EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS RED VITAL S.A. E.S.P.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PAIPA S.A. E.S.P. Red Vital

PAIPA
ENERO DE 2026

TABLA DE CONTENIDO

Pag.

INTRODUCCIÓN 03

1. OBJETIVO GENERAL 04

1.1 OBJETIVOS ESPECIFICOS

2. ALCANCE 05

3. RESPONSABLES 05

4. SOPORTE LEGAL 06

5. DEFINICIONES 09

6. DESARROLLO 12

6.1 METODOLOGIA PARA IMPLEMENTACIÓN 12

6.2 ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN 13

6.3 LINEAMIENTO DE SEGUIRDAD 15

6.4 ACUERDOS DE CONFIDENCIALIDAD 16

6.5 CLASIFICACION DE LA INFORMACION 17

6.6 SEGURIDAD DE LOS RECURSOS HUMANOS 17

6.7 ENSEÑANZA, FORMACIÓN Y CONCIENTIZACIÓN RESPECTO A SEGURIDAD DE LA INFORMACIÓN 17

6.8 PROCESOS DISCIPLINARIOS 18

6.9 DEVOLUCION DE ACTIVO 18

6.10 SEGURIDAD FISICA Y DEL ENTORNO 18

7. CRONOGRAMA DE ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION. 22

8. PLANES DE SEGUIMIENTOS 23

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se establece para la **Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P**. como un mecanismo encaminado a la gestión progresiva y sistemática de los riesgos que afectan la confidencialidad, integridad, disponibilidad y privacidad de la información.

En el marco del Sistema de Gestión de Seguridad de la Información (SGSI), este plan se articula con el modelo de madurez definido por la organización, permitiendo evaluar el nivel de ejecución de los controles, priorizar acciones de mejora y fortalecer la capacidad institucional para la gestión de la seguridad de la información. Lo anterior proporciona el cumplimiento normativo, la mejora continua y el aumento del nivel de confianza de las partes interesadas en el manejo responsable y seguro de la información.

PAIPA S.A. E.S.P. Red Vital

1. OBJETIVO GENERAL

Diseñar las estrategias y acciones de tratamiento para reducir, mitigar, aceptar, evitar o transferir los riesgos de seguridad y privacidad de la información identificados en la entidad, de acuerdo con su nivel de impacto y probabilidad en la empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P.

1.1 OBJETIVOS ESPECIFICOS

- Promover el uso de mejores prácticas de seguridad de la información en la institución.
- Mejorar la gestión de la seguridad de la información al interior de la entidad.
- Emplear de manera correcta la legislación relacionada con la protección de datos personales.
- Optimizar la labor de acceso a la información pública.
- Garantizar la confianza de las partes interesadas en la responsabilidad institucional de salvaguardar apropiadamente la confidencialidad, integridad y disponibilidad de la información bajo responsabilidad de la entidad.

2. ALCANCE

El alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información alcanza todos los procesos misionales, estratégicos y de apoyo de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P.; de igual manera contiene la información gestionada por la entidad, independientemente de su formato o medio, ya sea físico o digital.

Además, abarca los activos de información, tecnológicos, humanos y aquellos suministrados o administrados por terceros que se encuentren relacionados con la prestación del servicio público y que soportan las operaciones de la organización.

3. RESPONSABLES

El Plan de Seguridad y Privacidad de la Información aplica a todos los funcionarios, colaboradores, terceros, procesos, servicios de la empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P.

