POLÍTICAS DE SEGURIDAD DIGITAL

GOBERNACIÓN DEL DEPARTAMENTO DE LA GUAJIRA

CONTROL DE CAMBIOS			
VERSIÓN No.	**FECHA DE EMISIÓN**	**ELABORÓ**	**DESCRPCIÓN DEL CAMBIO**
1	2022-07-29	**CLEIDER MIGUEL SIERRA RAMOS**	VERSIÓN ORIGINAL

ELABORÓ	**REVISÓ**	**APROBÓ**
NOMBRE: CLEIDER MIGUEL SIERRA RAMOS	NOMBRE YONNEY ISMAEL DÍAZ JIMÉNEZ	NOMBRE: CIGD
CARGO: Profesional MIPG - MCI – CALIDAD	CARGO: Director Departamento Administrativo de Planeación	CARGO:

Tabla de contenido

1. INTRODUCCIÓN

La información es un activo que la Gobernación de La Guajira la cual tiene el deber y la responsabilidad de proteger y salvaguardar de una manera segura la información que produce, garantizando su disponibilidad, integridad y confidencialidad, con el objeto esencial de proporcionar servicios eficientes y oportunos a la comunidad en general.

Para garantizar la seguridad digital, la Gobernación de La Guajira propende por desarrollar los enfoques a nivel de seguridad de la entidad, donde se construyan las políticas de seguridad digital y de la información a fin de salvaguardar la misma a nivel físico y electrónico, de manera que se pueda en todo momento garantizar su integridad, disponibilidad y autenticidad. En esa línea el aseguramiento de los procesos relacionados con los sistemas de información debe complementarse con un enfoque de privacidad para garantizar tanto la protección digital como la información de la administración.

La política de Seguridad Digital tiene como objetivo definir las políticas de seguridad digital (información e informática) que se deben seguir por parte de los funcionarios, contratistas, pasantes y proveedores de la Entidad, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información.

2. JUSTIFICACION

Las entidades gubernamentales deben propender por el uso responsable de los activos informáticos y de igual manera minimizar los riesgos que propicien delitos informáticos a los que está expuesto un dispositivo al conectarse a una red o interactuar con otro dispositivo, máxime si no se tienen directrices, normas o lineamientos, riesgos como son uso indebido de información, interceptación, robo o suplantación de identidad, entre otros, se deben de contrarrestar y adoptar mecanismos de autenticación y control de acceso, atendiendo las prácticas del buen gobierno y como objetivo primordial; por lo tanto, se debe proveer una visión tecnológica y liderar el desarrollo e implantación de iniciativas que estén acordes con el entorno cambiante tecnológico, alineados con las metas institucionales y el cumplimiento de los fines esenciales del Estado.

Este documento Política de Seguridad Digital - PSD, busca protección y la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la protección de los datos, mediante la aplicación del proceso de gestión de la información en la entidad, brindando confianza a las partes interesadas acerca de la seguridad digital que brinda la Entidad.

3. Objetivo

El objetivo de este documento es establecer las políticas y lineamientos en seguridad digital de la Gobernación de LA Guajira, con el fin de regular su gestión al interior de la Entidad y definir las políticas de seguridad digital (información e informática) que se deben seguir por parte de los funcionarios, contratistas, pasantes y proveedores con el fin de preservar la disponibilidad, integridad y confidencialidad de la información.

4. Alcance

Las políticas de seguridad digital cubren todos los procedimientos que tiene la Entidad para la búsqueda de una adecuada protección y calidad de la información de acuerdo a las políticas y directrices definidas en la presente Política también aplican para todos los funcionarios, contratistas, pasantes y proveedores de la Gobernación de La

Guajira.

