1. POLÍTICA

IMPRETICS E.I.C.E. como entidad operadora y proveedora de soluciones integrales de logística, comunicaciones, informática y material gráfico para el sector público y privado, definirá y aplicará los protocolos de seguridad informática para proteger los sistemas de información, es decir, establecer los procedimientos para proteger la infraestructura computacional de la Entidad garantizando la integridad, confidencialidad y autenticidad de la información, así como una evaluación permanente del costo-beneficio y el nivel de satisfacción de las necesidades que ofrezcan los diferentes proveedores de servicios de ciberseguridad.

2. DEFINICIONES

- **Adware:** Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.
- **Alerta:** notificación automática de un suceso o error.
- **Arquitectura de seguridad**: Conjunto de principios que describe los servicios de seguridad que debe proporcionar un sistema a para ajustarse a las necesidades de sus usuarios, los
- elementos de sistema necesarios para implementar tales servicios y los niveles de rendimiento 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 distribuidor 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.

3. MARCO NORMATIVO

- **Documento CONPES 3854:** Política Nacional de 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 1499 de 2017:** 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.

4. PRINCIPIOS DE LA POLÍTICA

Con el propósito de generar unas buenas prácticas en torno al Código de Seguridad Digital se trabajará bajo los siguientes principios:

- **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 IMPRETICS E.I.C.E. 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. Mediante
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

5. 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 entidad.
- Desarrollar el modelo de seguridad y privacidad de la información
- Promover en los servidores de la entidad el uso y comportamiento responsable en el entorno digital.

6. LÍNEAS DE ACCIÓN

Se realizarán dos grandes líneas que contemplan:

- **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.
- **Seguridad General**
  - Implementar una VPN segura para blindar las comunicaciones internas.

7. METAS

- Licenciamiento de las herramientas ofimáticas de la entidad.
- Equipos actualizados y con antivirus.
- Adecuación de la red que permita la correcta administración de la información.
- Adecuación de VPN
- Protocolos de ciberseguridad documentados y socializados

8. INDICADORES

- Herramientas ofimáticas de la entidad licenciadas.
- Capacitación a usuarios de la entidad en temas de seguridad digital.
- Documentos de protocolos aprobados y socializados
- Riesgos de seguridad digital identificados

9. TABLA DE CONTROL DE MODIFICACIONES

Cuando un documento cambie de versión debe ser identificado con un sello de documento obsoleto.

REV.	APARTADO MODIFICADO	DESCRIPCIÓN	FECHA
001	Todas las páginas	Creación del Documento	Nov 2019

002	Todas las paginas	- Actualización de imagen. - Adición tabla de control de modificaciones.	Ene 2021

10. APROBACIÓN

Acción	Nombre	Cargo	Firma
Elaboró	Armando Rodríguez Cuellar	Asesor MIPG	
Revisó	Fernando Céspedes Martínez	Gerente General	
Aprobó	Comité Institucional de Gestión y Desempeño		