POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INDERBU

INSTITUTO DE LA JUVENTUD, EL DEPORTE Y LA RECREACIÓN DE BUCARAMANGA

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

INTRODUCCIÓN

La política de alto nivel o política general aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

Es así como, teniendo en cuenta la importancia que tiene que el instituto de la juventud , el deporte y la recreación de Bucaramanga INDERBU defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por la Dirección.

De esta forma, una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Son cortas, y enmarcan los principios que guían las actividades dentro de la entidad.

OBJETIVO

El siguiente documento es un formato que puede ser utilizado como plantilla para la elaboración de la política general de seguridad y privacidad de información para las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

GLOSARIO

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos 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 entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Adware: Software que se apoya en anuncios como parte del propio programa. La publicidad generada es mostrada después de la instalación de dicho programa.

Amenaza: Circunstancia que tiene el potencial de causar daños o pérdidas puede ser en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DOS).

Antispam: Aplicación o herramienta informática que se encarga de detectar y eliminar correo no deseado.

Antivirus: Software utilizado para eliminar programas elaborados con intención destructiva.

Aplicación engañosa: Las aplicaciones engañosas pueden introducirse sigilosamente en su equipo cuando navega por la Web. Una vez instaladas, los estafadores las utilizan para cometer fraudes y robos de identidad.

Autenticación básica: Esquema de autenticación basado en la web más simple que funciona mediante el envío del nombre de usuario y contraseña con cada solicitud.

Ataque Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Ataque Dirigido: Son aquellos ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona, empresa o grupos de ambas

Armouring: Es una técnica que utilizan los virus para esconderse e impedir ser detectados por los antivirus.

Blacklist (Lista negra): Es un proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Bots (Red): Son grupos de ordenadores infectados controlados de forma remota por un hacker.

Bulo: Mensaje de correo electrónico con contenido falso o engañoso, pero con contenido de alto impacto.

Caballo de Troya: Son un tipo de código malicioso que parece ser algo que no es. Permiten hacerse con el control de los ordenadores ajenos sin permiso de los

usuarios. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente.

Carga destructiva: Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware.

Cracker: Personas que rompen algún sistema de seguridad, (Fines de lucro, protesta o desafío)

Crimeware: Software malicioso como los virus, troyanos, spyware y más.

Ciberseguridad: Condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones en el ciberespacio.

Cibercrimen: Actos delincuenciales en el ciberespacio donde el principal objetivo es cometer ilícitos contra individuos, organizaciones y empresas.

Ciberdelito: Operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Cifrado: Proceso de codificación de información sensible para poder evitar que esta llegue a personas no autorizadas.

Control de acceso a la red (Nac): Su principal objetivo es asegurar que todos los dispositivos que sean conectados a las redes corporativas, cumplan con las políticas de seguridad establecidas para evitar amenazas.

Correo no deseado: cualquier comunicación que nos llega por cualquier medio no habiendo sido solicitada y que no era esperada por el usuario que la recibe.

Cookie: Archivos que se guardan en los equipos para que los sitios web recuerden determinados datos.

Definición de virus: Procedimiento por medio del cual el antivirus actualiza su base de datos de definiciones de virus. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes

Delito Informático: Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

Desbordamiento del búfer: Se producen cuando un programa sobrescribe otras partes de la memoria del equipo para almacenar más datos de los permitidos, provocando errores o bloqueos.

Driver: Es un programa, conocido como controlador, que permite la gestión de los dispositivos conectados al ordenador (generalmente, periféricos como impresoras, unidades de CD-ROM, etc.).

Dropper: Es un fichero ejecutable que contiene varios tipos de virus en su interior.

Economía Clandestina: La economía clandestina en línea es el mercado digital donde se compran y se venden bienes y servicios obtenidos a través de la ciberdelincuencia, con el fin de cometer delitos informáticos.

Encriptación: Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Exploit: Un error en el software que representa una brecha de seguridad.

Extorsión: El uso de Internet para amenazar con la intención de extorsionar a un individuo para conseguir dinero u otra cosa de valor.

Extensión: Los ficheros se representan asignándoles un nombre y una extensión, separados entre sí por un punto: NOMBRE.EXTENSIÓN.

Filtración de datos: Divulgaciones que no están autorizadas que tratan de adquirir información confidencial y que pueden dar lugar a robos o fugas.