4. SOPORTE LEGAL

Ley 527 (18 de agosto 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 Estatutaria 1581 (17 de octubre de 2012)	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1266 (31 de diciembre de 2008)	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1712 (06 de marzo de 2014)	Ley de Transparencia y acceso a la información pública nacional.
Ley 57 (05 de julio de 1985)	Por la cual se ordena la publicidad de los actos y documentos oficiales.
Ley 962 (08 de julio de 2005)	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

Ley 2052 de 2020	Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones.
Decreto Ley 2150 (05 de diciembre de 1995)	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
Decreto 1078 (26 de mayo de 2015)	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 019 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
Decreto 2364 (22 de noviembre de 2012)	Firma electrónica.
Decreto 1747 (11 de septiembre de 2000)	Por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.
Decreto 1078 (26 de mayo de 2015)	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto No. 2106 (22 de noviembre de 2019).	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
Resolución 3564 de 2015 (31 de diciembre de 2015)	Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
Documento CONPES 3854	Política Nacional de Seguridad Digital.

Documento CONPES 3975	Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES).
Norma Técnica Colombiana NTC- ISO/IEC Colombiana 27001:2013	Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

5. DEFINICIONES

Activo. Cualquier recurso, elemento o componente que interviene en el tratamiento de la información y que posee valor para la organización, incluyendo sistemas, soportes, infraestructuras, personas y servicios.

Activo de información. Recurso tangible o intangible que almacena, procesa o soporta información relevante para la organización, y que contribuye directa o indirectamente al cumplimiento de sus funciones, tales como aplicaciones, equipos, roles, instalaciones, repositorios físicos y digitales, así como la imagen y reputación institucional.

Antivirus. Herramienta de software diseñada para identificar, prevenir, neutralizar y eliminar códigos maliciosos que puedan comprometer la seguridad de los sistemas de información.

Amenaza informática. Evento o condición, real o potencial, de origen cibernético, capaz de afectar la seguridad de la información, los sistemas tecnológicos o la continuidad de los servicios de una organización o del Estado.

Análisis de riesgos. Proceso sistemático mediante el cual se identifican, analizan y evalúan los riesgos asociados a los activos de información, considerando amenazas, vulnerabilidades y posibles impactos.

Archivos PST. Archivos electrónicos generados por aplicaciones de mensajería como Microsoft Outlook, utilizados para almacenar de manera local correos electrónicos y otros elementos del buzón.

Anonimización del dato. Técnica mediante la cual se transforma la información personal de forma irreversible, eliminando o sustituyendo identificadores, con el fin de impedir la identificación de los titulares y proteger la confidencialidad.

Correo electrónico. Servicio de comunicación digital que permite el intercambio de mensajes y archivos entre usuarios a través de redes electrónicas.

Contraseña (PassWord). Dato confidencial utilizado como mecanismo de autenticación para restringir y controlar el acceso a sistemas o recursos de información.

Custodio del activo de información. Persona, rol o área designada responsable de operar y proteger un activo de información, garantizando la aplicación de los controles definidos por el responsable del activo.

Datos abiertos. Conjunto de datos puestos a disposición del público de forma libre y reutilizable, con el fin de promover la transparencia y el aprovechamiento de la información.

Datos biométricos. Información derivada de características físicas, fisiológicas o conductuales únicas de una persona, utilizada para su identificación o autenticación.

Datos personales sensibles. Información personal cuyo tratamiento indebido puede afectar la intimidad del titular o generar discriminación, incluyendo datos relacionados con salud, ideología, creencias, vida sexual y características biométricas.

Dato privado. Información personal de naturaleza reservada que solo concierne al titular y cuyo acceso se encuentra restringido.

Gestión de claves. Conjunto de procesos y controles orientados a la generación, almacenamiento, uso, protección y eliminación de claves criptográficas.

Gestión de incidentes de seguridad de la información. Proceso estructurado para identificar, reportar, analizar, responder y aprender de los incidentes que afecten la seguridad de la información.

Habeas data. Derecho fundamental que permite a los titulares conocer, actualizar, rectificar y controlar el uso de su información personal almacenada en bases de datos o archivos.

Infraestructura tecnológica. Conjunto de recursos tecnológicos que soportan los servicios y procesos de la organización, incluyendo hardware, software, redes y herramientas de comunicación.

Responsable del activo de información. Persona o área designada encargada de definir, autorizar y supervisar el uso, protección y controles aplicables a un activo de información específico.

