


INDERBU Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

PROCEDIMIENTO SEGURIDAD DE LA INFORMACIÓN
2023-2024

**INSTITUTO DE LA JUVENTUD EL DEPORTE Y LA RECREACION DE
BUCARAMANGA**



	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023


INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente. Esta estrategia se fundamenta en cuatro componentes, TIC para servicios, TIC para gobierno abierto, TIC para la gestión y seguridad y privacidad de la información, a través de los cuales se busca facilitar la masificación de la oferta y demanda del Gobierno en Línea. Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha diseñado un documentos de lineamientos “Modelo de Seguridad y Privacidad de la Información” el cual lo largo de los últimos años se ha ido actualizando en función de las modificaciones de la norma técnica que le sirve de sustento: ISO 27001, las mejores prácticas y los cambios normativos que tengan impacto sobre el mismo. A su turno el Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión

INDERBU <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

OBJETIVOS

La presente guía tiene como objetivo principal, indicar los procedimientos de seguridad que pueden generarse durante el diseño y la implementación del modelo de seguridad y privacidad de la información para las entidades del estado. Dependiendo de la entidad, dichos procedimientos pueden variar o si la entidad desea puede generar más procedimientos si lo considera conveniente.


	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

GLOSARIO

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Instructivo: Documento que describe de una manera detallada cómo debe ejecutarse una actividad o tarea determinada para garantizar su realización, hablan sobre métodos específicos sobre plataformas, sistemas de información o algún proceso definido

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

1. PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En este documento presenta algunas recomendaciones de procedimientos de seguridad de la información para el Modelo de Seguridad y privacidad de la Información para las Entidades del Estado. El conjunto de procedimientos que se presentará a continuación, constituye una base sólida para que cada entidad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar. Con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad, se tomaron en cuenta los 14 numerales de control de seguridad de la información definidas en la norma ISO/IEC 27001, para definir los procedimientos de seguridad necesarios. Es importante aclarar que en los procedimientos, se pueden citar instructivos o documentos informativos adicionales como complemento. Así mismo, la complejidad o extensión de cada procedimiento dependerá del tipo de entidad y los recursos de los cuales disponga.

1.1. SEGURIDAD DEL RECURSO HUMANO:

En este dominio relacionado con el personal que labora dentro de la entidad, se pueden definir los siguientes procedimientos:


- **PROCEDIMIENTO DE CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL**

Indica la metodología empleada por la entidad para realizar la capacitación y sensibilización del personal en temas de seguridad de la información teniendo en cuenta los diferentes roles y responsabilidades, la periodicidad de dichas capacitaciones y sensibilizaciones etc...

La entidad tiene un programa llamado jueves de TIC donde se tratan temas relacionado con la información y la seguridad de la misma, así como temas relacionados con el uso de las herramientas tecnológicas y los servicios tecnológicos con los cuales cuenta la entidad

Metodología:

1. Listado de servicios tecnológicos de la entidad.
2. Manual de uso de servicios tecnológicos de la entidad.

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

3. Capacitación presencial en espacios semanales para hablar del trabajo colaborativo, seguridad de la información, uso de la información, gestión documental.

- **PROCEDIMIENTO DE INGRESO Y DESVINCULACIÓN DEL PERSONAL**

Este procedimiento indica la manera como la entidad gestiona de manera segura el ingreso y desvinculación, incluyendo temas como verificación de antecedentes, firma de acuerdos de confidencialidad, recepción de entregables requeridos para generar paz y salvos entre otras características. Este procedimiento va de la mano con el área de gestión de recursos humanos o contratación puede generarse con su colaboración.

- **Procedimiento de gestión de activos tecnológicos, de la mano con la vinculación y desvinculación del personal**


Descripción del procedimiento.

La entidad rota de personal constantemente, sin embargo, esas personas que entran y salen de la entidad, deben pasar por procesos que les permitan acceder o bloquear servicios tecnológicos.

1. Diligenciar el formulario de asignación de servicios tecnológicos, luego de que se realiza la posesión o firma del contrato del funcionario o contratista.
2. Remitir el formulario debidamente diligenciado y firmado por la persona que autoriza dichos servicios a la subdirección administrativa y financiera.
3. El supervisor administrativo y financiero asignara los servicios solicitados para el funcionario o contratista.
4. La asignación emana un formulario soporte donde se expresan las credenciales de acceso y niveles de acceso a los diversos servicios tecnológicos de la entidad, este documento será enviado al beneficiario de este servicio.
5. Fin del proceso.