5. DEFINICIONES

- **Activo de información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de servicio de la Entidad y, en consecuencia, debe ser protegido.
- **Acuerdo de Confidencialidad:** es un documento en los contratistas y personal provisto por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.
- **Acuerdo de Nivel de servicio (ANS):** son los acuerdos que se hacen con los usuarios de los servicios en los cuales se estipula el nivel de calidad para la aceptación del servicio.
- **Análisis de riesgos de seguridad digital:** proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades, comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **Autenticación:** es el procedimiento de comprobación de la Entidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Capacity Planning:** es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la Entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.
- **Centros de cableado:** son cuartos o habitaciones donde se deben instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
- **Centro de cómputo:** es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.
- **Ciberamenaza o amenaza cibernética:** aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.
- **Ciberataque o ataque cibernético:** acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.
- **Ciberespacio:** entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.
- **Ciberiesgo o riesgo cibernético:** posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.
- **Ciberseguridad:** Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.
- **Cifrado:** es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, acceso no autorizado a los repositorios de información.

- **Componentes informáticos:** son todos aquellos recursos tecnológicos que hacen referencia a: aplicativos, software de sistemas, sistemas operativos, bases de datos, redes, correo electrónico, software ofimático, software de seguridad, hardware y equipos de comunicaciones.
- **Confidencialidad:** es la garantía de que la información no es divulgada a personas, Entidades o procesos no autorizados.
- **Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, lineamientos, manuales, guías, formatos, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- **Criptografía:** es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
- **Custodio del activo de información:** es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
- **Derechos de Autor:** es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
- **Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- **Equipo de cómputo:** dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
- **Evento de seguridad:** ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el servicio.
- **Guías de clasificación de la información:** directrices para catalogar la información de la Entidad y hacer una distinción entre la información que es calificada como pública clasificada o pública reservada y de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información
- **Hacking ético:** es el conjunto de actividades para ingresar a las redes de datos y voz de la entidad con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.
- **Incidente de seguridad:** ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la Entidad que son esenciales para el servicio.
- **Información en reposo:** datos guardados en dispositivos de almacenamiento persistente (por ejemplo, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).
- **Información en tránsito:** información que fluye a través de la red pública, como Internet, y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial.
- **Integridad:** es la protección de la exactitud y estado completo de los activos.
- **Inventario de activos de información:** es una lista ordenada y documentada de los activos de información pertenecientes a la Gobernación de La Guajira.
- **Licencia de software:** es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
- **LOG (Registro):** es el registro de auditoría de las acciones y de los acontecimientos que ocurren en un sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para

reportar rastro de lo que se está ejecutando sobre la plataforma tecnológica.

- **Medio removible:** es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
- **Perfiles de usuario:** son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- **Propiedad intelectual:** es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.
- **Propietario de la información:** es la unidad organizacional o proceso donde se crean los activos de información.
- **Resiliencia:** es la capacidad de un mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que pudo estar sometido.
- **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Gobernación de La Guajira.
- **Registros de Auditoría:** son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la Entidad. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
- **Responsable por el activo de información:** es la persona o grupo de personas, designadas por la Alta Dirección, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **Sensibilización:** es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- **SGSI**: Sistema de Gestión de Seguridad de la Información.
- **Sistema de información:** es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Gobernación de La Guajira o de origen externo ya sea adquirido por la Entidad como un producto o servicio estándar de mercado o desarrollado para las necesidades de ésta.
- **Sistemas de control ambiental:** son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.
- **Software malicioso:** es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- **Teletrabajo:** Hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de

trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual".

- **Terceros:** todas las personas, jurídicas o naturales, como proveedores, contratistas, pasantes o consultores, que provean servicios o productos a la Entidad.
- **Vulnerabilidades:** son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Entidad (amenazas), las cuales se constituyen en fuentes de riesgo.

6. POLÍTICA GLOBAL DE SEGURIDAD DIGITAL

En la Gobernación de La Guajira es vital importancia brindar la confianza a nuestros ciudadanos y partes interesadas, propendiendo porque la información administrada, está debidamente protegida, porque con ella, establecemos un marco de referencia de gestión para iniciar y controlar la implementación de la seguridad digital al interior de la Entidad por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de TIC. Los productos y servicios están asegurados con un modelo de seguridad digital, que gestiona los riesgos para garantizar la confidencialidad, integridad, disponibilidad y privacidad que contribuyen al desarrollo de la estrategia del servicio y el cumplimiento de misión institucional.