Firewall: Un componente de hardware o software diseñado para bloquear el acceso no autorizado.

Firma de Antivirus: Las bases de firmas de un antivirus son el conjunto de cadenas que posee para detectar distintos códigos maliciosos. Sus actualizaciones se producen cuando el producto descarga nuevas firmas, que son incorporadas a su base para así poder detectar más amenazas.

Freeware: Salida no controlada de información que hace que esta llegue a personas no autorizadas. Freeware: Es todo aquel software, legalmente distribuido, de forma gratuita.

Gateway: Es un ordenador que permite las comunicaciones entre distintos tipos de plataformas, redes, ordenadores o programas.

Greylisting o Lista Gris: Una lista gris o greylist es una técnica para el control de mensajes spam. Es un método de defensa que bloquea la mayoría de los spams que se reciben en un servidor de correo.

Gusanos: Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios.

Hacker: Persona experta en tecnología dedicada a intervenir y /o realizar alteraciones técnicas con buenas o malas intenciones.

Hacking: Acceder de forma ilegal a datos almacenados en un ordenador o servidor.

Hacktivismo: Es la función del Hacking y el activismo, la política y la tecnología.

Hardware: Término que hace referencia a cada uno de los elementos físicos de un sistema informático (pantalla, teclado, ratón, memoria, disco duro, otros)

HTTP (HyperText Transfer Protocol: Es un sistema de comunicación que permite la visualización de páginas Web, desde un navegador.

Ingeniería Social: Término que hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

Incidente Informático: Es la violación o amenaza que afectan la confidencialidad, disponibilidad y la integración como la continuidad de los servicios que son ofrecidos.

Inyección de código SQL: Técnica donde el atacante crea o altera comandos SQL, para exponer datos ocultos, sobre escribir los valiosos, o ejecutar comandos peligrosos en un equipo que hospeda bases de datos.

Índice de peligrosidad: Es un valor calculado que permite medir lo peligroso que puede llegar a ser un virus.

Infección: Es la acción que realizan el virus, consistente en introducirse en el ordenador o en áreas concretas de éste y en determinados ficheros.

IP (Internet Protocol) / TCP-IP: La IP es la dirección o código que identifica exclusivamente a cada uno de los ordenadores existentes.

Keylogger: Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Lista Blanca: Método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad.

Malware: Término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos, Gusanos, keyloggers, Botnets, Ransomware, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues.

Mecanismo de Propagación: Un mecanismo de propagación es el método que utiliza una amenaza para infectar un sistema.

Mutex: Técnica utilizada por algunos virus para controlar el acceso a recursos (programas u otros virus) y evitar que más de un proceso utilice el mismo recurso al mismo tiempo.

Negación de servicio (DoS): Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Nivel de Propagación: Se trata de un valor que indica cómo de rápido se puede extender o se ha extendido el virus por todo el mundo. Es usado para mirar la peligrosidad del mismo.

Nuke (ataque): Caída o pérdida de la conexión de red, provocada de forma intencionada por alguna persona. El ordenador sobre el que se realiza un nuke, además puede quedar bloqueado.

Parches: Programa que se encarga de hacer cambios en busca de la corrección de vulnerabilidades de seguridad.

Pharming: Redirigir el tráfico a un sitio web falso para capturar información confidencial de los usuarios.

Phishing: Técnica utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

Piratería: Infringir los derechos de autor para obtener ganancias financieras o distribuir sin permiso un trabajo que se está preparado para su distribución comercial.

Programa malicioso: También conocidos como malware que contienen virus, spyware y otros programas indeseados que se instalan sin consentimiento.

Protección Heurística: En el contexto de la protección antivirus, la heurística se compone de un conjunto de reglas que se emplean para detectar el comportamiento de los programas maliciosos sin necesidad de identificar de forma exclusiva a la amenaza específica, como es requerida por la detección clásica basada en firmas.

Redes punto a punto: son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.

Ransomware: Programa maligno que bloquea totalmente nuestro equipo y pide dinero a cambio de devolver el control.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque.

Robo de datos: Los robos de datos pueden producirse tanto dentro de la empresa (por ejemplo, a manos de un trabajador descontento) como mediante ataques de delincuentes desde el exterior.

Rootkits: Es un juego de herramientas (programas) que permiten acceder a los niveles administrativos de un ordenador o una red.

Scareware: Hacer creer a los usuarios que el equipo está infectado, para hacer comprar una aplicación falsa.

