POLÍTICA DE SEGURIDAD DIGITAL

ARTICS S.A.S, es una sociedad de economía mixta, empresa filial del orden departamental, vinculada a la Gobernación del Valle del Cauca, organizada bajo el tipo de las sociedades por acciones simplificadas S.A.S., compuesta por aportes estatales de más del cincuenta (50%) por ciento de participación público y por capital privado, proveedor de redes y servicios de telecomunicaciones, regida principalmente por la ley 1258 de 2008, la ley 1341 de 2009, la ley 594 del 2000 y demás normas concordantes que reglamente, modifiquen, o sustituyan la materia.

ARTICS S.A.S., de conformidad con la naturaleza jurídica que le atañe, y como entidad operadora y proveedora de soluciones de archivo y de tecnologías de la información, procede a realizar la definición de protocolo de seguridad de la información para proteger los sistemas de información, estableciendo los procedimientos para proteger su infraestructura computacional y de conectividad, garantizando la integridad, confidencialidad y autenticidad de la información.

1. DEFINICIONES

- **Hardware:** Es un Software, generalmente no deseado, que facilita el envió de contenido publicitario a un equipó.
- **Alerta:** Notificación automática de un suceso o error.
- **Arquitectura de seguridad:** Conjunto de principios que describe los servicios de seguridad que deba proporcionar un sistema para ajustarse a las necesidades de sus usuarios, los elementos del sistema necesarios para implementar tales servicios y los niveles de rendimientos que se necesitan en los elementos para hacer frente a las posibles amenazas.
- **Crimeware:** Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidos del software.
- **Suite de seguridad:** es la suma de varios programas de seguridad: Antivirus, Antispyware, Firewall o cortafuegos, Antirootkit, Control Parental, Antiphishing, Filtro Web, Antispam, Copia de seguridad, Disco de Arranque.
- **Rootkit:** es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.
- **Phishing:** El termino Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

- **Keystroke Logger o programa de captura de teclado (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.

2. MARCO NORMATIVO

- **Documento CONPES 3995:** Política Nacional de Confianza y Seguridad Digital.
- **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 489 de 1998:** Por la cual regula el ejercicio de la función administrativa, determina la estructura y define los principios y reglas básicas de la organización y funcionamiento de la Administración Pública. Capitulo XIII Capítulos 85 al 94 Empresas Industriales y Comerciales del Estado y se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.
- **Ley 1712 de 2014**: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1437 de 2011:** Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Decreto 1083 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
- **Decreto 1893 de 2020** Por medio del cual se actualiza el Modelo para el orden nacional y se hizo extensiva su implementación diferencial a las entidades territoriales del Modelo Integrado de Planeación y Gestión MIPG.

3. PRINCIPIOS DE LA POLÍTICA

A continuación, presentamos los principios que rigen la presente política de seguridad digital:

- **Integridad:** Mantener la integridad de los datos significa asegurarse de que los datos permanezcan intactos y sin cambios a lo largo de todo su ciclo de vida. Para que la integridad de los datos se mantenga, es necesario que no haya habido cambios o alteraciones en los datos. Para cumplir con este principio **ARTICS S.A.S,** asume el compromiso de emprender todas las acciones que se requieran para conservar integra la información que maneja.

- **Confidencialidad:** La confidencialidad se entiende en el ámbito de la seguridad informática, como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros.
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

4. ESTRATEGIAS

Las estrategias definidas para la implementación de la política son las siguientes:

- Identificar, gestionar, tratar y mitigar los riesgos de seguridad digital de la empresa
- Desarrollar el modelo de seguridad y privacidad de la información
- Promover en los colaboradores de la entidad el uso y comportamiento responsable en el entorno digital.

5. LÍNEAS DE ACCIÓN

5.1. Seguridad específica para cada equipo propiedad de la entidad que incluye:

- Suite de seguridad informática (Antivirus, administrar firewall)
- Software licenciado y actualizado
- Culturización de usuarios

5.2. Seguridad general

- Implementar una VPN segura para blindar las comunicaciones internas.

6. INDICADORES

- Herramientas ofimáticas de la entidad licenciados
- Documentos de protocolos aprobados y socializados
- Riesgos de seguridad digital identificados

7. GESTIÓN DE ACTIVOS:

- Usar el repositorio institucional asignado por **ARTICS S.A.S** para guardar la información, en caso de almacenarla en los discos locales del equipo asignado, se debe utilizar la partición protegida y descargar la información en los repositorios institucionales posteriormente, para prevenir qué ante una situación de hurto del equipo de cómputo, se pierda y exponga la información de la institución.
- La conexión de medios extraíbles al equipo como (USB, Unidades CD/DVD, Discos externos, entre otros, son monitoreadas y eventualmente podrá ser restringida de acuerdo con los

lineamientos que **ARTICS S.A.S** disponga para evitar la fuga de información y garantizar la confidencialidad y protección de los datos.

- En los equipos de cómputo no se permite el almacenamiento de archivos de música, videos y cualquier otro formato o información de carácter personal, salvo aquellos cuyo uso o almacenamiento sea para ejecutar labores propias de **ARTICS S.A.S**
- El personal de **ARTICS S.A.S** son responsable por los daños ocasionados a los equipos de cómputo generados por mal uso de estos, por lo tanto, se tienen en cuenta las siguientes recomendaciones:
    - Evitar exponer el equipo de cómputo en sitios públicos como centros comerciales o campos abiertos.
    - Hacer uso del equipo de cómputo asignado únicamente en el lugar de trabajo aprobado por **ARTICS S.A.S**
    - Evitar exponer el equipo de cómputo en zonas donde exista humedad.
    - Evitar golpes y consumir líquidos mientras se desarrollan actividades propias del cargo ya que existe el riesgo de avería parcial o total del equipo de cómputo.
    - Evitar utilizar o dejar el equipo de cómputo donde pueda sufrir calentamiento, esto generaría daño en la fuente y a nivel general.
    - No está autorizado ningún tipo de medicación en el hardware.
    - Las personas en el momento de desvinculación o cambio de labores deben realizar la entrega de su puesto al jefe inmediato o a quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

8. MENSAJERÍA ELECTRÓNICA

- Los colaboradores de **ARTICS S.A.S** deben conocer que la cuenta de correo electrónico asignada es de carácter individual; y no se debe utilizar una cuenta de correo que no sea la propia, a menos que se autorice la administración de varias cuentas.
- Los colaboradores deben utilizar el correo electrónico para envío de mensajes e información relacionada con el desarrollo de las labores y funciones asignadas a cada usuario.
- Las cuentas de usuario de correo son generadas bajo el estándar estipulado en la creación de cuentas de **ARTICS S.A.S** en caso de que un usuario deba realizar un cambio de cargo se conserva la misma cuenta de correo, se parte del principio que el correo es un medio de comunicación mas no de almacenamiento de información.
- Cada cuenta de correo electrónico tiene asociado un conjunto de recursos de almacenamiento que es limitado de conformidad con lo establecido con el software contratado.

- El servicio de correo administrativo permite la transferencia de archivos como adjuntos del mensaje o compartidos a través de sus herramientas.
- Las imágenes enviadas en el cuerpo del mensaje electrónico no son mayores a 10 Megabytes, un mayor peso de la imagen genera lentitud en la distribución y saturación del correo.

9. LÍNEA TELEFÓNICA

Evitar el intercambio de información en la comunicación telefónica con personas ajenas a **ARTICS S.A.S**, puesto que esta herramienta facilita la aplicación de técnicas de ingeniería social para obtener información sensible de la Organización.

En constancia de lo anterior