POLÍTICA DE SEGURIDAD DIGITAL

La Presidencia de la **INDUSTRIA MILITAR,** entendiendo la importancia de la implementación de Gobierno Digital y el Modelo de Seguridad y privacidad de la información, se ha comprometido con el mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información SGSI (ISO 27001:2013), orientada a la identificación, gestión y mitigación de riesgos de seguridad digital, así como establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos digitales, todo esto enmarcado, en el estricto cumplimiento de las leyes, el Modelo de Planeación y Gestión – MIPG y en concordancia con la misión y la visión de la Entidad.

Así mismo, se tiene el firme propósito de realizar una gestión sistemática de riesgos en seguridad digital, protección de activos de información y promover un entorno digital confiable y seguro, buscando preservar la confidencialidad, integridad y disponibilidad de la información.

Por lo anterior, esta política aplica para toda la Entidad (Funcionarios, practicantes, terceros, proveedores y demás partes interesadas), teniendo en cuenta los principios de confidencialidad, integridad y disponibilidad, sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI.

Nota: La **Gerencia de Tecnologías de la Información**, para efectos de la presente política también se denominará con la sigla **GTI**.

La presente política estará determinada por los siguientes lineamientos:

1. Política Dispositivos Móviles

Para el uso de dispositivos móviles como: Equipos de cómputo, portátiles, teléfonos móviles, tablet, la **GTI** debe implementar controles de acceso, como técnicas criptográficas para cifrar la información crítica almacenada en los mismos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información, de ahí se establece lo siguiente:

a) Obligaciones

- Los dispositivos móviles deben contar con un software de cifrado que protejan la integridad y confidencialidad de la información, en caso de pérdida y/o robo del dispositivo.

- En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de la Industria Militar, se debe reportar la perdida lo más pronto posible a la **GTI**.

- Los dispositivos móviles (Portátiles) deben contar con guayas de seguridad que ayuden a controlar la manipulación o traslado no autorizado.

- Los dispositivos móviles deben tener activa en la configuración, la opción remota de borrado seguro de la información con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.

- Los dispositivos autorizados permanentemente deben estar registrados en el formato relación de entrada y salida de dispositivos móviles autorizados a las instalaciones físicas y red de Indumil IM OC OFI FO 026, y deberá reposar una copia del formato en las porterías principales de cada unidad de negocio, debidamente firmado por el Gerente de Tecnologías de la Información.

- Todos los dispositivos móviles deben contar con una herramienta de antivirus debidamente actualizada.

b) Restricciones

- Está prohibido realizar instalación de aplicaciones y/o software no autorizado por la **GTI**.

- Está prohibido el uso de teléfonos celulares personales para el manejo de procesos e información pública reservada de la Industria Militar.

- Está prohibido el almacenamiento de información de la Industria Militar en dispositivos móviles que no son activos fijos de la organización.

2. Política de Control de Acceso

Evitar el acceso no autorizado a los sistemas y/o servicios de tecnología de la información (TI), estableciendo lineamientos y controles de acceso, a

personas no autorizadas para hacer uso de los recursos tecnológicos asociados a la **GTI**.

a) Obligaciones

- Cada usuario de la Entidad debe hacer uso de su cuenta y contraseña, que será de manejo exclusivo, personal e intransferible.

- Al otorgar acceso a los sistemas de información se debe dar una capacitación clara al usuario sobre los requisitos de seguridad que debe cumplir, para proteger apropiadamente la información de la Entidad.

- Los equipos que por motivos de fuerza mayor estén fuera de la red de Indumil tendrán un usuario Gestor, el cual será el administrador del equipo. Así mismo, los equipos serán controlados por los funcionarios de soporte a usuarios de la **GTI**.

- Los usuarios a excepción de los administradores y el personal de soporte de Tecnologías de la Información, tienen restringida la instalación de software, si se requiere instalar algún programa, se debe solicitar soporte a la Mesa de Ayuda.