Nuestros funcionarios, procesos e infraestructura tecnológica están dispuestos con la finalidad de cumplir con los requisitos legales y de seguridad digital para mejorar continuamente las nuevas necesidades que surjan sobre la seguridad digital.

7. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección (Gobernador) y el Comité Institucional de Gestión y Desempeño aprueban esta Política de Seguridad Digital como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad digital de la Entidad.

La Alta Dirección de la Entidad demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad Digital contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de esta política todos los funcionarios, contratistas y pasantes de la Entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad digital.
- La verificación del cumplimiento de las políticas aquí mencionadas.

8. SANCIONES POR LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DIGITAL

El incumplimiento de las políticas de seguridad digital se gestiona a través de procedimientos administrativos que pueden conducir a procesos disciplinarios o penales según aplique de acuerdo con la gravedad de la falta. La Gobernación de La Guajira cuenta con canales de comunicación donde el personal puede reportar posibles incumplimientos que afecten la seguridad digital.

La utilización indebida de perfiles de usuarios para obtener beneficio propio o en favor de terceros será sancionado de

acuerdo con los procedimientos administrativos definidos.

9. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DIGITAL

Cada rol y responsabilidad para la seguridad digital está claramente definido y se realiza con las políticas institucionales. La orientación, definición y revisión de la administración del Sistema de Gestión Seguridad de la Información es liderada por el Comité de Seguridad de la Información.

A cada uno de los funcionarios, contratistas y pasantes se le asignará una responsabilidad con el Sistema de Gestión Seguridad de la Información y las mismas están reflejadas en este documento. La gestión de riesgos y la evaluación de riesgo residual es responsabilidad de los Líderes de los Procesos con el apoyo de la Dirección de Planeación - Oficina de MIPG – MECI Y CALIDAD.

10. POLÍTICAS DE SEGURIDAD DIGITAL

10.1. Política de organización interna

Establecer un marco de referencia de gestión para iniciar y controlar la implementación de la seguridad digital al interior de la Gobernación de La Guajira por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con la ciudadanía y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de TIC, buscando preservar la confidencialidad, integridad y disponibilidad de la información.

Alcance
La Política de Organización Interna aplica a todos los funcionarios, contratistas, pasantes y terceros de la Gobernación de La Guajira.

10.2 Política para dispositivos móviles

Establecer los lineamientos para el buen uso y administración de los equipos de computación y comunicación móvil asignados o autorizados por la Gobernación de La Guajira, en el desarrollo de las actividades por parte de los funcionarios, contratistas, pasantes en el ejercicio de sus funciones y así asegurar la confidencialidad, la integridad y la disponibilidad de la información de la Entidad contenida en estos.

Alcance
La política para uso de dispositivos móviles será aplicada por la Secretaría General, a todos los funcionarios, contratistas, pasantes y terceros que utilicen dispositivos móviles para acceder a los servicios ofrecidos por la Gobernación de La Guajira (red, Internet, correo electrónico, sistemas de información etc.).

10.3 Política de Teletrabajo

Proteger la información de la Gobernación de La Guajira a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Alcance
La política de teletrabajo aplica para los funcionarios de planta de la Gobernación de La Guajira, con quienes se establezca un contrato de trabajo que, para su ejecución, se realice mediante el teletrabajo.

10.4 Política de trabajo remoto

Proteger la información de la Gobernación de La Guajira a la que se tiene acceso y aquella que es procesada o almacenada en los lugares en los que se realiza el trabajo remoto por parte de los funcionarios, contratistas, pasantes y terceros que lo requieran y estén autorizados.