Sistema de detección de intrusos (IDS): Hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Sistema de prevención de intrusiones (IPS): Encargados de detectar y bloquear cualquier intento de intrusión, transmisión de código maliciosos, o amenazas a través de la red.

Software de seguridad fraudulento (rogue): Falsos programas de seguridad que no son realmente lo que dicen ser, sino que, todo lo contrario. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios.

Spear phishing: Estafa por correo electrónico cuyo objetivo es acceso no autorizado a datos, se centra en organizaciones en busca de: robo de propiedad intelectual, datos financieros, secretos comerciales, otros.

Spyware: Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas sin permiso de los usuarios.

Toolkit: Son programas de software que pueden usarse tanto por novatos como por expertos para facilitar el lanzamiento y distribución de ataques a computadoras en red.

Tracware: Es todo programa que realiza el seguimiento de las acciones que realiza el usuario mientras navega por Internet (páginas visitadas, banners que pulsa, etc.) y crea un perfil que utiliza con fines publicitarios.

Variante: Es una versión modificada de un virus original, que puede infectar de forma similar o distinta y realizar las mismas acciones u otras.

Vector de ataque: Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

Virus: Programa de ordenador capaz de incrustarse en disco y replicarse repetidamente, sin el conocimiento o permiso del usuario.

Vulnerabilidad: Debilidad del sistema informática que puede ser utilizada para causar algún tipo de daño.

Zombie: Ordenadores infectados controlados de forma remota por los ciberdelincuentes.

ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Líder de Seguridad de la Información: Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información, y someterlos a decisión del Comité de Seguridad, realizando la implementación y seguimiento de estos.

Comité Institucional de Gestión y Desempeño: Comunicar a los funcionarios, contratistas y/o particulares que participan en actividades de forma directa o indirecta con la entidad, la importancia de satisfacer los requisitos de seguridad digital.

Líder o responsable de protección de datos personales: establecer lineamientos para la protección de datos personales tratados en la entidad.

Líderes de proceso: Identificar e inventariar los nuevos activos digitales de información y los riesgos cibernéticos asociados.

Responsable o Asesor de TI: Participar en la elaboración del cronograma de capacitación de seguridad digital en la entidad. Implementar las mejoras identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura TI.

Partes interesadas (funcionarios, contratistas y proveedores): cumplir con las políticas de seguridad y privacidad de la información y cláusulas establecidas en el MSPI.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección del Instituto de la juventud, el deporte y la recreación de Bucaramanga INDERBU, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el INDERBU, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del INDERBU con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información. El INDERBU, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- ✓ Minimizar el riesgo de los procesos misionales de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de los funcionarios, contratistas y terceros.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema de gestión de seguridad de la información.
- ✓ Proteger los activos de información.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del INDERBU.
- ✓ Garantizar la continuidad del negocio frente a incidentes.
- ✓ Alcance/Aplicabilidad
- ✓ Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del INDERBU y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de

El INDERBU:

• Ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

• Protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

• Protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• Protegerá su información de las amenazas originadas por parte del personal.

• Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• Implementará control de acceso a la información, sistemas y recursos de red.

• Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• Garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

• Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

FASES DE IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

1. Desarrollo de las políticas: En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

- ✓ Justificación de la creación de política: Debe identificarse el por qué la Entidad requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.

- ✓ Alcance: Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?
- ✓ Roles y Responsabilidades: Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.
- ✓ Revisión de la política: Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma.
- ✓ Aprobación de la Política: Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de las mismas. Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas.

2. Cumplimiento: Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

3. Comunicación: Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los funcionarios contratistas y/o terceros de la entidad debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.

4. Monitoreo: Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos ejemplo indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

5. Mantenimiento: Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

6. Retiro: Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

IMPORTANCIA DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.

RECOMENDACIONES PARA LA REDACCION DE UNA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se presenta una serie de recomendaciones para realizar redacción de políticas de seguridad y privacidad de la información en la Entidad:

- ✓ La política debe tener como parte de su texto la declaración en la cual se indica ¿qué es lo que se desea hacer?, ¿qué regula la política?, ¿cuál es la directriz que deben seguir los funcionarios, contratistas y/o terceros?, todo esto alineado con la estrategia de la organización.
- ✓ Alinearse con el alcance del Modelo de Seguridad y Privacidad de la Información.
- ✓ Debe especificarse a quién (es) va dirigida la política, se debe identificar fácilmente quien (es) deben cumplir la política.
- ✓ En los casos que aplique se hace referencia de la regulación mediante la cual se soporta la política.
- ✓ En caso de que aplique la política debe indicar las excepciones a la misma y a quienes les aplica la excepción.
- ✓ Datos de las personas o roles de la entidad que pueden brindar información sobre la política.
- ✓ Nombre, rol o responsable de quien autoriza la política.