- El acceso a la información de la Industria Militar obliga al usuario a la aceptación formal de los reglamentos de acceso y tratamiento de la información, que definan las leyes, políticas, estándares y/o acuerdos establecidos por la Entidad.

- Todos los funcionarios, contratistas y terceros que prestan sus servicios a la Industria Militar, deben cumplir con los controles de seguridad definidos por la Entidad, para garantizar la confidencialidad, integridad y disponibilidad de la información que está a su cargo.

- La **GTI** debe establecer los roles de acceso de los usuarios con base a los requisitos de cada proceso y/o sub proceso de la Industria Militar.

b) Restricciones

- No se permite la modificación de la información de la Industria Militar, sin contar con la autorización formal para dichas novedades.

- No se permite la divulgación no autorizada de la información privada y clasificada de la Entidad.
- No se permite negar el acceso a la información de la Entidad, sin la debida justificación por parte de la **GTI**.
- No se permite la modificación y/o eliminación de los controles de seguridad que protejan la información de la Entidad.

3. Política de Controles Criptográficos

Identificar la información de la Entidad que requiera ser protegida por razones de confidencialidad, integridad y disponibilidad, con el objeto de establecer y hacer uso de técnicas y herramientas de cifrado criptográfico, las cuales serán administradas por la **GTI** de INDUMIL.

a) Obligaciones

- La información reservada y la información clasificada de la Entidad, que deba ser transportada por líneas de comunicación, dispositivos móviles o sistemas de almacenamiento removible, debe ser cifrada antes de su transporte o almacenamiento
- Con el fin de validar la autenticación de origen, no repudio y confirmar que el mensaje enviado no ha sido alterado desde que fue firmado por el emisor, se implementaran las firmas digitales y llaves criptográficas a través de un ente certificador.

b) Restricciones

- No se permite utilizar software de cifrado de datos, que no esté autorizado por la **GTI**.
- No se permite cifrar información sin la autorización del responsable de la información.
- No se permite cifrar información de datos abiertos.
- No se permite divulgar claves, contraseñas o llaves de cifrado de datos, a personal no autorizado por parte de la **GTI**.

- No se permite utilizar firmas digitales y llaves criptográficas ajenas a las asignadas por la **GTI**, para beneficio propio o de terceros.

4. Política de Escritorio y pantalla limpia

El objetivo es reducir los riesgos de acceso no autorizado, pérdida o daño de información en escritorios y estaciones de trabajo desatendidos por parte de funcionarios, contratistas terceros que prestan sus servicios a la Entidad.

a) Obligaciones

- Los lugares de trabajo de los funcionarios, contratistas y terceros que prestan sus servicios a la Entidad y, cuyas funciones no obliguen a la atención directa de ciudadanos, deben estar en ubicaciones físicas que no queden expuestas al público, para minimizar el riesgo de acceso no autorizado a la información de la Entidad.

- Los dispositivos de almacenamiento masivo, como CD-ROM, DVD o unidades USB con información reservada o pública clasificada, se deben guardar en un lugar seguro bajo llave.

- Los documentos impresos que contienen información reservada o pública clasificada, no se pueden utilizar como papel reciclable, se debe proceder a la destrucción del material.

- No debe permanecer información reservada o pública clasificada a la vista de cualquiera, esta debe permanecer bajo llave en los escritorios de trabajo.

- Las estaciones de trabajo deben apagarse completamente al final de la jornada laboral, se exceptúan los equipos autorizados a utilizar conexión a VPN, estas estaciones de trabajo deberán permanecer encendidas, bloqueadas y con la pantalla apagada.

- Todos los equipos de Tecnologías de la Información, deben tener configurado y operativo un protector de pantalla, además del bloqueo automático, el cual debe activarse cuando el equipo no esté en uso.

b) Restricciones

- No se debe dejar sin bloqueo la sesión de su equipo cuando esté ausente de su puesto de trabajo

- No se debe dejar en el puesto de trabajo documentos con información pública clasificada.