Alcance
La política de trabajo remoto será aplicada por la Secretaría General – Dirección de Talento Humano, a todos los funcionarios, contratistas, pasantes y terceros de la Gobernación de La Guajira que requieran por su tipo vinculación o contrato acceder a los servicios tecnológicos ofrecidos por la Entidad (conectar sus equipos móviles, ingresar a la red, internet, correo electrónico, sistemas de información, acceder a la información etc.), en un sitio diferente a las instalaciones de Gobernación
.

10.5 Política de seguridad de los recursos humanos

Asegurar que los funcionarios, contratistas, pasantes y terceros comprendan y toman conciencia sobre sus responsabilidades de seguridad de la información y las cumplan, además asegurar que son idóneos en los roles asignados y que se protegen los intereses de la Gobernación de La Guajira como parte del proceso de cambio de vinculación o terminación de esta.

Alcance
La política de seguridad de los recursos humanos debe ser cumplida por todos los funcionarios, contratistas, pasantes y terceros de todos los procesos de la Entidad; cubre los objetivos de control (Norma ISO 27001): antes de asumir, durante la ejecución y la terminación o cambio de la vinculación a la Entidad.

10.6 Política de uso adecuado de los recursos

Dar un buen uso a los recursos: correo electrónico, internet, redes sociales, recursos tecnológicos (Equipo de cómputo), uso de software legal y derechos de autor, acceso inalámbrico que provee la Gobernación de La Guajira a todos los funcionarios, contratistas, pasantes y terceros para el cumplimiento de sus funciones u obligaciones, y para proteger la información de la Entidad.

Alcance
Aplica para todos los funcionarios, contratistas, pasantes y terceros vinculados con la Gobernación de La Guajira que tienen acceso a los servicios de correo electrónico, acceso a internet, redes sociales, recursos tecnológicos (Equipos de cómputo), uso de software legal y derechos de autor, acceso inalámbrico para el desarrollo de sus funciones
.

10.7 Política de gestión de activos de información

Identificar los activos de información de la Gobernación de La Guajira para definir las responsabilidades de protección apropiadas y clasificarlas para asegurar que la información de la Entidad recibe un nivel apropiado de protección, de

acuerdo con su importancia, y se efectúe un manejo adecuado de los medios para evitar la divulgación, modificación, el retiro o la destrucción no autorizada de la información de la Gobernación almacenada en ellos.

Alcance
Aplica para los activos de información de todos los procesos de la Gobernación de La Guajira.

10.8 Política de control de acceso

Definir las directrices generales para un acceso controlado a servicios de tecnología (Red, servicios asociados, sistemas de información) e información de la Gobernación de La Guajira.

Alcance
Esta política aplica para todos los funcionarios, contratistas, pasantes y terceros que cuenten con accesos a los servicios de tecnología (Red, servicios asociados, sistemas de información) e información de la Gobernación de La Guajira.

10.9 Política sobre controles criptográficos

Buscar que se dé un uso adecuado y eficaz de sistemas y técnicas criptográficas para la protección de la información de la Gobernación de La Guajira, con base al análisis de riesgo efectuado, con el fin de asegurar la protección de su confidencialidad e integridad.

Alcance
La política de controles criptográficos aplica para las comunicaciones, bases de datos y unidades de disco duros de los equipos de cómputo portátiles con que cuenta la Entidad.

10.10 Política de seguridad física y del entorno

Minimizar los riesgos de daños e interferencias a la información y a las operaciones de la Gobernación de La Guajira, evitando accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información de la Entidad.

Alcance
Esta política aplica para el control de acceso físico a las áreas seguras dentro de las cuales se encuentran el centro de datos, centros de cableado, áreas de archivo, áreas de recepción, tesorería, despachos y entrega de correspondencia, las cuales deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información de la Gobernación de La Guajira.

10.11 Política de escritorio y pantalla limpios

Mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información de la Gobernación de La Guajira.

Alcance
Esta política aplica para todos los funcionarios, contratistas, pasantes y terceros de la Gobernación de La Guajira.

10.12 Política de seguridad de las operaciones

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información de la Gobernación de La Guajira.

Alcance
Esta política aplica para la oficina de sistema de la Secretaría General de la Gobernación de La Guajira.

10.13 Política de gestión de seguridad de las redes

Fortalecer la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte de la Entidad.

Alcance
Esta política aplica para todas las redes, los servicios de red y los controles utilizados para proteger la información en la transferencia de información de la Entidad.

10.14 Política de intercambio de información

Proteger la transferencia de información de la Gobernación de La Guajira mediante el uso de todo tipo de instalaciones de comunicación, como correo electrónico, VPN, SFTP, etc.

Alcance
Esta política de intercambio de información aplica para la información que sea enviada por los funcionarios, contratistas, pasantes y terceros a través de correo electrónico y los demás canales que se autoricen VPN, SFTP, etc.

10.15 Política de adquisición, desarrollo y mantenimiento de sistemas

Fortalecer la seguridad digital y que sea una parte integral de los sistemas de información de la Gobernación de La Guajira durante todo su ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

Alcance
Esta política aplica para todos los sistemas de información de la Entidad, incluyendo los sistemas de información que prestan servicios sobre redes públicas.

10.16 Política de desarrollo seguro

Propender para que la seguridad digital esté diseñada e implementada dentro del ciclo de vida planeación y desarrollo de los sistemas de información.

Alcance
Esta política aplica para todos los desarrollos de sistemas de información en la Entidad.

10.17 Política de seguridad de la información para las relaciones con proveedores

Buscar la protección de los activos información de la Gobernación de La Guajira que sean accesibles a los proveedores.

Alcance
Esta política aplica para todos los proveedores que para la ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica de la Entidad.

10.18 Política de gestión de incidentes y mejoras en la seguridad digital.

Gestionar todos los incidentes de seguridad digital reportados en la Gobernación de La Guajira, adecuadamente, dando cumplimiento a los procedimientos establecidos.

Alcance
Esta política aplica para todos los funcionarios, contratistas, pasantes y terceros de la Gobernación de La Guajira que detecten un evento o incidente de seguridad digital el cual deben reportar, adecuadamente, de acuerdo con los procedimientos establecidos por la Entidad.

11. INFORMACIÓN DE CONTACTO

Cualquier inquietud relacionada con las políticas, favor remitirla al correo seguridaddigital@laguajira.gov.co.

12. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DIGITAL

Estas políticas deben ser revisadas oportunamente por la Oficina de Sistema de la Secretaría General como mínimo una vez al año.

13. REFERENTES NORMATIVOS

13.1. Referentes de políticas de la Gobernación de La Guajira

Manual del Sistema Integrado de Gestión, Sistema de Gestión de Seguridad de la Información

13.2. Referentes de política nacional

Manual de seguridad y privacidad de la información, Estrategia de Gobierno Digital.
Norma técnica Colombiana NTC-ISO/IEC 27001.

Política definida en el manual	Control ISO27001	Modelo de Seguridad y Privacidad Min TIC
Política de organización interna	Dominio A.6.1 Organización interna Controles: A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4, A.6.1.5	Guía no 2 - Política General MSPI Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información. Inventario

Política definida en el manual	Control ISO27001	Modelo de Seguridad y Privacidad Min TIC
Política para dispositivos móviles	Dominio A.6.2 Dispositivos móviles y teletrabajo: Controles A.6.2.1	Guía no 2 - Política General MSPI
Política de teletrabajo	Dominio A.6.2 Dispositivos móviles y teletrabajo – Controles A.6.2.2	Guía no 2 - Política General MSPI
Política de trabajo remoto	Dominio A.6.2 Dispositivos móviles y teletrabajo – Controles A.6.2.2	Guía no 2 - Política General MSPI
Política de seguridad de los recursos humanos	Dominio A.7 Seguridad de los recursos humanos Controles A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1	Guía no 2 - Política General MSPI
Política de uso adecuado de los recursos	Dominio A.7 Seguridad de los recursos humanos Controles: A.7.2.2	Guía no 2 - Política General MSPI
Política de seguridad de los recursos humanos	Dominio A.7 Seguridad de los recursos humanos Controles A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2., A.7.3.	Guía no 2 - Política General MSPI
Política de uso adecuado de los recursos	Dominio A.7 Seguridad de los recursos humanos Objetivo de control A.7.2 Durante la ejecución del empleo Controles A.7.2.2	Guía no 2 - Política General MSPI
Política de gestión de activos	Dominio A.8 Gestión de activos. Controles A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.3, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3	Guía no 2 - Política General MSPI
Política de control de acceso	Dominio A.9 Control de acceso Controles A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3	Guía no 2 - Política General MSPI
Política de controles criptográficos	Dominio A.10 Criptografía Controles A.10.1.1, A.10.1.2	Guía no 2 - Política General MSPI
Política de seguridad física y del entorno	Dominio A.11 Seguridad física y del entorno Controles A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5	Guía no 2 - Política General MSPI