- ✓ Describir los pasos y procedimientos para realizar ajustes a la política.
- ✓ Explicación de las consecuencias que se pueden tener en caso de que un funcionario, contratista o tercero incumpla la política.
- ✓ Fecha que inicia la vigencia de la política.

Es importante aclarar que una política NO es un estándar, es decir, no debe indicar cómo se ejecutará ninguna labor o control de manera específica, NO indica tecnologías específicas de uso. Son declaraciones muy generales y de alto nivel que plasman un objetivo a cumplir por parte de la organización.

EJEMPLO:

Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, EL INDERBU, empleará y distribuirá equipos con los controles criptográficos en toda la organización, conforme se establece en el PROCEDIMIENTO XYZ123.

POLITICAS ESPECÍFICAS

En este documento presenta algunas recomendaciones de políticas de seguridad de la información para el Modelo de Seguridad y privacidad de la Información para las Entidades del Estado. Este conjunto de recomendaciones no es exhaustivo, se aconseja 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. A continuación, se agruparán las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información, las políticas relacionadas con gestión de activos deben contemplar como mínimo:

- ✓ Identificación de Activos: Esta política debe determinar la periodicidad con la cual se va a realizar al interior de la Entidad la identificación y/o actualización del inventario de Activos de Información, la política debe determinar el responsable de realizar la actividad, se debe determinar bajo que instrumento se va a realizar la actividad, dicho instrumento debe permitir identificar el propietario del activo de información.
- ✓ Clasificación de Activos: La Entidad debe determinar la clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma. En la elaboración de esta política debe tenerse en cuenta las leyes y normatividades actuales que afecten a la Entidad, algunos ejemplos: Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo a la naturaleza de la entidad.
- ✓ Etiquetado de la Información: Esta política debe determinar el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos.
- ✓ Devolución de los Activos: Esta política debe determinar el instrumento y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Entidad.
- ✓ Gestión de medios removibles: Esta política debe contemplar los usos y permisos que tienen los usuarios y/o funcionarios de la Entidad frente a los medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores. Esta política debe describir detenidamente en qué casos se autoriza y en los que no, el uso de medios removibles y los procedimientos en los cuales se determinen las autorizaciones; adicionalmente debe describir el responsable de las autorizaciones y responsabilidades de aquellas personas que tienen autorización para el uso del dicho medio de almacenamiento. El uso de medios removibles en la entidad debe ir alineados a las clasificaciones de activos dispuestas en la política de “Clasificación de Activos”.
- ✓ Disposición de los activos: Esta política debe determinar la obligatoriedad para la construcción y cumplimiento de un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos. Esta política debe determinar la toma de backup de los activos evitando así el acceso o borrado no autorizado de la

información, la política debe indicar quien es el responsable de emitir las correspondientes autorizaciones y debe aplicar tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.

- ✓ Dispositivos móviles: Esta política debe determinar los funcionarios, contratistas o terceros que pueden tener acceso a las redes inalámbricas, quiénes pueden realizar instalación de chats corporativos y/o correos electrónicos de la entidad mediante el uso de este tipo de dispositivos, adicionalmente debe describir las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles, así como como los controles de seguridad que la entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

GESTIÓN DE ACTIVOS DE INFORMACIÓN

Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información, las políticas relacionadas con gestión de activos deben contemplar como mínimo:

- ✓ **Identificación de Activos:** Esta política debe determinar la periodicidad con la cual se va a realizar al interior de la Entidad la identificación y/o actualización del inventario de Activos de Información, la política debe determinar el responsable de realizar la actividad, se debe determinar bajo que instrumento se va a realizar la actividad, dicho instrumento debe permitir identificar el propietario del activo de información.

- ✓ **Clasificación de Activos:** La Entidad debe determinar la clasificación de los activos de información de acuerdo con la criticidad, sensibilidad y reserva de la misma. En la elaboración de esta política debe tenerse en cuenta las leyes y normatividades actuales que afecten a la Entidad, algunos ejemplos: Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo con la naturaleza de la entidad.