- No se debe dejar al alcance de los visitantes información pública reservada o pública clasificada en especial en áreas de atención al público.

5. Política de Transferencia de Información

Establecer los lineamientos para mantener la seguridad de la información que es transferida por los diferentes sistemas de información dentro y fuera de la Entidad.

a) Obligaciones

- Se deben utilizar los diferentes sistemas de información que brinda la **GTI**, para transferir información corporativa dentro y fuera de la Entidad.

- Los medios asignados para transferir información interna y externa no deben contener información permanente.

- Se debe realizar proceso de depuración y limpieza de los datos almacenados en los diferentes medios de información.

- La Entidad debe contar con un sistema que permita detectar la presencia de códigos maliciosos (virus).

- Se debe tramitar la totalidad de la información asignada en el Gestor Documental de la Entidad, sin omitir, adulterar y/o eliminar ningún tipo de información para beneficio propio o de terceros.

- Toda información transferida por terceros a la Entidad, debe ser escaneada y verificada con el fin de evitar infiltraciones por códigos maliciosos (virus).

- La **GTI** realizara un seguimiento y control a la transferencia de la información que se realicen, desde o hacia su infraestructura de tecnología de información y comunicaciones.

- Las transferencias de información enmarcadas por contratos o acuerdos de intercambio de información, deben contar con acuerdos de confidencialidad y uso de la información.

- Al transferir información reservada o pública clasificada utilizando los servicios de correo electrónico, se deben cifrar los adjuntos que contienen la información y, las claves para el descifrado de la información deben ser comunicadas por un medio diferente al correo electrónico o por un correo diferente al que lleva la información base.

- Los funcionarios, contratistas o terceros que reciban información de INDUMIL, se deben comprometer a proteger dicha información, sin importar su nivel de clasificación para evitar la divulgación no autorizada, aplicando los acuerdos de confidencialidad.

- Se debe identificar la retención de los documentos electrónicos de archivo, de conformidad con lo dispuesto en el instrumento archivístico (Tablas de Retención Documental – TRD) y así, proceder a conformar expedientes que sirvan como repositorio en el Sistema de Gestión de Documentos Electrónicos de Archivo SGDEA.

- Se deben actualizar los expedientes electrónicos (Series Documentales) de conformidad con el instrumento archivístico (Tablas de Retención Documental – TRD).

- Cada área de la Industria Militar en cabeza de su jefe y/o gerente inmediato, deberá actualizar sus expedientes físicos y/o electrónicos de acuerdo a las TRD vigentes.

- Se deben etiquetar las Series documentales de acuerdo al nivel de seguridad (Información pública reservada, Información pública clasificada e Información Pública).

b) Restricciones

- No se permite transferir información de la Industria Militar por sistemas de información que no son corporativos.

- No se permite transferir información de carácter personal sin el cumplimiento de los requisitos de la Ley de Protección de Datos

Personales (Contrato/acuerdo de transferencia de información, autorización del titular).

- No se permite transferir información pública reservada sin la autorización del responsable o dueño de la información del proceso y/o subproceso de la Industria Militar.

- No se permite el almacenamiento permanente de datos, en los sistemas de información que permitan compartir información.

- No se permite el envío de archivos que contengan extensiones como .mp3, wav, .exe, .com, .dll, .bat. o cualquier otro archivo ejecutable; en caso de que sea necesario hacer un envío de este tipo de archivos, deberá ser autorizado por el Gerente de Tecnologías de la Información y/o el Comité Técnico de Seguridad de la información.

- No se permite enviar o recibir cadenas de correo, mensajes con contenido religioso, juegos, político, racista, sexista, pornográfico, publicitario no corporativo, político o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de la Ley, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

- No se permite realizar procesos de reprografía documental (Impresiones, fotocopias, fotografías…) que sean tramitados por medios digitales (Correos electrónicos).

  Nota: Los mismos serán tramitados y observados en su formato original.

