DE LA JUVENTUD EL DEPORTE Y LA RECREACION DEBUCARAMANGA



INDERBU <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS	4
3. ALCANCE	5
4. TERMINOS Y DEFINICIONES	6
5. MARCO NORMATIVO	9
6. DESARROLLO DE LA ACTIVIDAD	10
Descripción de actividades a realizar	10
Procedimiento de Gestión de Incidentes de Seguridad de la Información	10
7. ROLES Y RESPONSABLES	16
8. CONTROL DE CAMBIOS	17

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

1. INTRODUCCION

Mediante el presente documento se establece un manual de procedimientos mediante los cuales todos los colaboradores del INDERBU ya sean funcionarios de planta o contratistas tengan conocimiento de las acciones o procedimientos a seguir en el momento de ocurrencia de un incidente que vulnere la seguridad de la información del instituto.

2. OBJETIVO


El objetivo principal es proporcionar las herramientas para gestionar de manera oportuna los eventos e incidentes de seguridad de la información que signifiquen la vulnerabilidad de los principios de la seguridad de la información como lo son; la confidencialidad, la confiabilidad, la integridad y disponibilidad de la información del instituto de la juventud, el deporte y la recreación de Bucaramanga.

3. ALCANCE

Este procedimiento deberá ser aplicado para la gestión de todos los Eventos e Incidentes de Seguridad de la Información al interior del instituto de la juventud, el deporte y la recreación de Bucaramanga, iniciando desde el reporte hasta el cierre y finalización del incidente,

desarrollando las siguientes actividades:

- Reporte y registro del evento y/o incidente de seguridad de la información.
- Evaluación inicial del reporte.
- Análisis y evaluación del impacto.
- Aplicación de acciones de contención y acciones complementarias.

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

- Documentación de lecciones aprendidas.
- Notificación de cierre del evento y/o incidente

4. TERMINOS Y DEFINICIONES


Evento: La ocurrencia detectada en un estado de un sistema de información, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas (controles) o una situación desconocida hasta el momento y que puede ser relevante para la seguridad de la información.

Incidente: Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una política de seguridad o de tratamiento de la información personal de la Instituto de la juventud, el deporte y la recreación de Bucaramanga.

Activo de información: Es todo recurso que genera, procesa, transporta y/o resguarda información necesaria para la operación y el cumplimiento de los objetivos del Instituto de la juventud, el deporte y la recreación de Bucaramanga.

Información: Es cualquier forma de registro electrónico, óptico, magnético o en otros medios previamente procesados en varios datos que pueden ser almacenados o distribuidos y sirven para análisis, estudios, toma de decisiones, ejecución de un proceso o entrega de un servicio; y se constituye en un activo de información del INDERBU.

Seguridad de la información: Se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información, mediante la definición de estrategias, políticas y lineamientos.

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

Falsa Alarma: Reporte de evento que no cumple con la característica de afectación de la Confidencialidad, Integridad y Disponibilidad de la Información.

Niveles de clasificación de la información: Nivel asignado (Confidencial, Privada, Interna o Pública) a la información en función de los requisitos legales, valor de la información, criticidad y susceptibilidad a la divulgación o modificación no autorizada.

Ciberseguridad: Es la protección de los activos de información digitales, considerando las amenazas a la información, procesada, almacenada y transportada por sistemas o aplicaciones interconectados.

Amenaza: Todo evento previsible o no, que pueda afectar a las personas, bienes e información


Alta Dirección: Es la Gerencia General, Subgerencia General y miembros del Comité de Gestión de Seguridad de la Información.

Confidencialidad: Es el atributo de la seguridad de la información que permite que la información tenga acceso sólo al personal autorizado.

Disponibilidad: Es el atributo de la seguridad de la información que está relacionado con la garantía de que la información pueda ser utilizada en el momento que se la requiera por el personal autorizado.

Integridad: Es el atributo de la seguridad de la información para que la información mantenga su totalidad y exactitud garantizando los métodos de procesamiento.

Comité de Gestión de Seguridad de la información: Encargado de coordinar la seguridad de la información en la institución basada en las normas técnicas vigentes en Colombia según Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

Criptografía: Técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quién tenga autorización de descifrarlo.

Incidente de seguridad de la información: Interrupción o alteración del proceso normal de seguridad de los activos de información o una situación de fallas en seguridad de la información con probabilidad significativa de comprometer la confidencialidad, integridad y disponibilidad de la información de la institución. Ejemplos: 1. No se puede ingresar a los sistemas. 2. Identifican que ingresaron a su equipo sin autorización.