- ✓ **Etiquetado de la Información:** Esta política debe determinar el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos.

- ✓ **Devolución de los Activos:** Esta política debe determinar el instrumento y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Entidad.

- ✓ **Gestión de medios removibles:** Esta política debe contemplar los usos y permisos que tienen los usuarios y/o funcionarios de la Entidad frente a los medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores. Esta política debe describir detenidamente en qué casos se autoriza y en los que no, el uso de medios removibles y los procedimientos en los cuales se determinen las autorizaciones; adicionalmente debe describir el responsable de las autorizaciones y responsabilidades de aquellas personas que tienen autorización para el uso del dicho medio de almacenamiento. El uso de medios removibles en la entidad debe ir alineados a las clasificaciones de activos dispuestas en la política de “Clasificación de Activos”.

- ✓ **Disposición de los activos:** Esta política debe determinar la obligatoriedad para la construcción y cumplimiento de un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos. Esta política debe determinar la toma de Backup de los activos evitando así el acceso o borrado no autorizado de la información, la política debe indicar quien es el responsable de emitir las correspondientes autorizaciones y debe aplicar tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.

CONTROL DE ACCESO

Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales la Entidad determina los mecanismos de protección, los límites y

procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos;

las políticas relacionadas con el control de acceso deben contemplar como mínimo:

- ✓ Control de acceso con usuario y contraseña: Se debe elaborar una política sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la entidad, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas. La política debe enunciar las responsabilidades que los funcionarios, contratistas o terceros tienen al contar con un usuario o contraseña de la entidad, se debe estipular que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La entidad debe establecer que por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña para el acceso.
- ✓ Suministro del control de acceso: Esta política debe determinar los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, también deben tenerse en cuenta en esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad.
- ✓ Gestión de Contraseñas: Esta política debe definir los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la entidad. Esta política debe indicar a los funcionarios, contratistas y/o terceros los parámetros mínimos para que una contraseña sea considera como fuerte, gestión de cambio de contraseña, debe determinar que los accesos a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.
- ✓ Perímetros de Seguridad: La política debe definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los funcionarios, contratistas o terceros, tienen acceso y a cuáles no, la política

debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.

- ✓ Áreas de Carga: La política debe definir las condiciones e instalaciones físicas en las cuales se va a realizar despacho y carga de paquetes físicos para bodegas o espacios definidos de carga, esto con el fin de evitar el acceso no autorizado a otras áreas de la entidad. Esta política debe determinar el seguimiento que se debe realizar para garantizar el cumplimiento de dicha política y sus correspondientes responsables.

NO REPUDIO

La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción.

La política deberá incluir mínimo los siguientes aspectos:

- ✓ Trazabilidad: La política hará que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
- ✓ Retención: La política debe incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros de la Entidad.
- ✓ Auditoría: La política incluirá la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.
- ✓ Intercambio electrónico de información: La política incluirá en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

PRIVACIDAD Y CONFIDENCIALIDAD

Esta política debe contener una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente. La política de privacidad debe contener como mínimo lo

siguiente:

1. Ámbito de aplicación

2. Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales

3. Principios del tratamiento de datos personales:

a) Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
b) Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
c) Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
d) Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
e) Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
f) Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
g) Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
h) Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

4. Derechos de los titulares: La política debe indicar los derechos de los titulares de los datos, tales como:

- ✓ Conocer, actualizar y rectificar sus datos personales.
- ✓ Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
- ✓ Ser informado respecto del uso que se les da a sus datos personales.

- ✓ Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes con el Banco los servicios o productos que dieron origen a dicha autorización.
- ✓ Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales.

5. Autorización del titular: La política debe indicar cómo obtener autorización del titular para el tratamiento de sus datos personales, así como los casos en los cuales no se requiere autorización del titular.

6. Deberes de los responsables del Tratamiento: La política debe indicar cuales son los deberes de los responsables y/o encargados del tratamiento de los datos personales.

- ✓ Política de controles criptográficos: Esta política deberá especificar como se asegura la confidencialidad y autenticidad de la información que circula o se genera a través de los diferentes sistemas de información.
- ✓ La política de confidencialidad debe contener un compromiso o acuerdo de confidencialidad, por medio del cual todo funcionario, contratista y/o tercero vinculado a la Entidad, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Entidad, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.
- ✓ La política deberá indicar desde cuando se firma el acuerdo de confidencialidad, así como la vigencia del mismo.