6. Política proceso de desarrollo seguro.

Se deberá seguir los siguientes lineamientos, para el desarrollo, mantenimiento y adquisición de software, ya sea propio o de terceros (Proveedores).

a) Obligaciones

- El desarrollo de software debe realizarse cumpliendo el ciclo de vida; desarrollo de pruebas y producción, con ambientes totalmente diferentes y aislados para cada fin.

- El desarrollo de software debe cumplir con directrices de codificación segura, de acuerdo con el lenguaje de programación seleccionado para el mismo.

- Durante la fase de diseño del software o del sistema de información, se deben considerar los requisitos de seguridad de la información.

- El desarrollo de software contratado externamente, debe cumplir con las políticas de desarrollo y seguridad de la Entidad.

- El software que contemple transacciones comerciales electrónicas, debe contemplar controles que eviten pérdida de confidencialidad, disponibilidad e integridad de las mismas.

- Durante la fase de análisis de requerimientos, se deben identificar los riesgos de seguridad de la información del sistema

- El código fuente del sistema debe ser sometido a pruebas de análisis de vulnerabilidad con herramientas de análisis de código.

- Los proyectos de inversión o contratos con terceros que requieran la adquisición de software y hardware, deberán ser notificados a la **GTI** y Dirección de Servicios Generales para agregarlos a los controles y beneficios respectivos.

7. Política relaciones con los proveedores

Toda la información institucional que se genere debido a la relación con los proveedores de bienes y servicios y con los clientes de la Industria Militar, debe contar con un lineamiento para la seguridad de la información de acuerdo a la normativa vigente.

a) Obligaciones

- Con el fin de preservar la seguridad de la información en los contratos de la Industria Militar, se debe incluir y firmar el ACUERDO DE CONFIDENCIALIDAD.

- Los proveedores que deban tener acceso a la información y sistemas de información de la Industria Militar, deben aceptar y cumplir las políticas, directrices, controles de seguridad y privacidad de la información.

- Los proveedores y/o contratistas que presten sus servicios a la Industria Militar deben usar la información y equipos de tecnología, para los propósitos definidos en sus respectivos contratos.

- El proveedor y/o contratista debe suscribir acuerdo de confidencialidad y no divulgación de la información de la Entidad, junto con el personal contratado y quienes intervienen en servicios tercerizado para la Industria Militar.

- Los proveedores deben acatar y cumplir las leyes y acuerdos suscritos por Colombia en materia de protección de información personal, derechos de autor y propiedad intelectual. El supervisor del contrato debe definir mecanismos administrativos para verificar el cumplimiento de estas obligaciones legales.

- Al finalizar los contratos, los proveedores deben efectuar la devolución de la información y/o activos de información propiedad de la Entidad, el supervisor del contrato debe verificar la destrucción o borrado seguro de las copias de la información reservada o publica clasificada que aún este bajo el control del proveedor.

- Cuando se requiera realizar transferencias de información con proveedores, se debe cumplir con la política de transferencia de información establecida en este documento.

- Cuando se requiera desarrollar software con proveedores se debe cumplir con la política de desarrollo seguro.

- Los proveedores deben cumplir con los procedimientos de seguridad y privacidad de la información establecida por **GTI**.

- Los supervisores de los contratos deben mantener un inventario de la información que se suministra a los proveedores, siendo responsables en velar por el estricto cumplimiento de esta política.

- El software y los equipos que utilice el proveedor para el desarrollo de sus actividades, deberán cumplir con los requisitos del sistema de gestión de seguridad y privacidad de la información de la Entidad, incluidos, derechos de autor, controles contra código malicioso, control de acceso y los demás controles acordados con la Entidad.

- El proveedor no está autorizado a conectar, desconectar, retirar o cambiar partes, reubicar equipos de la Entidad o cambiar de configuración a los mismos sin autorización del supervisor del contrato de la Entidad.

