1. OBJETIVO

Establecer las actividades que se deben realizar para mantener la seguridad de la información en las redes de RED VITAL PAIPA S.A. E.S.P., así como asegurar que ésta sea transferida desde la empresa hacia entidades o personas externas de manera segura.

2. ALCANCE

El procedimiento aplica a la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P. incluyendo su monitoreo con el uso de internet, servidores y equipos de red.

3. RESPONSABLES

Profesional Gobierno Digital / Técnico Administrativo Gobierno Digital	• Garantizar que los sistemas de comunicación sean seguros y estén protegidos contra amenazas cibernéticas y otros riesgos. • Mantenerse actualizado sobre las últimas tecnologías de seguridad de comunicaciones y evaluar su idoneidad para la organización. Esto puede incluir la adopción de soluciones de seguridad avanzadas, como sistemas de prevención de intrusiones o detección de amenazas avanzadas. • Capacitar a los usuarios y al personal de la organización en prácticas de seguridad de comunicaciones. Ayudar a crear una cultura de seguridad donde todos comprendan la importancia de proteger la información y sigan buenas prácticas de seguridad.
Jefe Oficina Control Interno / Profesional del Sistema Integrado de Gestión	• Supervisar la investigación del origen del virus y determinar si hubo fallas en los controles de seguridad previos, identificando posibles brechas de seguridad y su causa raíz. • Generar un informe detallado para la Gerencia sobre el incidente, los controles implementados, los riesgos identificados y las medidas adoptadas para prevenir incidentes similares en el futuro. • Proponer mejoras en los controles de seguridad de la información, como actualizaciones de antivirus, políticas de acceso, capacitaciones en seguridad informática y auditorías periódicas de seguridad, para fortalecer la protección de los sistemas.

4. DEFINICIONES / TERMINOLOGÍA

Antivirus	Software utilizado para evitar, analizar, detectar y eliminar virus de los dispositivos.
Base de datos	Un conjunto organizado de datos almacenados electrónicamente que se pueden buscar, recuperar y manipular fácilmente.
Ciberseguridad	Prácticas y medidas para proteger sistemas, redes y datos contra amenazas cibernéticas.
LAN	Son un conjunto de dispositivos conectados entre sí que comparte comunicación o enlaces con un servidor.
Red de Computadoras	Infraestructura que permite la comunicación y el intercambio de datos entre dispositivos informático.
Seguridad de la información	Medidas y prácticas para proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas.

Virus informático	Un programa o código malicioso que se propaga y daña los sistemas y archivos de una computadora.

5. POLÍTICAS DE OPERACIÓN

Política de Acceso y Control de Usuarios:

- Define quién tiene acceso a los sistemas y datos de comunicación.
- Establece procedimientos para la gestión de contraseñas y autenticación.
- Especifica niveles de acceso y privilegios para diferentes roles de usuario.

Política de Uso Aceptable:

- Establece reglas y restricciones sobre el uso de los recursos de comunicación de la organización.
- Define lo que se considera uso inapropiado, como la navegación en sitios web no relacionados con el trabajo o el envío de correos electrónicos no autorizados.

Política de Monitoreo y Registro:

- Describe los procedimientos para supervisar y registrar las actividades de red y comunicación.
- Define cuánto tiempo se deben mantener los registros y quién tiene acceso a ellos.

Política de Seguridad de la Red:

- Establece directrices para la configuración segura de la infraestructura de red, incluidos firewalls, enrutadores y conmutadores.
- Define reglas de segmentación de red para proteger la información crítica.

Política de Cifrado de Datos:

- Requiere el cifrado de datos confidenciales durante la transmisión y el almacenamiento.
- Define los algoritmos de cifrado y las prácticas de gestión de claves.

Política de Gestión de Vulnerabilidades:

- Describe el proceso para identificar, evaluar y remediar vulnerabilidades en los sistemas de comunicación.
- Establece plazos para la aplicación de parches y actualizaciones de seguridad.