Seguridad de la información. Conservación de la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de controles adecuados.

Autenticación. Mecanismo de verificación que permite confirmar la identidad de un usuario, sistema o entidad antes de conceder acceso a un recurso.

Autenticidad. Propiedad que garantiza que una entidad, usuario o información es legítima y corresponde a quien afirma ser.

Copia de respaldo (Backup). Duplicado de información realizado con el propósito de garantizar su recuperación ante pérdida, daño o indisponibilidad de los datos originales.

Buzón de correo. Espacio asignado dentro de un servidor de mensajería electrónica para el almacenamiento y gestión de correos, contactos, calendarios y otros elementos asociados.

Canal de comunicación. Medio físico o lógico utilizado para la transmisión de información entre emisores y receptores, como cableado, fibra óptica, redes inalámbricas u otros medios.

Centro de cómputo. Instalación que concentra la infraestructura tecnológica necesaria para el procesamiento, almacenamiento y gestión de la información de la organización, también conocido como centro de datos.

Control informático. Medida administrativa, técnica u organizacional implementada para prevenir, detectar o reducir los riesgos de seguridad de la información, disminuyendo la probabilidad o el impacto de eventos no deseados.

6. DESARROLLO

La seguridad de la información en la entidad se basa en tres pilares fundamentales: la confidencialidad, la integridad y la disponibilidad. Con la intención de garantizar el apropiado funcionamiento de los métodos institucionales y la continuación en el tratamiento de la información, se hace necesaria la implementación y gestión de controles de seguridad acordes con los riesgos identificados. Estas medidas permiten mitigar los impactos asociados a sucesos adversos y a las diferentes amenazas que pueden afectar los activos de información bajo responsabilidad de la empresa.

6.1 METODOLOGIA PARA IMPLEMENTACIÓN

Para el desarrollo del Plan de Seguridad y Privacidad de la Información de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P., se adopta como marco de referencia la norma NTC ISO/IEC 27001:2013, relativa al Sistema de Gestión de Seguridad de la Información. Adicionalmente, el plan se basa en el modelo de gestión de la seguridad de la información de la entidad y se desarrolla bajo el enfoque de mejora determinado por la metodología PHVA, en articulación con los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

FASES DE IMPLEMENTACION.

- **Fase de Análisis:** Corresponde a la etapa previa a la implementación del plan, en la cual se ejecuta el diagnóstico del estado actual de la entidad frente a los requisitos de seguridad y privacidad de la información. En esta fase se valora la situación de la gestión de la seguridad de la información al interior de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P., con el fin de establecer el nivel de efectividad de los controles existentes, identificando avances en su implementación y verificando la adecuada aplicación de las buenas prácticas adoptadas por la empresa.

- **Fase de Organización:** En esta fase se examinan los resultados logrados en la fase de análisis, a partir de los cuales se estructura y formaliza el Plan de Seguridad y Privacidad de la Información, en proporción con los objetivos estratégicos de la empresa. Su intención es definir y priorizar las acciones, responsables y recursos necesarios para la ejecución de las medidas de seguridad y privacidad de la información.

- **Fase de Ejecución:** Esta fase permite establecer las actividades formuladas en la fase anterior.

- **Fase de Valoración**: Pertenece a la etapa de seguimiento y control del plan, en la cual se efectúa el monitoreo sistemático de los resultados obtenidos. En esta fase se evalúa el nivel de eficiencia y efectividad de las acciones implementadas, con el fin de identificar oportunidades de mejora y certificar el cumplimiento de los objetivos establecidos en materia de seguridad y privacidad de la información.

- **Fase de Mejora Continua**: Se consolidan los resultados de la evaluación para trazar el plan de mejoramiento y rastreo continuo, tomando las acciones pertinentes para mitigar las debilidades.

  El Plan de Tratamiento de Riesgos será inspeccionado y actualizado de manera constante, teniendo en cuenta los resultados del seguimiento, auditorías, incidentes de seguridad y cambios en el contexto de la empresa.