Incidente de ciberseguridad: Interrupción o alteración del proceso normal de seguridad de los activos de información digitales, la infraestructura tecnológica, los componentes lógicos de la información y las interacciones en el ciberespacio con probabilidad significativa de comprometer las operaciones de la institución. Ejemplos: 1. Comportamiento inusual al ingresar a los aplicativos e infraestructura tecnológica. 2. Correo electrónico de remitente y origen desconocido.

Oficial de Seguridad de la Información: Es el responsable de alinear las estrategias y actividades de seguridad de la información con los objetivos de la institución, y gestiona las políticas y procedimientos, para que sea gestionado apropiadamente por los responsables de los activos de información del INDERBU y se encuentren adecuadamente protegidos del impacto de los riesgos de seguridad de la información.

Mintic: el ministerio de tecnologías de la información y las comunicaciones lidera la iniciativa pública para impulsar la inversión en el sector tic y para la transformación digital del estado

5. MARCO NORMATIVO

Ley 1581 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

Norma técnica colombiana NTC - ISO/IEC 27001 2013 Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa.

Ley 23 de 1982 2015 Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar Constitución Política de Colombia 1991 - Artículo 15 2015 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

Ley 527 de 1999 2015 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.


Ley 1474 de 2011 2017 Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.

Decreto 2573 de 2014 2018 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


Ley 1712 de 2014; 2018 Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.

6. DESARROLLO DE LA ACTIVIDAD


- a. Descripción de actividades a realizar
- b. Procedimiento de Gestión de Incidentes de Seguridad de la Información

 INDERBU Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023


No	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO /REGISTRO
1	REPORTAR	<p>Todos los funcionarios, contratistas y terceros deberán reportar cualquier evento y/o incidente de seguridad de la información, a través de los siguientes canales:</p> <ul style="list-style-type: none"> - Correo institucional sistemas@inderbu.gov.co - correo institucional subdirector_admin_financiero@inderbu.gov.co - Línea de Atención telefónica: 607-6323644 Extensión 109 <p>Sin excepción, sea cual sea el medio por el cual se reportó el evento y/o incidente de Seguridad de la Información, deben quedar registradas en la herramienta de gestión destinadas para ello.</p>	Funcionarios y Contratistas	PA.05-F07 Formato Registro Incidentes de Seguridad y Privacidad de la Información
2	CATEGORIZAR Y REGISTRAR	El Área de apoyo tecnológico y de sistemas del INDERBU recibe el reporte del evento y/o incidente de seguridad de la Información, lo identifica, registra, clasifica y escala inmediatamente al Especialista de Seguridad Informática o al Oficial de Seguridad que haya designado el instituto.	Subdirector Administrativo y Financiero y/o Equipo Apoyo Gestión Tecnológica	PA.05-F07 Formato Registro Incidentes de Seguridad y Privacidad de la Información
3	RECOLECCION DE INFORMACION	<p>El Oficial de Seguridad debe realizar la evaluación inicial que involucra el análisis de la información descrita en el reporte e información adjuntada en caso que existiere.</p> <p>Además, de ser necesario, el Oficial de Seguridad debe establecer comunicación con el personal involucrado para así recolectar la información</p> <p>Necesaria que permita ser precisos en la clasificación del reporte.</p> <p>El reporte puede ser clasificado en:</p>	Equipo Apoyo Gestión Tecnológica	Documento de información recolectada

 Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023


No	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO /REGISTRO
		<ul style="list-style-type: none"> • Evento de seguridad de la información. • Incidente de seguridad de la información. • Falsa alarma. <p>Son catalogados incidentes de seguridad de la información los que coincidan con las siguientes causales:</p> <ul style="list-style-type: none"> • Ejecución de Denegación de Servicio. • Hacking. • Ejecución de Pruebas Maliciosas o Escaneos de Red. • Contraseñas comprometidas. • Llaves de cifrado comprometidas. • Suplantación de sitios Web Phishing. • Suplantación de identidad de funcionarios. • Eavesdropping: Escuchar Secretamente y sin Autorización llamadas o comunicaciones. • Introducción de código malicioso (Virus, gusanos, troyanos) • Ingeniería social. • Distribución de spam. • Acceso no autorizado a sistemas de información o redes. • Cambio de privilegios sobre sistemas de información sin autorización. • Modificación o inserción de transacciones, archivos o bases de datos sin autorización. 		

