1. OBJETIVO

Establecer actividades para el control de acceso seguro a los equipos y redes, así como para prevenir el acceso a la información no autorizada, el daño a los equipos o de la información.

2. ALCANCE

Inicia con la actividad de ingreso del personal, a la sede de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P., y termina con el control del acceso a los equipos y redes de la entidad.

3. RESPONSABLES

Profesional Gobierno Digital / Técnico Administrativo Gobierno Digital	• Trabaja en colaboración con otros departamentos y partes interesadas para desarrollar políticas de seguridad lógica que establezcan las directrices y normas de seguridad para la organización. • Identifica y evalúa los riesgos de seguridad lógica que enfrenta la organización. Esto implica analizar amenazas potenciales, vulnerabilidades y las posibles consecuencias de los incidentes de seguridad. • Capacita al personal de la organización en prácticas de seguridad lógica, conciencia de seguridad y el cumplimiento de políticas de seguridad.
Líderes de Procesos	• Verificar que las medidas de protección (como contraseñas seguras, actualizaciones de software y restricciones de acceso) se implementen correctamente dentro de su proceso. • Informar inmediatamente al Departamento de Sistemas o al equipo responsable de seguridad informática sobre cualquier incidente o amenaza de seguridad lógica, como accesos sospechosos, intentos de intrusión o pérdida de datos.

4. DEFINICIONES / TERMINOLOGÍA

Seguridad lógica	Medidas establecidas por la administración de usuarios y administradores de recursos de tecnología de información para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando los recursos tecnológicos y medios de Información.
Inventario tecnológico	Se refiere al inventario de dispositivos electrónicos que hacen parte de los activos de la entidad.
Acceso a la información	Conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema de bases de datos, bibliotecas, archivos e Internet.

5. POLÍTICAS DE OPERACIÓN

Controles de acceso. Los controles de acceso pueden implementarse en el sistema operativo, en la información, en las bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. Suele ser la primera línea de defensa para la mayoría de los sistemas informatizados, siendo su finalidad impedir que personas no autorizadas accedan a los mismos. Son la base de casi todos los controles ulteriores, ya que también permite efectuar un seguimiento de las actividades de cada uno de los usuarios.

Roles. En este caso, los derechos de acceso se agrupan de acuerdo a un rol determinando. En correspondencia el uso de los recursos se restringe a las personas autorizadas a asumir dicho rol. El uso de roles es una forma bastante efectiva de implementar el control de accesos, siempre y cuando el proceso de definición de roles esté basado en un riguroso análisis previo de la forma de actuar de la organización.

Política de contraseñas segura. Una contraseña débil puede llevar al traste toda tu estrategia de defensa. Crea una norma que introduzca la complejidad suficiente para que sean robustas. Tampoco te pases en esa complejidad, si no, acabarán por escribirla en post-it con lo que no habremos ganado nada.

Cargos con Correos Corporativos con Acceso a Información

CARGO ACTUAL	CORREO ELECTRÓNICO
GERENTE GENERAL	gerencia@redvitalpaipa.com
SUBGERENTE GENERAL ADMINISTRATIVO	subadministrativo@redvitalpaipa.com
SUBGERENTE GENERAL OPERATIVO	suboperativo@redvitalpaipa.com
JEFE OFICINA ASESORA JURÍDICA	juridico@redvitalpaipa.com
JEFE OFICINA CONTROL INTERNO	controlinterno@redvitalpaipa.com
COORDINADOR DE PLANEACIÓN Y PROYECTOS	planeación@redvitalpaipa.com
COORDINADOR DE SISTEMA INTEGRADO DE GESTIÓN	sig@redvitalpaipa.com
COORDINADOR DE ACUEDUCTO Y ALCANTARILLAD	redes@redvitalpaipa.com
COORDINADORA AMBIENTAL (JEFE DE PLANTAS)	plantas@redvitalpaipa.com
COORDINADOR DE LABORATORIO	laboratorio@redvitalpaipa.com
COORDINADOR DE ASEO	aseo@redvitalpaipa.com
COORDINADOR DE SELECCIÓN EN LA FUENTE	aprovechamiento@redvitalpaipa.com
COORDINADOR DE COMERCIAL, FACTURACIÓN Y PQRSD	comercial@redvitalpaipa.com
PROFESIONAL CONTABILIDAD Y PRESUPUESTO	contabilidad@redvitalpaipa.com
PROFESIONAL CONTRATACIÓN	contratacion@redvitalpaipa.com
TESORERO GENERAL	tesoreria@redvitalpaipa.com
TÉCNICO DE SISTEMAS	sistemas@redvitalpaipa.com
TÉCNICO OPERATIVO ECA	aprovechamiento@redvitalpaipa.com
AUXILIAR ADMINISTRATIVO FACTURACIÓN	redvital@paipa-boyaca.gov.co
AUXILIAR ADMINISTRATIVA CONTABLE	redvital@paipa-boyaca.gov.co
AUXILIAR ADMINISTRATIVA ARCHIVO	archivo@redvitalpaipa.com
AUXILIAR ADMINISTRATIVA ALMACÉN	almacen@redvitalpaipa.com
AUXILIAR ADMINISTRATIVA GERENCIA	gerencia@redvitalpaipa.com