Política definida en el manual	Control ISO27001	Modelo de Seguridad y Privacidad Min TIC
	A.11.2.1, A.11.2.2, A.11.2.3 A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8., A.11.1.3 A.11.1.6	
Política de escritorio limpio y pantalla limpia	Dominio A.11 Seguridad física y del entorno Control A.11.2.9	Guía no 2 - Política General MSPI
Política de seguridad de las operaciones	Dominio A.12 Seguridad de las operaciones Controles A.12.1.1, A.12.1.2, A.12.1.3, A.12.1.4, A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.3, A.12.4.4, A.12.5.1, A.12.6.1, A.12.6.2, A.12.7	Guía no 2 - Política General MSPI
Política de seguridad de las comunicaciones	Dominio A.13 Seguridad de las comunicaciones Controles A.13.1.1, A.13.1.2, A.13.1.3 .13.2.1, A.13.2.2 A.13.2.3, A.13.2.4	Guía no 2 - Política General MSPI
Política de adquisición, desarrollo y mantenimiento de sistemas	Dominio A.14 Adquisición, desarrollo y mantenimiento de sistemas Objetivo de control A.14.1 Requisitos de seguridad en los sistemas de información Controles A.14.1.1, A.14.1.2, A.14.1.3	Guía no 2 - Política General MSPI
Política de desarrollo seguro	Dominio A.14, A.14.2 A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1	Guía no 2 - Política General MSPI
Política de seguridad de la información para las relaciones con proveedores	Dominio A.15 Objetivo de control A.15.1 Controles A.15.1.1, A.15.1.2 A.15.1.3, A.15.2 A.15.2.1 A.15.2.2	Guía no 2 - Política General MSPI

Política definida en el manual	Control ISO27001	Modelo de Seguridad y Privacidad Min TIC
Política de gestión de incidentes y mejoras en la seguridad digital.	Dominio A.16 Gestión de incidentes de seguridad de la información Objetivo de control A.16.1 Controles A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7.	Guía no 2 - Política General MSPI
Política de seguridad de la información en la continuidad de negocio.	Dominio A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio Objetivo de control A.17.1 Continuidad de seguridad de la información Controles A.17.1.1, A.17.1.2, A.17.1.3 A.17.2, A.17.2.1	Guía no 2 - Política General MSPI
Política cumplimiento de requisitos legales y contractuales	Dominio A.18 Cumplimiento Objetivo de control A.18.1 Cumplimiento de requisitos legales y contractuales Controles A.18.1.1, A.18.1.2 A.18.1.3, A.18.1.4 A.18.1.5. A.18.2.1, A.18.2.2 A.18.2.3	Guía no 2 - Política General MSPI

14. CONTROL DE CAMBIO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre y Cargo: Cleider Miguel Sierra Ramos, Profesional Universitario, Coordinador MIPG-MECI **Fecha:** *29 de julio de 2022*	**Nombre y Cargo: Yonner Ismael Díaz Jiménez,** Director de Planeación. **Fecha:** *29 de julio de 2022*	**Nombre y Cargo: CIGD**. **Fecha**: 29 de julio de 2022