PAIPA S.A. E.S.P. Red Vital

6.2 ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN

Se establecen las actividades y procedimientos necesarios para el desarrollo de la seguridad y la privacidad de la información, ajustables a cada uno de los procesos de la **Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P**., afirmando la correcta implementación de los controles de seguridad y el cumplimiento de los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información.

- **Política de Seguridad de la Información.**

La Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P. establece la presente Política de Seguridad de la Información acogiendo medidas administrativas, técnicas y organizacionales encaminadas a prevenir el acceso no autorizado, la divulgación indebida, la alteración, la pérdida o el uso inadecuado de la información contenida en sus sistemas de información, bases de datos y plataformas asistenciales y administrativas.

- **Seguridad de activos de información.**

Enfocada a la identificación y asignación de responsables y custodios de los activos de información, certificando su protección conforme a su nivel de criticidad.

- **Seguridad ligada al Talento Humano.**

Todos los funcionarios, sin importar el tipo de vinculación o modalidad de contratación, que posean acceso a la información de la **Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P**., deberán contar con autorización previa y cumplir como mínimo con los siguientes criterios:

- Salvaguardar los expedientes e información que, por razón de su cargo o función, almacene bajo su cuidado o a la cual tenga acceso, impedir o evitar la sustracción, destrucción, desaparición o utilización indebidas de la información institucional.

- Firma de compromisos de confidencialidad y responsabilidad sobre el manejo de la información.

- Uso apropiado de los sistemas de información y recursos tecnológicos de la empresa.

- Acatamiento de la normatividad legal vigente en materia de protección de datos personales.

- Resguardar los software, los aplicativos, los equipos de comunicación y procesamiento de datos, que le han sido estipulados para su manejo de acuerdo al uso de las buenas prácticas, de forma racional y de aprobación con los fines a que han sido propuestos.

- Los funcionarios deben garantizar que el acceso de la información y la utilización de ella sea exclusivamente para actividades relacionadas con la empresa y sea utilizada de acuerdo a los criterios de confidencialidad.

- **Protección de los Recursos Tecnológicos.**

- La Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P asegurará la contratación requerida para mantener actualizadas las licencias de Antivirus, Firewall, el mantenimiento de las redes y equipos.

- Estudio de controles de seguridad sobre la infraestructura tecnológica, incluyendo sistemas, redes, equipos y aplicaciones que soportan los procesos institucionales.

- **Copias de respaldo y recuperación de la información**

Práctica de políticas y procedimientos para la ejecución de copias de seguridad, así como la recuperación de la información ante eventos de pérdida.

- **Gestión de proveedores y terceros**

Valoración y vigilancia de los peligros asociados a terceros que tengan acceso a la información o a los sistemas de la entidad, garantizando el cumplimiento de los requisitos de seguridad establecidos.

- **Capacitación en seguridad de la información.**

Desarrollo de actividades de sensibilización y formación dirigidas a los funcionarios y terceros, con el fin de fortalecer la cultura de seguridad de la información.

6.3 LINEAMIENTO DE SEGUIRDAD.

- La información almacenada y suministrada deberá ser resguardada durante todo su ciclo de vida, optimizando su confidencialidad, integridad, disponibilidad y privacidad, de acuerdo con su nivel de clasificación.

- Toda información deberá estar debidamente identificada, inventariada y contar con un responsable designado.

- El ingreso a la información y a los sistemas de información será concedido únicamente a usuarios autorizados, acorde a sus funciones, roles y responsabilidades.

- La empresa realizará controles técnicos, administrativos y organizacionales para notificar, detectar y mitigar riesgos que puedan afectar la seguridad de la información.

- El tratamiento de los datos personales de los funcionarios, sin importar el tipo de vinculación o modalidad de contratación se realizará en cumplimiento de la normativa vigente, garantizando los derechos de los titulares y la protección de la información sensible.