INTEGRIDAD

La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que hagan parte de la Entidad, la cual se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos.

De esta manera, toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el Compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

La política de integridad deberá establecer asimismo la vigencia del mismo acorde al tipo de vinculación del personal al cual aplica el cumplimiento.

SEGURIDAD FISICA Y DEL ENTORNO

Los equipos de cómputo y servidores de Inderbu, ubicados en las instalaciones de la entidad, deberán ser mantenidos en un ambiente seguro y protegido por: controles de acceso y seguridad física, detección de incendio y sistemas de extinción de conflagraciones y sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

El acceso a los cuartos de cómputo deberá ser restringido y sólo a personal autorizado.

No se permitirá ingerir alimentos o bebidas en las instalaciones del Centro de Cómputo ni en los puestos de trabajo donde se encuentren equipos de cómputo.

El Inderbu contará con equipos de protección (firewall) desde y hacia internet para proteger la integridad y confidencialidad de la información.

Ningún usuario del Inderbu podrá instalar software sin licencia, solo podrá ser autorizado por el Líder Gestión TIC, quien revisará en los mantenimientos preventivos en este tema, de acuerdo con lo establecido en el Procedimiento Mantenimiento Correctivo y Preventivo.

Ningún equipo podrá ser retirado de su sitio sin autorización del responsable del proceso de Gestión TIC y haber diligenciado el formato de Traslado de Elementos.

Todo computador, servidor, dispositivo de comunicaciones como switches, enrutadores o cualquier otro hardware que requiera ser conectado a la red, debe tener la autorización y supervisión del Líder de Gestión TIC.

Los funcionarios y contratistas del Inderbu evitarán colocar encima o cerca de los computadores ganchos, clips u otros elementos o comida que puedan caer accidentalmente dentro del equipo y afectar su buen funcionamiento.

Con el fin de ahorrar energía, los funcionarios y contratistas apagarán las pantallas si se retiran temporalmente de su puesto y apagarán totalmente el equipo al finalizar la jornada laboral.

El Inderbu a través del proceso de Gestión TIC, realizará mantenimiento preventivo dos veces al año a los equipos de cómputo de propiedad de la Entidad, atendiendo el procedimiento establecido para ello.

Ningún funcionario o contratista está autorizado para efectuar algún tipo de intervención, reparación y/o modificación en un equipo a su cargo. El mantenimiento preventivo y correctivo debe ser realizado por personal del proceso de Gestión TIC.

Cuando se requiera sacar un equipo de cómputo de la Entidad, se deberá diligenciar el Formato de salida de préstamo de elementos.

La información que reposa en medios físicos como el papel, en lo posible debería permanecer guardada en sitios bajo llave o archivadores mientras no se esté haciendo uso de ella o se termine la jornada laboral. El manejo de esta información es responsabilidad de quien la tenga en custodia.

Los escritorios deberán permanecer libres de papeles una vez culmine la jornada laboral.

SEGURIDAD DE LAS OPERACIONES

El proceso de Gestión TIC del Inderbu realizará seguimiento al tráfico de la red especialmente cuando se tenga evidencia de actividad inusual o detrimentos en el desempeño.

Todos los equipos de cómputo de la Entidad deberán tener instalado software de antivirus licenciado y actualizado.

El proceso Gestión TIC, mantendrá actualizado el procedimiento de Administración de la red y comunicaciones del Inderbu.

El proceso de Gestión TIC registrará en las hojas de vida de cada equipo de coputo, todo evento ocurrido en ellos..

El Inderbu a través del proceso de Gestión TIC establecerá e implementará controles para evitar la descarga de software no autorizado, la infección con código malicioso proveniente de internet y el acceso a sitios catalogados como restringidos y de alta peligrosidad.

Los funcionarios y contratistas de la Entidad deben evitar la descarga de software, archivos, música, juegos o videos desde internet que puedan saturar el canal dedicado de internet, disminuir la velocidad de transmisión o llegar a ocasionar algún daño en el equipo.

Los funcionarios y contratistas usarán los recursos y servicios de internet para asuntos institucionales. El uso personal no debe interferir con la operación eficiente de los sistemas de la Entidad, ni con los deberes y obligaciones de funcionarios y/o contratistas.

El Inderbu establecerá un procedimiento para la publicación y actualización de la información en la Página Web, basada en la Ley 1712 de Transparencia y acceso a la información.