- El proveedor no está autorizado a instalar o ejecutar programas que perjudiquen la estabilidad de los equipos, el sistema operativo o sus programas internos o aplicaciones de la Entidad. Esto incluye los programas conocidos como virus informáticos, cualquier tipo de ensayo o experimento, hardware, software o cualquier software considerado como malicioso.

b) Restricciones

- No se otorgará permiso de acceso a información que no es necesaria para el cumplimiento de las obligaciones del proveedor.

- No se otorgará la información a proveedores que no tengan vigente relación contractual y compromiso de confidencialidad.

8. Política de respaldo de información

La información institucional generada en la Industria Militar debe contar con un respaldo por parte de la **GTI**.

a) Obligaciones

- Se debe realizar proceso de respaldo diario y anual incluyendo el respaldo de imágenes.

- La **GTI** debe disponer y controlar la ejecución de las copias a los equipos y la información, así como la prueba periódica de su restauración. Para esto, se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información de la Entidad.

- La **GTI** es responsable del cumplimiento de los lineamientos de respaldo de la Información.

- Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.

- Realizar réplicas de la información del sitio principal al sitio alterno.

- Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos y/o configuraciones Básicas.

- Las copias de respaldo, se deben realizar en horario no hábil, lo cual será verificado a través de procesos automáticos por parte de la **GTI**.

b) Restricciones

- No se permite alojar en servidores información catalogada como personal, música, videos, documentos transitorios, documentos confidenciales, backups de equipos de escritorio, backups de correo electrónico y demás que no sea relevante en el cumplimiento de los objetivos de la Entidad.

9. Política de Trabajo Remoto (Trabajo en Casa)

Esta política define las pautas generales para asegurar la información de la Entidad, frente a riesgos asociados al trabajo en casa. Aplica a todos los funcionarios, que se encuentren autorizados para realizar actividades en casa y tengan acceso a través de VPN (En inglés, virtual private network)

a) Obligaciones

Brindar los servicios de TI necesarios para el buen funcionamiento de las labores del personal de la Industria Militar en casa.

- Contar con software y hardware seguro que permita controlar las infiltraciones de código malicioso o ciber ataque.

- Todo acceso a servicios de TI para trabajo en casa, debe ser autorizado por el responsable del proceso al que pertenece el funcionario que lo solicita, considerando las evaluaciones de riesgos de seguridad de la información y riesgos administrativos.

- Si un funcionario requiere acceso remoto a un equipo que se encuentra en las instalaciones de la Industria Militar, deberá solicitarlo a la Mesa de ayuda y, éste debe ser autorizado por el Comité Técnico de seguridad de la información.

- Para el acceso al trabajo en casa, se deben tener en cuenta las necesidades técnicas y tecnológicas que garanticen que el funcionario cuente con las herramientas necesarias para poder realizar su trabajo, así como las configuraciones de acceso seguro, los medios y horarios que solicite el responsable del proceso, manteniendo en todo momento los principios de eficiencia, eficacia y uso racional de los recursos del Estado.

- Cualquier dispositivo que se emplee para las actividades de trabajo en casa, deberá cumplir con los requisitos y controles de seguridad que defina la **GTI**.

- Los funcionarios que realicen trabajo en casa, son responsables de reportar a la mayor brevedad posible la pérdida o hurto de los equipos y dispositivos móviles de la Entidad usados para este trabajo.

- La estación de trabajo del funcionario que está en casa, debe cumplir con la reglamentación en cuanto al uso de software legal y debe contar con un software de protección contra código malicioso.

- El funcionario que realiza trabajo en casa o trabajo remoto asume los acuerdos de confidencialidad descritos en su contrato.

- Todo responsable de proceso que tenga funcionarios usando los servicios de TI en casa o acceso remoto, debe realizar seguimientos periódicos sobre el cumplimiento de la política de teletrabajo para certificar su cumplimiento.

b) Restricciones

- El acceso a los servicios de trabajo en casa se debe usar únicamente para el cumplimiento de las funciones asignadas y la consecución de la misión y los objetivos de la Industria Militar.

- Está prohibido el almacenamiento de información de la Industria Militar en equipos de cómputo que no son activos de Indumil.