6. DESARROLLO DEL PROCEDIMIENTO

No	ACTIVIDAD (QUE)	DESCRIPCIÓN (COMO)	RESPONSABLE (QUIEN)	REGISTRO / DOCUMENTO
1	Topología de Red	Deberá existir documentación magnética e impresa sobre la tipología de red y diagramas topológicos de la ubicación de los puntos de red. Se creará una base de datos con los distintos usuarios y contraseñas de los dispositivos de red (Router, Switch, servidores, etc.)	Profesional Gobierno Digital Técnico Administrativo Gobierno Digital	Registro de Custodia
2	Conexiones	La conexión a internet será suministrada únicamente para temas relacionados con el buen desarrollo de las actividades de los funcionarios y/o contratistas según el manual de funciones o contrato.	Profesional Gobierno Digital Técnico Administrativo Gobierno Digital	PA-GCOM-FO-01 Oficios / Comunicaciones

		Por ningún motivo se permitirán conexiones a internet inalámbrico a terceros a menos que este en el marco de una actividad institucional o sea autorizado por el Gerente General mediante solicitud escrita. Los funcionarios de la Entidad no podrán acceder a configuraciones del equipo de cómputo impresoras u otros dispositivos.		
3	Antivirus	Se deberá adquirir un software antivirus que se ajuste a las necesidades de seguridad de la Entidad bajo los lineamientos legales y licenciamiento. Se realizarán análisis trimestral con el software antivirus instalado en los equipos de cómputo de propiedad de la Entidad. Se informará al Jefe Oficina Control Interno y al Profesional del Sistema Integrado de Gestión acerca de la incidencia de virus en los equipos asignados a los funcionarios de la Entidad, con el fin de implementar medidas que eviten la incidencia de esta falla.	Profesional Gobierno Digital Técnico Administrativo Gobierno Digital	PA-GCOM-FO-01 Oficios / Comunicaciones

PUNTO DE CONTROL

1. Topología de Red. Documentación para determinar los puntos de red para los funcionarios y/o contratistas de la Entidad.

7. DOCUMENTOS DE REFERENCIA

Ley 1273 de 2009. Protección de la información y de los datos
Ley 1341 de 2009. Tecnologías de la Información y las Comunicaciones
Ley 1581 de 2012. Protección de datos personales
Decreto 1078 de 2015. Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones
Decreto 1008 de 2018. Lineamientos generales de la Política de Gobierno Digital
Plan de Seguridad y Privacidad de la Información de la Entidad, versión vigente
Lineamientos internos para administración de redes y comunicaciones de la Entidad, versión vigente
NTC-ISO 9001:2015. Sistema de gestión de la calidad – Requisitos

Capítulo 7.1.3. Infraestructura
Capítulo 7.1.5. Recursos de seguimiento y medición (opcional si lo quieres mantener por monitoreo)
Capítulo 8.5.1. Control de la producción y de la provisión del servicio
Capítulo 7.5. Información documentada

8. ANEXOS

PA-GCOM-PL-01 Plan de Seguridad y Privacidad de la Información
PA-GCOM-FO-01 Oficios / Comunicaciones
Registro de Custodia

ELABORÓ	NATURALEZA DEL CAMBIO	VERSIÓN	FECHA DE APROBACIÓN
Deysi Carolina Rodríguez Molano	Procedimiento inicial	01	14/03/2023
Andrew Masami Asakura Garcia	Cambio de logo, actualización de contenido y responsables de elaboración, revisión y aprobación	02	10/01/2024
Andrew Masami Asakura Garcia	Inclusión del Logo ICONTEC / MIPG y ajuste de Pie de Página / Ajuste de contenido	03	26/08/2024
Andrew Masami Asakura Garcia	Actualización del Correo Corporativo	04	01/04/2025

ELABORÓ	REVISÓ	APROBÓ
Nombre: Andrew Masami Asakura Garcia	Nombre: Julián Alfonso Amaya Reyes	Nombre: Yeison Rokney Torres Suarez
Cargo: Profesional SIG	Cargo: Técnico Administrativo Gobierno Digital	Cargo: Gerente General
Firma:	Firma:	Firma:

Km 1 Vía Francisco Montaña / Código Postal 150444
Números de Contacto: +(57) 320 8587785 – 320 8585284
Correo electrónico: redvital@paipa-boyaca.gov.co / sistemas@redvitalpaipa.com
Página Web: www.redvitalpaipasaesp.com