El acceso a internet a través del WIFI del Inderbu sólo será autorizado para computadores portátiles y celulares; la clave solo puede ser ingresada por personal autorizado de Gestión TIC.

Todos aquellos dispositivos de interconexión y servidores que conforman la plataforma tecnológica de la entidad y que lo ameriten, deben tener direcciones IP fijas. La asignación de estas direcciones debe estar documentada al detalle y mantenida por el administrador de la red de la entidad.

El Inderbu debe contar con un Plan de Contingencias tecnológico debidamente probado y actualizado que garantice la continuidad de los sistemas de misión crítica en la plataforma de la entidad, que cubra desde aplicativos y máquinas hasta sitio de operaciones.

COPIAS DE SEGURIDAD Y RESPALDO

Se deberán realizar y mantener copias de seguridad de la información del Inderbu, bases de datos e información de las unidades de red, dentro y fuera de la Entidad.

El Inderbu a través del proceso de Gestión TIC, establecerá un procedimiento o guía para realizar copias de seguridad, restauración y migración de la información.

Todos los sistemas de información que componen la plataforma de la entidad deberán incluir la documentación necesaria para garantizar la ejecución de tareas de recuperación de la información.

El proveedor del Hosting deberá tener mínimo 2 copias de seguridad de la información contenida en las páginas web de la Entidad.

Cuando haya rotación de equipos de cómputo, se eliminará la información, pero antes el usuario realizará Backup del disco duro y el proceso de Gestión TIC a la información contenida en las unidades de red.

- ✓ Se debe contar con un sistema automático para la recolección de copias de respaldo.
- ✓ Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.
- ✓ Los medios magnéticos que contienen información deben ser almacenados en lugares estrictamente seguros.
- ✓ Los medios magnéticos deben tener rótulos visibles y legibles tanto internos como externos.
- ✓ Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportunamente.
- ✓ Para responder adecuadamente a una contingencia, los respaldos de la información se deben almacenar en sitios externos.
- ✓ Cualquier medio magnético que contenga información clasificada como restringida o confidencial, debe estar claramente identificada.
- ✓ AI enviar Información clasificada como restringida o confidencial a terceros se debe exigir una notificación de recibo.
- ✓ Todos los medios que contengan información clasificada como restringida o confidencial y que finalice su ciclo de vida, deben ser sobre escritos o destruidos físicamente para que la información no pueda ser recuperada.

- Es responsabilidad de los Administradores de las Plataformas, mantener respaldo de la configuración del sistema operativo y de los servicios que estas proveen.

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Los desarrolladores de software deberán garantizar ambientes seguros de desarrollo, pruebas y producción, materializado en obligaciones específicas de los contratos.

Los desarrolladores de software deberán conocer e implementar la guía de estilo e imagen institucional en aspectos en los que aplique e implementar la metodología propuesta para el desarrollo de sistemas de información.

Los desarrolladores de software deberán especificar las carpetas y archivos a los cuales se les debe sacar copias de seguridad.

Cada sistema de información o aplicativo debe mantener actualizado su documentación.

En los contratos de los proveedores, se debe establecer como obligación específica la entrega de la documentación necesaria para la administración y funcionamiento del sistema o aplicativo, incluir manuales de uso.

Los proveedores de software deberán realizar transferencia de conocimiento, obligación específica que debe estar consignada en el contrato.

REGISTRO Y AUDITORÍA

Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

Esta política deberá contener:

- ✓ Responsabilidad: Incluir la responsabilidad de la Oficina de Control Interno y similares, acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.

- ✓ Almacenamiento de registros: La política debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de las mismas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.
- ✓ Normatividad: La política de auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.
- ✓ Garantía cumplimiento: La política de auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar las deficiencias detectadas.
- ✓ Periodicidad: La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logra a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

La entidad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

- ✓ La política debe contemplar para su elaboración los siguientes parámetros:
  - Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.
  - Visión General: ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?
  - Definir responsables: Se deben mencionar de manera muy general quienes serán los responsables de gestionar los eventos.
  - Actividades: Explicar de manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución.
  - Documentación: Se debe hacer referencia sobre la documentación del esquema de gestión y los procedimientos.
  - Descripción Del Equipo Que Manejará Los Incidentes: Se debe indicar como está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad.