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023


No	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO /REGISTRO
		<ul style="list-style-type: none"> • Descarga o envió de contenido inapropiado. • Divulgación no autorizada de información del negocio. • Piratería de software. • Robo de información de negocio. • Robo de información personal de clientes y/o funcionarios (ej.: Phishing). • Pérdida o hurto de equipo de cómputo. • Robo de software. • Robo de información de autenticación. • Daño o pérdida de los servicios o enlaces de comunicaciones. • Pérdida de energía. • Daño o pérdida de los equipos del Centro Alterno de Datos. <p>Si el reporte corresponde a una falsa alarma, se debe documentar en el sistema la justificación de la decisión y posteriormente se debe cerrar y notificar a los interesados.</p> <p>Si el evento o incidente de seguridad de la información, atenta contra los sistemas de información o bases de datos que contienen datos personales y es catalogado como crítico entrañando un alto riesgo para los derechos y libertades de los titulares de la información se procederá sin dilación a realizar la actividad # 8 y # 9.</p>		

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023


No	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO /REGISTRO
4	ANALISIS Y EVALUACION DEL NIVEL DE AFECTACION.	<p>las acciones pueden ser:</p> <p>La criticidad para clasificarla en función de su impacto, y establecer el nivel de prioridad en la resolución de cada incidente de Seguridad de la Información.</p> <p>Podemos categorizar las incidencias en los siguientes aspectos:</p> <ul style="list-style-type: none"> • Critica • Grave • Moderada • Leve <p>Y dependiendo del análisis de ellas se procederá a realizar:</p> <ul style="list-style-type: none"> • Acciones de contención (Si se requieren). • Acciones complementarias (Si se requieren). 	Subdirector Administrativo y Financiero y/o Equipo Apoyo Gestión Tecnológica	Formato de categorización de afectación
5	APLICACIÓN DE ACCIONES DE CONTENCION.	<p>El Especialista de Seguridad Informática si aplica, debe identificar las acciones de respuesta inmediata (Contención) con el equipo especialista del sistema de información para tratar el incidente, esto puede dar como resultado controles de Emergencia y/o controles permanentes adicionales.</p> <p>El plan de acción puede contener acciones como:</p> <ul style="list-style-type: none"> • Activar Contingencias • Desconectar • Copiar/Clonar • Registrar posibles evidencias • Establecer posibles causas • Notificar a los interesados 	Subdirector Administrativo y Financiero y/o Equipo Apoyo Gestión Tecnológica	PA.05-F07 Formato Registro Incidentes de Seguridad y Privacidad de la Información

 Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

No	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO /REGISTRO
		<p>Si la acción de Contención requiere un cambio de Emergencia, se debe activar el proceso de Gestión de Cambios de Emergencia. El Especialista de Seguridad Informática gestiona la ejecución de las actividades del plan de acción enfocadas en la recuperación de la operación. Dentro de estas actividades pueden estar:</p> <ul style="list-style-type: none"> • Ejecución de las acciones de restauración • Implantación de medidas de remediación • Pruebas • Ejecución de plan de retorno <p>Cualquiera que sea el resultado de las acciones realizadas, se debe hacer seguimiento a las acciones por parte del Oficial de Seguridad de la información verificando la documentación y evidencias registradas. Una vez finalizada las acciones de contención, el oficial de Seguridad determina si el incidente de Seguridad de la Información está bajo control.</p>		
6	APLICACIÓN DE ACCIONES COMPLEMENTARIAS.	<p>El Especialista de Seguridad Informática con el equipo especialista del sistema de información debe identificar si se requieren actividades complementarias para tratar los incidentes de seguridad de la información, esto puede incluir la restauración del Sistema(s), Servicio(s) y/o redes de información a su estado normal. Si las acciones complementarias requieren de un cambio normal, se debe activar el proceso de Gestión de Cambios de TI.</p>	<p>Subdirector Administrativo y Financiero y/o Equipo Apoyo Gestión Tecnológica</p>	<p>PA.05-F07 Formato Registro Incidentes de Seguridad y Privacidad de la Información</p>

 Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

No	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO /REGISTRO
7	NOTIFICACION Y MANEJO DE EVIDENCIAS	<p>El Especialista de Seguridad Informática, almacena copia de las evidencias recopiladas, y documenta el incidente por medio del sistema que corresponda. La información que debe contener como mínimo es:</p> <ul style="list-style-type: none"> * Fecha de solicitud * Persona que lo diligencia * Ubicación * Descripción del incidente (descripción cronológica de los acontecimientos) * Clasificación del incidente de acuerdo al procedimiento (en caso que el evento sí sea incidente) * Posibles Impactos * Partes involucradas (especificar especialmente si hay terceros involucrados) * Acciones realizadas (Medidas de contención y de recuperación) 	Subdirector Administrativo y Financiero y/o Equipo Apoyo Gestión Tecnológica	PA.05-F07 Formato Registro Incidentes de Seguridad y Privacidad de la Información
8	REPORTE EN EL REGISTRO NACIONAL DE BASE DE DATOS RNBD.	En la Plataforma tecnológica de la Superintendencia de Industria y Comercio reportar el incidente de seguridad dentro los (15) días hábiles siguientes al registro del incidente o evento de seguridad	Subdirector Administrativo y Financiero y/o Equipo Apoyo Gestión Tecnológica	Pantallazo de registro de novedades del RNBD
9	COMUNICACIÓN A LOS AFECTADOS.	Una vez identificado el incidente de seguridad y cumplidas con las actividades descritas en el presente procedimiento, la Oficina de Seguridad de la Información comunicara al interesado en un lenguaje claro y sencillo la violación de seguridad, las medidas correctivas adoptadas por la organización y las recomendaciones de seguridad que deberán seguir los interesados.	Subdirector Administrativo y Financiero y/o Equipo Apoyo Gestión Tecnológica	Formato de dictamen técnico de afectación de incidentes

 Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

No	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO /REGISTRO
10	DOCUMENTAR LECCIONES APRENDIDAS.	El Oficial de Seguridad con el equipo que atendiendo el incidente es responsable de identificar las lecciones aprendidas con el objeto de evitar la reincidencia de los hechos y la eliminación de las debilidades aprovechadas por la amenaza que causó el incidente de seguridad. Así mismo, el oficial de Seguridad de la Información es responsable de identificar si aplica, controles nuevos o modificaciones a los existentes en la Universidad, esto en Pro de mejorar el proceso y la Seguridad de la Información del INDERBU.	Subdirector Administrativo y Financiero y/o Equipo Apoyo Gestión Tecnológica	Documento de análisis y recomendaciones sobre incidentes informáticos
11	CERRAR EL INCIDENTE.	Oficial de Seguridad informa al Centro de Servicios de Tecnología para el cierre del incidente en la herramienta de gestión e informa a las personas interesadas.	Subdirector Administrativo y Financiero y/o Equipo Apoyo Gestión Tecnológica	Acta de cierre de incidente informático


Tabla 1. Descripción Proceso de Gestión de Incidentes de Seguridad de la Información.

7. ROLES Y RESPONSABILIDADES.

- **Oficial de Seguridad**

El Oficial de Seguridad de la Información es el responsable de planificar, desarrollar, controlar, gestionar y/o coordinar las estrategias de seguridad de la información, con el fin de mantener la confidencialidad, integridad y disponibilidad; y de promover el diseño, establecimiento, implementación, operación, revisión, mantenimiento y mejora continua de la gestión en seguridad de la información.

- **Especialista de Seguridad Informática**

 INDERBU <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD01
	PROCEDIMIENTO GESTION INCIDENTES	VERSIÓN: 01
		FECHA: 22/03/2023

El especialista de Seguridad Informática es responsable de gestión y administración de la infraestructura de seguridad informática, gestionar la remediación de vulnerabilidades técnicas y monitorear los eventos de seguridad de la plataforma tecnológica, así como coordinar las acciones de respuesta y recuperación al incidente de seguridad de la información.

- **Coordinador de Protección de Datos**

El Coordinador de Protección de Datos es responsable de velar por la implementación efectiva de las políticas y procedimientos del programa de protección de datos personales para dar cumplimiento a las normas sobre protección de datos personales, así como la implementación de buenas prácticas de gestión de datos personales dentro del INDERBU.

8. CONTROL DE CAMBIOS.

VERSIÓN	DESCRIPCIÓN Y/O MODIFICACIONES	FECHA
01	Creación del documento	22/03/2023

ELABORÓ: Firma: _____ Nombre: William Oswaldo Barrera Contratista SAF Mónica Niño Entralgo Contratista SAF	REVISÓ: Firma: _____ Nombre: Silvia Nathalia Niño Villamizar Cargo: subdirectora Administrativa y Financiera	APROBÓ: Firma: _____ Nombre: Eliana León de Ordoñez. Cargo: Directora General	FECHA DE APROBACIÓN: 22/03/2023