Se sigue este mismo proceso para 4 opciones, las cuales son:

1. Dar de alta
 - cuando la funcionario o contratista ingresa por primera vez a la entidad en un periodo de anualidad.
2. Suspende
 - cuando el funcionario o contratista, sale de vacaciones, se suspende el contrato, incapacidades mayores a 30 días, y casos similares.
3. Modificar

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

- cuando se van a modificar los parámetros de los servicios tecnológicos asignados con un documento anterior al funcionario o contratista.

4. Dar de baja

- Cuando el funcionario o contratista termina su vinculación laboral o contractual con la entidad. Adicionalmente cuando usamos esta opción, el funcionario o contratista debe entregar el material de valor institucional que produjo durante su proceso contractual o laboral. Entiéndase que toda información de tipo intelectual o documental producto del trabajo en el inderbu es de propiedad del inderbu.

1.2. GESTION DE ACTIVOS:

En este dominio relacionado con la identificación y clasificación de activos de acuerdo a su criticidad y nivel de confidencialidad se pueden definir los siguientes procedimientos:

- **PROCEDIMIENTO DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS**

En este procedimiento se debe indicar la manera en que los activos de información son identificados e inventariados por la entidad, así como también se debe especificar como son clasificados de acuerdo a su nivel de confidencialidad o criticidad, como se asignan y se devuelven los activos una vez se termina la relación laboral con la entidad.

Adicionalmente se debe explicar cómo se hace una correcta disposición de los activos cuando ya no se requieran y su transferencia hacia otros lugares de manera segura.

En cuanto a la forma en que se identifican los activos de información, la entidad no ha realizado esta actividad, pero la metodología será la siguiente:

https://mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf


aplicando el siguiente formulario para la recolección de la información: (ejemplo)

INDERBU <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA				CÓDIGO: PA.05-PD02	
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION				VERSIÓN: 01	
					FECHA: 11/12/2023	

Modelo de tabla para gestión de activos de información

DEPENDENCIA					CATEGORIA O SERIES DE INFORMACIÓN	NOMBRE O TÍTULO DE LA INFORMACIÓN		DESCRIPCION DE LA INFORMACIÓN	IDIOMA	FORMATO	MEDIO DE CONSERVACIÓN Y/O SOPORTE
PROCESO	SECCIÓN	CÓDIGO	SUBSECCIÓN	CÓDIGO		SERIE	SUBSERIE				
					Comités y reuniones Informes					Físico Físico y digital	

FECHA DE GENERACION DE LA INFORMACION	FRECUENCIA DE ACTUALIZACION	LUGAR DE CONSULTA	RESPONSABLE DE LA PRODUCCION DE LA INFORMACION	RESPONSABLE DE LA INFORMACION	OBJETIVO LEGITIMO DE LA EXCEPCION		FUNDAMENTO CONSTITUCIONAL O LEGAL	FUNDAMENTO JURIDICO DE LA EXCEPCION	EXCEPCION TOTAL O PARCIAL		FECHA DE LA CLASIFICACION	PLAZO DE LA CLASIFICACION O RESERVA
	Anual Recurrente Semestral Trimestral	Dirección General Sub Administrativa Sub Operativa Sub Técnica										

 Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

Se podrán adicionar de 2 a 4 columnas para fines de organización de acuerdo a:

- Su propietario y su custodio.
- Los usuarios y derechos de acceso.
- Si se publica y la periodicidad de publicación.

La metodología para poder llenar toda esta tabla es reunirse con cada funcionario líder de proceso y con sus tablas de retención documental armonizar la producción documental de su puesto de trabajo, con las tablas de retención y con la realidad de producción documental importante del puesto.

Luego de ello con la tabla construida para cada funcionario se establecen los niveles de acceso a esta información en cuanto a los tipos de modificaciones que se pueden hacer en los archivos digitales.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA


Tabla 1: Criterios de Clasificación

1.3. CONTROL DE ACCESO

En este dominio relacionado con el acceso a la información y a las instalaciones de procesamiento de la información, se pueden generar los siguientes procedimientos:

- **PROCEDIMIENTO PARA INGRESO SEGURO A LOS SISTEMAS DE INFORMACIÓN**

En este procedimiento la entidad debe indicar como gestiona el acceso a sus sistemas de información de manera segura, empleando métodos preventivos contra ataques de fuerza bruta, validando los datos completos para ingreso a los sistemas,

 INDERBU Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

empleando métodos para cifrar la información de acceso a través de la red entre otros.