- Se deberán instaurar y mantener mecanismos de autenticación seguros para el acceso a los sistemas de información y recursos tecnológicos de la empresa.

- La infraestructura tecnológica deberá contar con medidas de protección que reduzcan la posibilidad de incidentes de seguridad y afirmen la continuidad de los servicios a brindar

- La información o datos críticos deberán contar con esquemas de respaldo y recuperación que permitan su restablecimiento oportuno ante eventos de pérdida, daño o acceso.

- Los incidentes de seguridad de la información deberán ser reportados, solucionados y documentados de manera oportuna, con el fin de minimizar impactos y prevenirlos nuevamente.

- Las personas externas que tengan acceso a la información o a los sistemas de la empresa deberán cumplir con los lineamientos y controles de seguridad establecidos por Red Vital Paipa S.A. E.S.P.

- La empresa incluirá sensibilizaciones y capacitaciones relacionadas en materia de seguridad y privacidad de la información.

- Toda información que sea de interés para un proceso asistencial, administrativo o de misión crítica debe ser guardada y respaldada mediante copias de seguridad, las cuales deben conservarse en lugar seguro.

PAIPA S.A. E.S.P. Red Vital

6.4 ACUERDOS DE CONFIDENCIALIDAD

Todos los funcionarios, colaboradores y/o terceros que presten sus servicios a la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P, deben aceptar los respectivos acuerdos de confidencialidad establecidos, los cuales manifiestan los compromisos de protección y buen uso de la información de acuerdo a los criterios señalados en ella.

En el caso de los contratistas, sus respectivos contratos deben contener una cláusula de confidencialidad, de la misma forma cuando se permita el acceso a información y/o a los recursos de la empresa, personas o entidades externas.

Estos acuerdos se deben aceptar por cada uno como parte del proceso de contratación, razón por la cual todo lo mencionado hace parte integral de cada uno de los contratos.

Las intervenciones que se establezcan como obligatorias a partir del análisis de riesgos deben ser manifestadas y admitidas por el tercero a partir de la firma de acuerdos, antes de la entrega de los accesos requeridos o que se vayan a solicitar.

6.5 CLASIFICACION DE LA INFORMACION

La **Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P** con el fin de proteger la información que pueda ser divulgada de forma no autorizada o manejada erróneamente por sus funcionarios, colaboradores y/o terceros, ha determinado varios niveles para la categorización de la información, donde se puede encontrar mediante correos electrónicos, impresos, verbales o transmitidos por cualquier medio.

Toda información relacionada a la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P debe estar identificada, clasificada y documentada a partir de su categorización establecida, a continuación, se presentan así:

- CATEGORIA DE USO EXTERNO
- CATEGORIA DE USO PÚBLICO
- CATEGORIA DE USO PÚBLICO INTERNO
- CATEGORIA DE USO PÚBLICO CLASIFICADA
- CATEGORIA DE USO PÚBLICA RESERVADA

6.6 SEGURIDAD DE LOS RECURSOS HUMANOS

Todos los funcionarios, colaboradores y/o terceros que hacen parte de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P que tienen acceso a la información de la empresa e infraestructura para su procesamiento, son garantes de conocer y cumplir tal cual con las políticas e instrucciones establecidas en el Modelo de Gestión de Seguridad de la Información de la empresa. Así mismo, son encargados de reportar por medio de los canales oportunos, el incumplimiento de las políticas y procedimientos determinados.

6.7 ENSEÑANZA, FORMACIÓN Y CONCIENTIZACIÓN RESPECTO A SEGURIDAD DE LA INFORMACIÓN.

La Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P, debe asegurarse que cada uno de sus funcionarios tenga bien determinadas sus responsabilidades en la seguridad de la información, que sean competentes para realizar sus ocupaciones, contando con capacitaciones y preparaciones para ello.

Así mismo cada uno de los funcionarios y, cuando sea requerido colaboradores y/o terceros tendrán procesos de concientización, donde se les capacitará de manera correcta sobre las políticas de seguridad en la empresa, así como los riesgos a los que se pueden ver expuestos, en caso que no se lleve un correcto uso.