10. Política de protección de dispositivo propio (BYOD)

Esta política define los lineamientos a seguir con los dispositivos electrónicos personales (Teléfonos inteligentes, tabletas, computadores y portátiles), de un funcionario y/o proveedor de la Industria Militar, y en los cuales se encuentre almacenada información pública privada o reservada de la Entidad, pudiendo comprometer la integridad, disponibilidad y confidencialidad de esta. A estos dispositivos se les conoce como BYOD (*Bring Your Own Device*).

a) Obligaciones

- Los responsables de los procesos y subprocesos deben determinar bajo qué circunstancias se autorizará el uso de dispositivos que no pertenecen a la Entidad (BYOD) para almacenar o procesar información pública reservada o pública clasificada.

- El funcionario o proveedor al que se autorice un BYOD, debe garantizar bajo compromiso de confidencialidad que la información pública reservada o información pública clasificada, correspondiente a las labores asignadas y, será almacenada de forma aislada a la información personal que guarde en su dispositivo.

- Todo dispositivo BYOD autorizado para almacenar información de la Entidad, debe cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.

- El propietario del dispositivo BYOD debe aplicar todas las medidas de seguridad que estén a su alcance para mantener la integridad, confidencialidad y disponibilidad de la información que se encuentre en su dispositivo personal.

- En caso de hurto el funcionario informara inmediatamente al Gerente de Tecnologías de la Información o cualquier medio de comunicación de la mesa de Ayuda (Ext 1702, soporte@Indumil.gov.co, Mesa de ayuda)

11. Política de derechos de Autor

Esta política define los lineamientos que debe seguir la Industria Militar para la aplicación de derechos de autor, esto con el fin de mantener un equilibrio apropiado entre los intereses de los titulares del derecho y los usuarios de contenidos protegidos, así como las leyes sobre derecho de autor que permiten ciertas limitaciones respecto de los derechos patrimoniales, y en los casos en los que las obras protegidas pueden ser utilizadas sin autorización del titular de los derechos y contra el pago o no de una remuneración.

a) Obligaciones

- Todo ordenador o dispositivo móvil debe tener software (programa de ordenador) con licencia de uso, que la Entidad ha adquirido con el fin de lograr un resultado específico. En caso de requerir ajustes en un software para adaptarlo a las necesidades de la Entidad, se deberá contar primero con la autorización y viabilidad del fabricante.

- El software sin costo (Free, libre, open source etc…**)** debe ser verificado por el gestor del software y, de ser autorizado se debe solicitar su descarga e instalación por medio de la Mesa de Ayuda- Software – Instalación y configuración.

- El representante legal de la Industria Militar en sus informes de gestión, dará a conocer el estado de cumplimiento de las normas sobre propiedad intelectual y derechos de autor por parte de la Entidad.

- Toda información y/o software desarrollado por la Industria Militar, se identificará como un activo que se debe proteger de los riesgos que atentan contra su confidencialidad, integridad y disponibilidad. El incumplimiento a este deber de confidencialidad, le acarreará al empleado y/o contratista infractor la correspondiente responsabilidad por todos los perjuicios tanto patrimoniales como extra patrimoniales que presente la Entidad.

- En relación a la Página Web y la Intranet, todos los derechos de los contenidos y las fotografías publicadas a la página web www.indumil.gov.co

e Intranet intranet.indumil.gov.co son propiedad de la Entidad o están autorizados por sus autores o referenciadas las fuentes de las cuales se extrajeron. Su uso y/o publicación está autorizado, con la consecuente incorporación de la fuente y enlace a la página principal.

b) Restricciones

- Se prohíbe la copia de archivos, software informático y otro contenido perteneciente a la Industria Militar sin previa autorización de los Jefes de Área, o facilitar su copia, su distribución o permitir descargas de contenido a terceros.

12. Política de Protección de datos personales

Bajo el precepto legal de la Ley Estatutaria No. 1581 de 2012, reglamentada parcialmente por los Decretos 1377 de 2013, 1081 de 2015 y 255 de 2022, se dictaron disposiciones generales para la protección de datos personales en Colombia.