Procedimiento para gestión de acceso a sistemas de información:


1. Lo primero que debe existir es un listado de sistemas de información de la entidad

Nombre del sistema	Administrador del sistema	Criticidad	Ubicación del sistema
Sistema de gestión de información financiera y contable , activos fijos y nomina	Sistemas	Alta	local
Sistema de gestión de solicitudes ciudadanas	Sistemas	Alta	Remoto (web)
Sistema de ventanilla única	Sistemas	Alta	Local
Sistema de gestión de préstamo de escenarios deportivos	Subdirección Técnica	Alta	Remoto (web)
Sistema de gestión documental	Sistemas	Alta	Local – Remoto (web)
Descripción	Rol que se encarga de gestionar el sistema de información	Alta / media /baja	Local / remoto /

2. Lo segundo que debe existir es un listado de usuarios con acceso a cada sistema

Nombre del sistema	Nombre de usuario	Nivel de acceso	Fecha de inicio	Fecha de terminación
Sistema de gestión de información financiera y contable , activos fijos y nomina	Elizabeth Pico Díaz	Administrador		
	Jorge Pinilla Cruz	Usuario		

3. Debe existir un manual de uso de los sistemas de información.


 INDERBU <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

Para poder tener acceso a cualquier sistema de información de la entidad, se debe llenar el formato de asignación de recursos tecnológicos, donde la persona jerárquicamente superior da acceso a un rol jerárquico inferior, esto brinda la correcta gestión del acceso, adicionalmente la entidad cuenta con gestión de acceso a los equipos de cómputo a través de un directorio activo, así como bloqueos de acceso en la red de datos segmentando en 3 grupos funcionarios, contratistas e invitados, esto se logra gracias a la gestión de direcciones Mac de cada uno de los equipos que se encuentran en la red.

Nombre del sistema	Administrador del sistema	Lugares desde los cuales se puede usar el sistema	Forma de uso del sistema
Descripción del sistema de información	Identificación del administrador – id y nombre	Interno Externo Interno y externo	Descripción de cómo se usa el sistema.
Ejemplo			
Sistema de gestión de información financiera y contable , activos fijos y nomina	Sistemas	Local	El sistema se debe usar de manera responsable digitando la información de manera correcta, se recomienda tener en cuenta inducción y reinducción al personal para poder manejar el sistema o experiencia en el mismo. Para mayor información lea el manual de uso del sistema.

En conclusión, la gestión de activos de información cubre este apartado también.

- **PROCEDIMIENTO DE GESTIÓN DE USUARIOS Y CONTRASEÑAS**

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

En este procedimiento, la entidad deberá indicar como realiza la creación de usuarios y la asignación de contraseñas (las cuales deberán tener un nivel de seguridad aceptable, con base a una política de contraseñas seguras definida previamente), prohibiendo su reutilización posterior, permitiendo a los usuarios cambiarla regularmente, llevando un registro de las mismas. Este procedimiento debe aplicar a todos los sistemas de información, también se debe tener en cuenta el rol que cada usuario requiera en los determinados sistemas, para brindar el acceso necesario.

Política de contraseñas:


Para asignar las contraseñas a los diferentes sistemas de información que la entidad maneja, el inderbu solicita al usuario gestionar las contraseñas con las siguientes características.

1. La contraseña debe tener una longitud mínima de 8 caracteres
2. Excluir de la contraseña el nombre de usuario o la descripción del mismo.
3. Incluir mayúsculas y minúsculas mezcladas
4. Incluir caracteres numéricos
5. Incluir caracteres especiales, tales como (+ - * . - () & % # " ' ! °)
6. Excluir contraseñas débiles como 12345 , Dios, mama, papa, hijo, el nombre de hijos, de padres, de mascotas entre otras de fácil consecución por parte de los delincuentes informáticos.
7. En lo posible usar gestores de contraseñas tales como
 - <https://www.clavesegura.org/es/>
 - <https://password.es/>
 - <https://passwordsgenerator.net/es/>

procedimiento para gestión de usuario y contraseñas.

Se encuentra entrelazado en el procedimiento de solicitud y asignación de servicios y recursos tecnológicos.