- Aspectos Legales: Deben citarse los aspectos legales que se deben tener en cuenta o los cuales debe darse cumplimiento.
-

CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN:

Esta política se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

Dicha política debe contener los siguientes parámetros.

- ✓ El compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas.
- ✓ ¿Quiénes deberán ser entrenados? ¿Quiénes deberán ser sensibilizados?
- ✓ La obligación de los usuarios a asistir a los eventos o cursos de capacitación.
- ✓ Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
- ✓ Definir los roles y responsabilidades de quienes diseñarán los programas, quienes los comunicarán.
- ✓ Documentación sobre planes de estudio y desarrollo de los programas.
- ✓ Compromisos y obligaciones por parte del personal capacitado.
- ✓ Contener políticas adicionales relacionadas directamente con el debido comportamiento de los usuarios como las siguientes:
- ✓ Política De Escritorio Limpio
- ✓ Política De Uso Aceptable
- ✓ Ética Empresarial

APOYO Y APRENDIZAJE

TOMA DE CONCIENCIA

- Brindar lineamientos para que los servidores públicos, contratistas y proveedores de la Entidad reciban la educación y formación en toma de conciencia adecuada, y actualizaciones sobre las políticas y procedimientos.
- El proceso de Gestión de Talento Humano y el supervisor del contrato, deberán velar por que los servidores públicos, contratistas y proveedores de la Entidad,

que desempeñen funciones en el mismo reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.

- Será responsabilidad de Recursos Humanos, incorporar la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

COMUNICACIÓN

- El presente manual de políticas de Seguridad y Privacidad de la Información será comunicado a todas las partes interesadas de la Entidad, a través de las tecnologías de la información y medios físicos de ser necesario.
- La Alcaldía de Bucaramanga deberá establecer los canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI), algunos canales accesibles y formales para la comunicación son: Correo Electrónico, intranet, comunicación impresa, charlas y capacitaciones.

EVALUACIÓN DE ACTIVIDADES

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

- Se deben establecer los indicadores de medición de los Objetivos de Seguridad y Privacidad de la Información.
- Se deben realizar revisiones mínimo una vez al año del cumplimiento de las políticas de Seguridad y Privacidad de la Información e incluir el criterio de seguridad en los planes de auditoría anual.

REVISIÓN POR LA DIRECCIÓN

La Alta Dirección debe realizar anualmente la revisión al Sistema de Gestión de Seguridad de la Información. Esta revisión debe incluir:

a. Seguimiento de tareas, actividades o acciones asignadas en la reunión anterior.

b. Informe de resultados de las revisiones del Sistema de Gestión de Seguridad de la Información al interior de los procesos.

c. Resultados del último ciclo de auditoría interna al SGSI (informe de Auditoría Interna).

d. Cambios en las cuestiones internas y externas que sean pertinentes al SGSI.

e. Propuestas o mejoras al SGSI por parte de los servidores públicos y contratistas.

f. Estado de acciones correctivas y de mejora (se evalúa la eficacia de las acciones), para Seguridad de la Información sólo aplica las acciones correctivas y de mejora.

g. Retroalimentación de las partes interesadas.

h. Resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos.

i. Vulnerabilidades y amenazas no tratadas adecuadamente en la valoración previa de los riesgos.

j. Revisión anual de la política, objetivos de Seguridad de la Información (su contenido y cumplimiento en los diferentes procesos) por medio de planes de acción.

REVISIÓN, VIGENCIA Y APROBACIÓN DEL MANUAL DE POLÍTICA

La presente política se revisa anualmente, o antes si existiesen cambios relevantes en el contexto interno y externo que afecten el logro de los objetivos institucionales y de seguridad de la información gestionada por la entidad, con el objeto de mantener la política oportuna, eficaz y suficiente. La obligación descrita está bajo la responsabilidad del Líder de Seguridad de la Información y por el Comité Institucional de Gestión y Desempeño.

El presente manual empieza a regir a partir de la fecha de su aprobación y oficialización.

Aprobado por:	**Aprobado por:**	**MEDIANTE COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO MIPG DEL 9 DE DICIEMBRE DE 2022, ACTA N°08**
Cargo:	**Cargo:**	**SUBDIRECCION ADMINISTRATIVA Y FINANCIERA**
Firma:	**Firma:**	**SILVIA NATHALIA NIÑO VILLAMIZAR**
Fecha:	**Fecha:**	**9 DE DICIEMBRE DE 2022**