COMUNICADO

NORMAS DE SEGURIDAD DE LA INFORMACIÓN

“Año de la Responsabilidad Social y la Transformación Empresarial”

NORMAS DE SEGURIDAD DE LA INFORMACIÓN

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, con el apoyo del PROCESO GESTIÓN DE SERVICIOS DE TIC "IM OC GTI PS 001" establece la POLÍTICA DE SEGURIDAD DIGITAL "IM OCGTI CP003 ver 10", acorde con la normatividad vigente, los requisitos de los grupos de valor, partes interesadas, se compromete con el mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (ISO 27001:2013), medio por el cual busca 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, en concordancia con la misión y la visión de la entidad, y con 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, orientando su gestión a preservar la confidencialidad, integridad y disponibilidad de la información.

En la DECLARACIÓN DE APLICABILIDAD (SOA) DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN "IM OC OFI CP 001", se establecen todos los controles existentes definidos en el Sistema de Gestión de Seguridad de la Información (SGSI), además, se establece la metodología para realizar el análisis de riesgos, y los controles y objetivos de control que han sido seleccionados con base en el análisis y evaluación de riesgos, en los requerimientos de seguridad identificados y por ende en las definiciones dadas en el plan de tratamiento del riesgo. Estos controles están basados en los controles definidos en la norma ISO/IEC 27001:2013 Anexo A.

El Sistema de Gestión de Seguridad de la Información aplica a los servicios de procesamiento electrónico de datos de la Industria Militar, soportados en sus activos de información e infraestructura tecnológica, ubicadas físicamente en Oficinas Centrales, FAGECOR, FEXAR y FASAB. (Certificación ICONTEC N° SI-CER180683). Este sistema cubre los procesos de la Empresa incluidos en el mapa de macro procesos de INDUMIL, particularmente en los aspectos en los que sean dependientes del PROCESO GESTIÓN DE SERVICIOS DE TIC "IM OC GTI PS 001".

La POLÍTICA DE SEGURIDAD DIGITAL "IM OCGTI CP003 ver 10" embebe las siguientes políticas:

1. **Política Dispositivos Móviles**

   Lineamientos para el uso de dispositivos móviles como: equipos portátiles, teléfonos móviles, tabletas, entre otros. la Oficina de Informática implementa 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.

2. **Política Control de Acceso**

   Directrices para evitar el acceso no autorizado a los sistemas y/o servicios de TI, estableciendo lineamientos y controles de acceso a personas no autorizadas a los recursos tecnológicos asociados al proceso GESTIÓN INFORMÁTICA

3. Política Controles Criptográficos

Parámetros sobre uso de técnicas y herramientas de cifrado administrados por el Proceso Gestión Informática de Indumil donde se identifica la información que requiera ser protegida con controles criptográficos encaminados a proteger la confidencialidad, integridad y disponibilidad de la información

4. Política Escritorio y pantalla limpia

Lineamientos aplicables con el objetivo es reducir los riesgos de acceso no autorizado, pérdida o daño de información en escritorios y estaciones de trabajo desatendidos.

5. Política Transferencia de Información

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

6. Política Proceso de Desarrollo Seguro.

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

7. Política Relaciones con los proveedores

Establecer los lineamientos para la seguridad de la información en la relación con proveedores, cumpliendo los requisitos del negocio, cliente y ley.

Aplica a toda la información institucional compartida en la relación con proveedores de bienes y servicios de la Industria Militar

8. Política de respaldo de información

Establece los lineamientos para el respaldo de la información.

9. Política Trabajo Remoto (Trabajo en Casa)

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

10. Política de protección de dispositivo propio (BYOD)

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*).

11. Política de derechos de Autor

Define los lineamientos que debe seguir la Industria Militar para la aplicación de derechos de autor, este con el fin de mantener un equilibrio apropiado entre los intereses de los titulares del derecho y los usuarios de contenidos protegidos, así como con 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.

12. Política de Protección de datos personales

Establece los lineamientos aplicables, con el propósito de darle cumplimiento a lo estipulado en el artículo 10 del Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2012, y demás normas que lo adicionen o modifiquen relativas a la protección de datos personales, expedidas 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, y los derechos, libertades y garantías a los que se refieren el artículo 15 y 20 de la Constitución Política.