Puesto que allí jerárquicamente se asignan los usuarios de acuerdo al número de cedula, que es el dato por excelencia que la entidad luego de múltiples pruebas decidió sea el usado para todos los sistemas de información, la clave si será asignada por cada funcionario o contratista de acuerdo a la política de calves.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

1.4. SEGURIDAD FÍSICA Y DEL ENTORNO

Este dominio está relacionado con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información. Se pueden generar los siguientes procedimientos (estos procedimientos pueden tener la participación del área de seguridad y vigilancia de la entidad):

- **PROCEDIMIENTO DE CONTROL DE ACCESO FÍSICO**

En este procedimiento se debe describir como se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas etc...


Se debe construir con el apoyo de subdirección técnica, definiendo el listado de ubicaciones de la entidad y las personas que pueden tener acceso a cada una de esas ubicaciones en una matriz, actualmente se encuentra en funcionamiento la bitácora de registro de visitantes en la portería de la entidad, y la habilitación de un carnet que identifica a los funcionarios y contratistas de la entidad, así como la gestión de horas de entrada y salida para los funcionario y contratistas a través de un sistema biométrico de control de horario

- **PROCEDIMIENTO DE PROTECCIÓN DE ACTIVOS**

Este procedimiento debe contener los pasos con los cuales los equipos son protegidos por la entidad. Se recomienda que este procedimiento indique como se determina la ubicación de los equipos que procesan información confidencial, como se aseguran dichas las instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas etc...

- **PROCEDIMIENTO DE RETIRO DE ACTIVOS**

En este procedimiento debe especificarse como los activos son retirados de la entidad con previa autorización. Se debe indicar el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos etc...)


- **PROCEDIMIENTO DE MANTENIMIENTO DE EQUIPOS:**

Este procedimiento debe especificar como se ejecutan mantenimientos preventivos o correctivos dentro de la entidad, indicando los intervalos en que estos deberán realizarse, con base a las sugerencias de los proveedores o si existen seguros atados a los equipos y los mantenimientos sean requisitos. Se debe especificar el modo en que los mantenimientos se llevarán a cabo y el personal que deberá ejecutarlo, llevando el registro apropiado.

1.5. SEGURIDAD DE LAS OPERACIONES

Este dominio busca asegurar las operaciones correctas dentro de las instalaciones de procesamiento de información:

- **PROCEDIMIENTO DE GESTIÓN DE CAMBIOS:** En este procedimiento la entidad deberá como realiza el control de cambios en la organización, los procesos de negocio y los sistemas de información de manera segura. Se deben especificar aspectos como identificación y registro de cambios significativos, planificación y pruebas previas de los cambios a realizar, valoración de impactos, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, procedimientos de rollback (reversa) entre otros.
- **PROCEDIMIENTO DE GESTION DE CAPACIDAD:** Se debe especificar como la organización realiza una gestión de la capacidad para los sistemas de información críticos, en especial si los recursos requeridos son escasos, demorados en su arribo o costosos. La entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda etc.
- **PROCEDIMIENTO DE SEPARACIÓN DE AMBIENTES:** Con el fin de evitar problemas operacionales que pueden desencadenar en incidentes críticos, es necesario desarrollar un procedimiento de separación de ambientes que permita realizar una transición de los diferentes sistemas desde el ambiente de desarrollo hacia el de producción. Dentro de los aspectos más importantes a considerar se encuentran la implementación de un ambiente de pruebas para las aplicaciones, definición de los requerimientos para la transición entre

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023


ambientes, la compatibilidad de los desarrollos con diferentes sistemas entre otros.

- PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS:**
 La entidad debe indicar por medio de este procedimiento como realiza la protección contra códigos maliciosos teniendo en cuenta, que controles utiliza (hardware o software), como se instalan y se actualizan las plataformas de detección, definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo.

1.6. SEGURIDAD DE LAS COMUNICACIONES

Este dominio busca el aseguramiento y la protección de la información a través de los diferentes servicios de comunicaciones de la organización.