Estas actividades o procesos de concientización se diseñan de manera oportuna y detallada para cada uno de los roles, responsabilidades y habilidades de las personas que deben realizarlos.

6.8 PROCESOS DISCIPLINARIOS

Cuando se presentan incidentes de seguridad, se hará la investigación pertinente para determinar las causas y responsables, posterior a ello la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P, será la encargada de tomar las acciones pertinentes para que la persona relacionada con el suceso, mediante un proceso disciplinario formal de acuerdo con su naturaleza, gravedad o impacto que se generó en la empresa.

6.9 DEVOLUCION DE ACTIVOS

Todo funcionario al momento de su retiro o cambio de funciones en la empresa debe hacer de manera oportuna y correcta la entrega del equipo que se le asigno en su momento, adjuntando un inventario con toda la información contenida en él.

6.10 SEGURIDAD FISICA Y DEL ENTORNO

La Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P, es la encargada de definir el perímetro de la seguridad física en base a la clasificación de los activos de la información, administrando el acceso a la información a través de controles (Ejemplo: ingreso a diferentes áreas, registro de entrada de los diferentes equipos y autenticación), lo cual reduce la posibilidad de riesgo de divulgación o perdida de la información.

- **Controles de Acceso Físico**

Las dependencias en las que se administren, procesen o resguarden información de carácter sensible, así como las áreas donde se ubican los sistemas, equipos y dispositivos tecnológicos que soportan los servicios de información y comunicaciones, serán consideradas áreas de acceso limitado. Por tal razón, deberán disponer de mecanismos de control físico que regularicen el ingreso, permitan su inspección y faciliten la verificación, escoltados de procedimientos operativos que ayuden a la protección de la información y de los activos tecnológicos respecto a riesgos accidentales o acciones deliberadas.

De igual modo, los centros de datos, salas técnicas, redes de cableado y demás instalaciones críticas deberán contar con escenarios ambientales controlados, de acuerdo con las especificaciones técnicas de los fabricantes, así como con medidas preventivas y de respuesta que permitan proceder de manera adecuada ante eventos como incendios, fallas eléctricas, inundaciones u otras situaciones que puedan comprometer la operación y continuidad de los servicios.

- **Protección y ubicación de los equipos**

Todos los equipos que hacen parte de la Infraestructura tecnológica de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P como lo son servidores, centros de cableado, UPS, subestaciones eléctricas, equipos de comunicaciones y seguridad electrónica, así como estaciones de trabajo y dispositivos de almacenamientos y/o comunicaciones móviles que contengan o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

Todos los funcionarios, colaboradores y/o terceros que hacen parte de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P que tengan acceso a los equipos que componen la parte de infraestructura tecnológica no pueden fumar, beber o consumir algún tipo de alimento cerca a los equipos.

Cualquier traslado de equipos de cómputo dentro de la empresa se realizará con la coordinación del área de Sistemas bajo previa verificación de las condiciones técnicas y de seguridad correspondientes.

Todo personal que note algún problema relacionado al funcionamiento o ataque de virus en una estación de trabajo debe notificar de inmediato al personal de soporte técnico para su solución respectiva.

No obstante, la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P debe proporcionar suministros y equipamiento de soporte como electricidad y un sistema de alimentación no interrumpida (UPS) que garantice el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de cualquiera de estos elementos, evitando así la pérdida o corrupción de información. Los suministros mencionados anteriormente deben ser monitoreados, revisados de forma permanente para garantizar su correcto funcionamiento, condicionamiento normal de operación y evitar daños futuros.

Finalmente, la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P, debe establecer un itinerario de planeación y realización de mantenimientos preventivos anuales a las infraestructuras tecnológicas que almacenan en ella.

PAIPA S.A. E.S.P. Red Vital

- **Gestión de contraseñas**

- Toda contraseña o clave de acceso a los activos de la información son de uso personal e intransferibles.