Ahora bien, en cumplimiento a dicha normativa, y en desarrollo del derecho constitucional de todas las personas a conocer, actualizar y rectificar de forma gratuita la información que se recaude sobre ellas en bases de datos o archivos, los derechos, libertades y garantías a los que se refieren el artículo 15 y 20 de la Constitución Política, la Industria Militar deberá informar que los datos personales serán utilizados para:

- Hacerle saber sobre las condiciones y características de nuestros requerimientos, productos, servicios y eventos atinentes a la razón social.
- Para efectos de obligaciones contractuales.
- Evaluación de nuestros servicios.
- Proveer acceso a los productos y servicios ofertados.
- Realizar internamente estudios de mercado.
- Efectos publicitarios y comerciales de los que participa o responde INDUMIL.

Los datos personales que se someten a tratamiento, son: Nombre y apellidos, documento de identidad, región, número de teléfono fijo, número de teléfono móvil, dirección de su Entidad o empresa, dirección de correo electrónico, profesión y ocupación.

a) Obligaciones

- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, utilizando los canales dispuestos por la Industria Militar (Pagina web, buzón de correo electrónico, formularios electrónicos y demás que estén a disposición de la ciudadanía y demás partes interesadas.

- Solicitar y conservar, copia de la respectiva autorización otorgada por el titular.

- Informar al titular sobre la finalidad de la recolección de los datos y los derechos que adquiere al dar la autorización.

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Garantizar que la información sea veraz, completa, exacta, actualizada y comprobable.

- Actualizar la información respecto de los datos del titular. Adicionalmente, se deberán implementar todas las medidas necesarias para que la información se mantenga actualizada.

- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al titular.

- Respetar las condiciones de seguridad y privacidad de la información del titular.

- Atender de manera eficaz y oportuna las Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD) interpuestos por los Ciudadanos y demás partes interesadas, de conformidad con lo dispuesto en los términos dispuestos por la Ley.

- Identificar la información que está en poder de la Entidad, y que se encuentra en discusión por parte del titular.

- Informar a la autoridad (Superintendencia de Industria y Comercio) de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

- Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio.

- Usar únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la Ley 1581 de 2012 y demás disposiciones sobre la materia.

b) Medio y manifestación para otorgar la autorización del titular:

La Industria Militar en los términos dispuestos en la Ley, ha preparado un aviso en el cual se comunica a los titulares que pueden ejercer su derecho al tratamiento de los datos personales a través de la página www.indumil.gov.co, correo electrónico indumil@indumil.gov.co las solicitudes serán registradas en el Sistema de Gestión Documental.

c) Eventos en los cuales no es necesaria la autorización del titular de los datos personales:

De conformidad con el artículo 10 de la Ley 1581 de 2012, la autorización del titular no será necesaria cuando se trate de las siguientes solicitudes:

- Información requerida por una Entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

d) Personas a quienes se les puede suministrar la información:

De conformidad con el artículo 13 de la Ley 1581 de 2012, las personas a quienes se les puede suministrar la información son:

- A los titulares, sus causahabientes (cuando aquellos falten) o sus representantes legales.
- A las Entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- A los terceros autorizados por el titular o por la Ley.

e) Responsable en el procedimiento para la atención de consultas, peticiones, quejas, reclamos, sugerencias y denuncias relacionadas con la protección de datos personales.

Con el objeto de atender las consultas, peticiones, quejas, reclamos, sugerencias y denuncias relacionadas con la protección de datos personales, la Industria Militar designará a un funcionario quien será el responsable de recibir y dar trámite a las solicitudes remitidas, en los términos, plazos y condiciones establecidos en la Ley 1581 de 2012 y en la presente política.

f) Procedimiento para la atención de consultas, peticiones, quejas, reclamos, sugerencias y denuncias relacionadas con la protección de datos personales.

Requisitos mínimos:

Las consultas dirigidas a la Industria Militar deberán contener como mínimo la siguiente información:

a. Nombres y apellidos del Titular y/o su representante y/o causahabientes.
b. Lo que se pretende consultar.
c. Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes.
d. Firma, número de identificación o procedimiento de validación correspondiente.
e. Haber sido presentada a través del correo indumil@indumil.gov.co o por los medios de consulta que habilite la Industria Militar.

Plazo de respuesta:

La solicitud de información será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la misma dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

g) Petición de actualización, rectificación y supresión de datos

La Industria Militar rectificará y actualizará, a solicitud del titular, la información de éste que resulte ser incompleta o inexacta, de conformidad con el procedimiento y los términos antes señalados, para lo cual el titular allegará la solicitud al correo electrónico indumil@indumil.gov.co indicando la actualización, rectificación y supresión de la información y, aportará la documentación que soporte su petición.

h) Revocatoria de la autorización y/o supresión del dato

Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual, para ello la Industria Militar pondrá a disposición del titular el correo electrónico indumil@indumil.gov.co. Si vencido el término legal respectivo, la Industria Militar no hubiera eliminado los datos personales, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio, que se ordene a la Entidad la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012.

i) Atención Prioritaria de peticiones.

Si la Petición es realizada por un periodista, para el ejercicio de su actividad, esta se tramitará de manera preferencial.

Los niños, niñas, adolescentes, adultos mayores y personas en situación de discapacidad y sin importar su identidad de género, podrán presentar directamente solicitudes, quejas, reclamos sugerencias en interés propio, las cuales tendrán prelación en el turno sobre cualquier otra.

j. Petición de información y documentos reservados.

Solo tendrán el carácter de reservado la información y documentos expresamente sometidos a reserva por mandato de la Constitución, y la Ley en especial los siguientes:

a. Los relacionados con la defensa o seguridad nacional.
b. Las instrucciones en materia diplomática o sobre negociaciones reservadas.
c. Los que involucren derechos a la privacidad e intimidad de las personas, incluidas en las historias laborales, así como las historias clínicas.
d. Los relativos a las condiciones financieras de las operaciones de crédito público y tesorería que realice la Nación, así como los estudios técnicos de valoración de activos de la Nación.
e. Los amparados por el secreto profesional.
f. Los protegidos por el secreto comercial e industrial.

En el evento de generarse modificaciones a las políticas anteriormente establecidas, la **GTI** deberá informar y justificar al **COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO** de la Industria Militar, quien en sesión analizará y determinará la procedencia o no de las mismas.

General (RA) RICARDO GÓMEZ NIETO
Presidente Industria Militar

REVISÓ	APROBÓ
Patricia Rodriguez Díaz Jefe Oficina Legal	**CN (R.A.) Jorge Alberto Arocha Muñoz** Gerente de Tecnologías de la información
Victor Manuel Moreno Ramírez Jefe de Grupo Oficina Legal	**Ronald Jamilton Moreno Samaniego** Jefe Oficina de Planeación
Sergio Alberto Villada Agudelo Director de Riesgos y Transformación	

Elaborado por:
Luisa Fernanda Pulido Paez
Profesional GTI

POLÍTICA DE SEGURIDAD DIGITAL

Control de Cambio
1. Cambio Nombre de la Política antes (Políticas Generales de Seguridad y Privacidad de la Información) ahora (Política de Seguridad Digital) siguiendo los lineamientos de Seguridad Digital. 2. Se anexa implementación de Gobierno Digital con modelo de seguridad y privacidad de información. 3.(Política de Controles Criptográficos) Primer párrafo se elimina sistemas de información. 4. (Política de transferencia de Información), b Restricciones= se modifica **reservada** **5.** (Política de respaldo de Información), a Obligaciones= se quita semanal, se modifica el quinto párrafo. 6. (Política Trabajo Remoto) Se complementa primer párrafo 7. Se anexa política de derechos de Autor. 8. Se anexa Política de Protección de datos personales.