- PROCEDIMIENTO DE ASEGURAMIENTO DE SERVICIOS EN LA RED:**
 Este procedimiento explica la manera en que la entidad protege la información en las redes, indicando los controles de seguridad (como se cifran los datos a través de la red por ejemplo) que se aplican para acceder a la red cableada e inalámbrica, satelital etc... con miras a proteger la privacidad de la información que circula a través de estos medios, también se debe incluir el uso de registros (logs) que permitan realizar seguimiento a acciones sospechosas.
- PROCEDIMIENTO DE TRANSFERENCIA DE INFORMACIÓN:** En este procedimiento la entidad deberá indicar como realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción. Se deben tener en cuenta acuerdos de confidencialidad y no divulgación, que deberán ser actualizados y revisados constantemente, donde se incluyan condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

1.7. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN:


- PROCEDIMIENTO ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE:** Este procedimiento deberá describir como se realiza la gestión de la seguridad de la información en los sistemas desarrollados internamente (inhouse) o adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información de la entidad. Dicha gestión y control también debe ser especificada para los sistemas ya existentes que son actualizados o modificados en la entidad. Se deben tener en cuenta el uso de ambientes de desarrollo, pruebas y producción para los sistemas de información.
- PROCEDIMIENTO DE CONTROL SOFTWARE:** En este procedimiento la entidad deberá indicar como realiza el control de software, es decir, como limita el uso o instalación de software no autorizado dentro de la entidad, quienes están autorizados para realizar la instalación de software, como se realizaría la gestión de las solicitudes de instalación de software para los usuarios, cómo se realiza el inventario de software dentro de la entidad entre otros aspectos.

1.8. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:** Este procedimiento debe indicar como responde la entidad en caso de presentarse algún incidente que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o confidencialidad. Deben especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los planes de BCP (Planes De Continuidad) dependiendo de la criticidad de la información.


1.9. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO


- PROCEDIMIENTO DE GESTIÓN DE LA CONTINUIDAD DE NEGOCIO:** En este procedimiento la entidad debe indicar la manera en que la entidad

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

garantizará la continuidad para todos sus procesos (de ser posible o por lo menos los misionales), identificando los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico.

El procedimiento debe indicar los pasos a seguir cuando existan estas situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir, los procesos alternos o que permitan continuar con el proceso de manera temporal

 <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CODIGO: PA.05-F06		
	PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSION: 01		
FECHA:xx/xx/2023				
1. OBJETIVO:				
2. ALCANCE:				
3. DEFINICIONES:				
4. SIGLAS:				
5. NORMATIVIDAD:				
5.1. CONSTITUCIÓN:				
5.2. LEYES:				
5.3. DECRETOS:				
5.4. RESOLUCIONES:				
5.5. OTRAS Por ejemplo normas o estándares.				
DESARROLLO				
No.	Actividad	Tarea	Punto De Control	Responsable
1				
2				

 INDERBU <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

3				
4				
5				
6				
7				
8				
9				
10				

Actividad: (Paso a ejecutarse)

- 1.
- 2.
- 3.

Tarea:(Descripción de la actividad incluyendo labores adicionales detallando paso a paso el proceso)

- 1.
- 2.
- 3.

Punto De Control: (Requerimiento mínimo para que la actividad pueda ejecutarse, por ejemplo un control de cambios, un formato o una aprobación).

Responsable: (Responsable de la actividad).

REGISTROS Posibles documentos de salida

INFORMACIÓN			
INFORMACIÓN GENERADA	RESPONSABLE	UBICACIÓN	FRECUENCIA

SISTEMAS DE INFORMACIÓN			
SISTEMA DE INFORMACIÓN	DESCRIPCIÓN	RESPONSABLE	UBICACIÓN

ANEXOS (Pueden referenciarse formatos, instructivos, informativos, reglas etc...)

INDERBU <small>Instituto de la Juventud, el Deporte y la Recreación de Bucaramanga</small>	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PD02
	PROCEDIMIENTO SEGURIDAD DE LA INFORMACION	VERSIÓN: 01
		FECHA: 11/12/2023

11.CONTROL DE CAMBIOS

FECHA	CAMBIO		VERSIÓN
<hr/>			
Elaboró	Revisó y Aprobó		

CONTROL DE CAMBIOS

VERSIÓN	VIGENCIA	DESCRIPCIÓN DEL CAMBIO
01	11/12/2023	Creación del documento.

CONTROL DE DOCUMENTOS			
ELABORÓ:	REVISÓ:	APROBÓ:	FECHA DE APROBACIÓN:
Nombre: Mónica Rocío Niño Entralgo Cargo: CPS Sistemas	Nombre: Tatiana Palencia Cargo: Subdirectora Administrativa y Financiera	Nombre: Comité Institucional de Gestión y Desempeño	11/12/2023