- Las acciones realizadas tanto con el usuario y contraseñas asignadas son exclusivamente responsabilidad del personal que se le asigno.

- Todas y cada una de las contraseñas no deben y no pueden ser divulgadas o compartidas entre usuarios. Cualquier intento de daño o alteración de la información es responsabilidad del usuario que la realizó.

- Está prohibido prestar el usuario y contraseña asignados, en caso de cometer alguna violación de seguridad, la responsabilidad recaerá única y exclusivamente sobre la persona a cargo de dicho usuario.

- **Seguridad de los equipos y medios de información fuera de las instalaciones**

- Todos y cada uno de los funcionarios son garantes de velar por la seguridad de los equipos pertenecientes a la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P. De igual manera los equipos de cómputo no pueden ser dejados en lugares públicos o a la vista, esto en el caso que se este transportando en un vehículo.

- Cada uno de los equipos de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P, deberá contar con un seguro de protección frente a robos.

- Frente a una pérdida o robo de un equipo perteneciente a la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P, se debe informar de carácter urgente e inmediato para iniciar el respectivo tramite interno y colocar la denuncia frente a la autoridad competente.

- El retiro de equipos de cómputo, dispositivos de almacenamiento, softwares e información irremplazable en propiedad de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P, fuera de las instalaciones deben seguir los procedimientos establecidos por el área de Sistemas de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P.

- **Eliminación o reutilización segura de equipos y medios**

La Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P debe identificar cada uno de los posibles riesgos potenciales que puede generar destruir, reconstruir o eliminar cada uno de los equipos y medios de almacenamiento. Con esto, se deben establecer e implementar los respectivos mecanismos y controles adecuados para que la información delicada que esta contenida en ellos sea eliminada de manera correcta y segura.

En caso tal que un equipo sea reasignado o dado de baja, se debe realizar el respectivo proceso de acuerdo al procedimiento que se vaya a aplicar a su finalidad.

7. CRONOGRAMA DE ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

DESCRIPCION DE ACTIVIDADES Y ESTRATEGIAS RED VITAL PAIPA S.A. E.S. P
Realizar el respectivo mantenimiento preventivo a la totalidad de equipos de informática.
Dar soporte y realizar los ajustes requeridos en el sistema de información.
Generar los informes requeridos por las diferentes áreas.
Dar solución en el menor tiempo posible frente a los requerimientos por fallas en los equipos de comunicación e informática.
Adquirir suministros de repuestos para computadores e impresoras de la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P.
Realizar el proceso de diagnóstico para evaluar los equipos que requieren de una actualización o solicitud de adquisición.
Realizar el respectivo proceso contractual para la adquisición de Antivirus para cada uno de los servidores y equipos de cómputo.
Realizar si es necesario el proceso de cambio de equipos en las áreas que se requiera.
Adquirir Hosting, Dominio y capacidad de almacenamiento para garantizar el óptimo funcionamiento de la página Web.
Adquirir servicios de almacenamiento en la nube para el correcto funcionamiento de cada uno de los correos electrónicos de la empresa.
Actualizar la página Web de acuerdo a lineamientos normativos.
Evaluar la efectividad y generar acciones de mejora.
Realizar el respectivo proceso de actualización del sistema de información de la página web, manteniendo su información al día.

8. PLANES DE SEGUIMIENTOS.

Se realizará el respectivo seguimiento de forma anual, de tal motivo que se compruebe su cumplimiento frente a las actividades establecidas y se puedan ejecutar ajustes o variaciones según lo ameriten o determinen las necesidades de estas.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Byron Duwar Maldonado Sanchez	Nombre: Andrew Masami Asakura García	Nombre: Yeison Rokney Torres Suárez
Cargo: Técnico Administrativo Sistemas.	Cargo: Profesional SIG	Cargo: Gerente General
Firma: Original con firma	Firma: Original con firma	Firma: Original con Firma

PAIPA S.A. E.S.P. Red Vital