6. DESARROLLO DEL PROCEDIMIENTO

No	ACTIVIDAD (QUE)	DESCRIPCIÓN (COMO)	RESPONSABLE (QUIEN)	REGISTRO
1	Inventario tecnológico	Se realizará un inventario tecnológico donde se tenga un registro verídico de la cantidad de equipos de cómputo con que cuenta la Entidad.	Profesional Gobierno Digital Técnico Administrativo Gobierno Digital	Registro de Custodia
2	Usuarios, contraseñas y privilegios	Con base en el registro de custodia responsabilidad de los equipos de cómputo pertenecientes a la entidad se crearán usuarios y contraseñas	Profesional Gobierno Digital	PA-GCOM-FO-06 Acta de Entrega De Correos Corporativos

		para el inicio de sesión en cada una de las estaciones de trabajo. Estas claves serán administradas por el contratista del área de sistemas. Los privilegios que sean asignados a cada funcionario o contratista dependerán de las actividades que le sean asignadas según el manual de funciones de la entidad o en su contrato, dichos privilegios no excederán ni limitaran el buen desarrollo de las actividades. El usuario administrador de todos los equipos de cómputo de la Entidad será el encargado del área de sistemas, los demás privilegios serán asignados de acuerdo al manual de funciones y/o actividades del contratista. Se realizarán revisiones trimestrales de las claves de acceso, realizando comprobaciones de cantidad de usuarios, El Área de Talento Humano o quien haga sus veces, al igual que las Dependencias notificarán cambios en el personal por medio escrito o verbal. Se realizará una base de datos con los usuarios y contraseñas mensuales de los funcionarios y contratistas que tengan bajo su custodia un equipo de cómputo o dispositivo, se realizarán cambios de contraseñas según la periodicidad requerida. Cada funcionario deberá limpiar de manera cuidadosa los equipos que tiene a cargo de tal manera que se alargue la vida útil de los dispositivos.	Técnico Administrativo Gobierno Digital Líderes de Procesos	

		No se permitirá el uso de equipos de propiedad de la Entidad a terceros sin previa autorización del contratista encargado del Área de Sistemas.		
3	Pasantes o Practicantes	Se les permitirá el ingreso de equipos de cómputo u otros dispositivos mediante solicitud y aprobación escrita por la Dependencia de Gobierno Digital. La conexión a internet que se otorgará será por cable y cumplirá con las demás disposiciones que en este documento expresa. La Entidad no se hará responsable por daño eléctrico, infección por virus, daño a la integridad del equipo hurto o pérdida. No podrá acceder a la información de la Entidad sin previa autorización del Jefe Inmediato y deberá a la Dependencia de Gobierno Digital.	Profesional Gobierno Digital Técnico Administrativo Gobierno Digital Líderes de Procesos	PA-GCOM-FO-01 Oficios / Comunicaciones
4	Las contraseñas de aplicativos, correos electrónicos, equipos de cómputo o cualquier otro sistema de información deberán cumplir las siguientes especificaciones	Mínimo 8 caracteres que contenga letras mayúsculas, minúsculas, Símbolos y números. No deberán contener nombres de los funcionarios, nombre o lema de la entidad, nombre de usuario o documento de identidad del contratista. Para el proceso de reinicio de contraseñas y/o usuarios de accesos se realizará la solicitud mediante comunicación escrita al encargado de sistemas de la Entidad.	Profesional Gobierno Digital Técnico Administrativo Gobierno Digital Líderes de Procesos	Soporte Digital
PUNTO DE CONTROL				

3. Usuarios, contraseñas, privilegios. Cadena de custodia de la creación de usuarios y contraseñas.

7. DOCUMENTOS DE REFERENCIA

Ley 1273 de 2009. Protección de la información y de los datos
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
Política de Seguridad de la Información de la Entidad, versión vigente (si la manejan separada; si no, se deja solo el Plan)
Lineamientos internos para administración de usuarios, contraseñas y privilegios de acceso, versión vigente
NTC-ISO 9001:2015. Sistema de gestión de la calidad – Requisitos
Capítulo 7.1.3. Infraestructura
Capítulo 7.1.6. Conocimientos de la organización
Capítulo 7.5. Información documentada
Capítulo 8.5.1. Control de la producción y de la provisión del servicio

8. ANEXOS

PA-GCOM-PL-01 Plan de Seguridad y Privacidad de la Información
PA-GCOM-FO-06 Acta de Entrega de Correos Corporativos
Registro de Custodia
Soporte Digital

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: