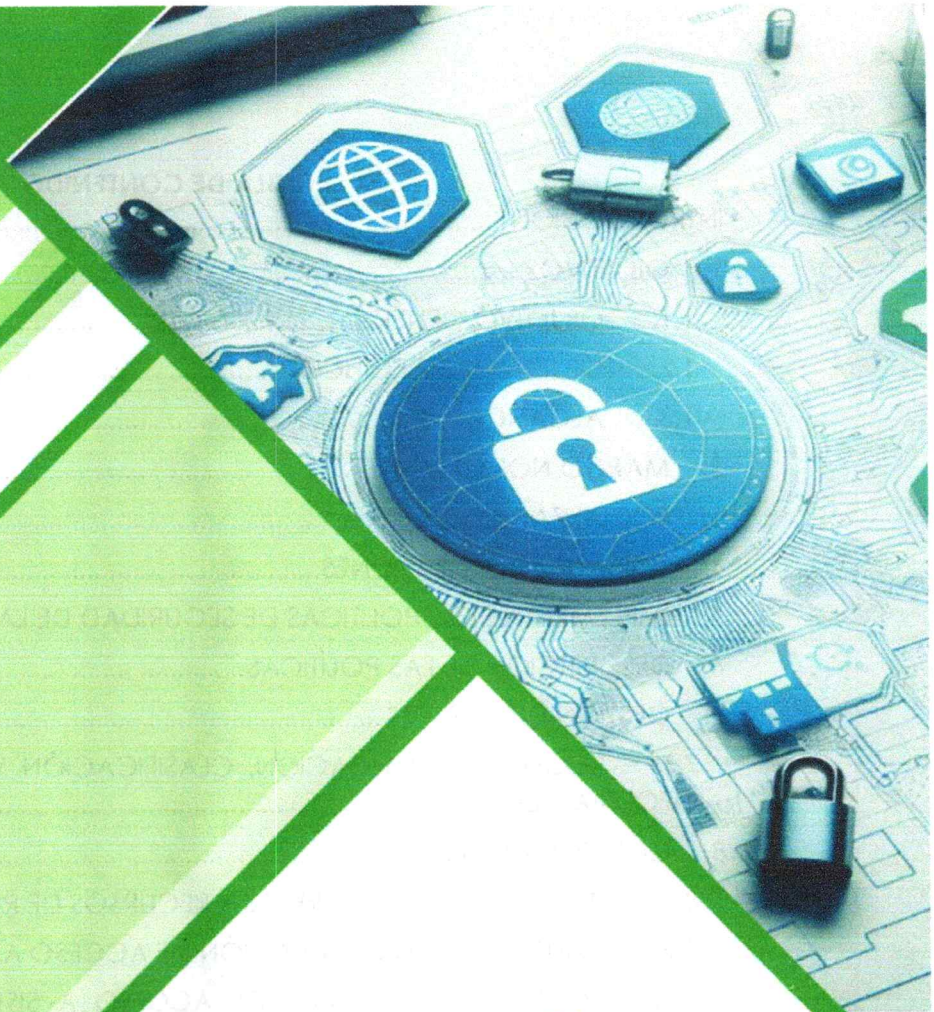

Girón E.S.P

Empresa de Servicios Públicos de Girón s.a.s / e.s.p.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2025

TABLA DE CONTENIDO

INTRODUCCIÓN

Orientada bajo una política de calidad; La Empresa de Servicios Públicos Domiciliarios Girón S.A.S. E.S.P., está direccionada a la satisfacción de la comunidad en los servicios públicos domiciliarios de acueducto, alcantarillado y aseo fundamentándose en el cumplimiento de la normatividad legal vigente, motivando la participación ciudadana, un manejo adecuado de los recursos humanos, físicos y financieros y el mejoramiento continuo de todos los procesos.

Por lo que lo anterior, se articula con la Política General de Seguridad y Privacidad de la Información, donde Girón S.A.S. E.S.P., ha decidido definir, implementar, operar y mejorar de forma continua procesos en Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Empresa, y a los requerimientos regulatorios.

Es así como La Empresa de Servicios Públicos Domiciliarios GIRÓN S.A.S. E.S.P. promueve la participación y el compromiso de todo el personal de planta, contratistas, usuarios, suscriptores, y visitantes para el cabal cumplimiento de cada una de las directrices dispuestas en el Plan de Seguridad y Privacidad de la Información, y los conmina a asumir una actitud de compromiso, el cumplimiento de los procedimientos, normas y políticas; Que finalmente identifique y dé a conocer el correcto tratamiento de la información teniendo presente la privacidad de la información como objetivo principal.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Implementar el Plan de Seguridad y Privacidad de la Información para la Empresa Girón S.A.S E.S.P., con el fin de describir las medidas oportunas para proteger activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

1.2. OBJETIVOS ESPECIFICOS

- Direccionar a los funcionarios y contratistas que trabajan para Girón S.A.S E.S.P., acerca de la importancia que tiene la seguridad y privacidad de la información para disminuir los riesgos asociados a la misma.
- Alinear las medidas y/o planes formulados cuando sea necesario con lo direccionado en el PETI para que sirva de herramienta para el mismo.

1.3. ALCANCE

El Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los trabajadores de la empresa Girón S.A.S E.S.P., a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad, contratistas y terceras partes, que usen activos de información que sean propiedad de la entidad.

Con este plan se formularán lineamientos y estrategias básicas para empezar a brindar capacitación en seguridad de la información enfocados en aumentar la cultura en seguridad de la información en los funcionarios y contratistas de la institución; así como también mejoras en los procedimientos realizados de manera interna relacionados con la seguridad de la información con el fin de mejorar los niveles de seguridad de la información de los usuarios y comunidad.

2. MARCO NORMATIVO

- **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.

- **Decreto 1122 de 1999**: Por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fe.

- **Ley 962 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.

- **Decreto 1151 de 2008**: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.

- **Ley 1341 de 2009:** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- **Decreto 235 de 2010**: Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

- **Conpes 3670 de 2010**: Lineamientos de política para la continuidad de los programas de acceso y servicio universal a las tecnologías de la información y las comunicaciones.

- **Conpes 3701 de 2011**: Lineamientos de política para ciberseguridad y ciberdefensa.

- **Ley 1581 del 2012**: Por la cual se dictan disposiciones generales para la protección de datos personales.

- **Ley 1712 del 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.

- **Decreto 2573 de 2014**: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

- **Decreto 0103 de 2015**: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- **Decreto 415 de 2016**: Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo

relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.

3. SOCIALIZACIÓN

Sin excepción alguna, todos los trabajadores, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento. La ubicación física del documento estará a cargo de la Dirección Administrativa y Jurídica de la entidad para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.gironesp.com.

Mediante socialización a todos los trabajadores de la Empresa Girón S.A.S E.S.P. se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

4. TÉRMINOS Y DEFINICIONES

- **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información**: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Amenazas**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Confidencialidad**: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000).

- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos**: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales Sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Derecho a la Intimidad**: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Disponibilidad**: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).

- **Encargado del Tratamiento de Datos**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).

- **Estimación del riesgo**: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

- **Gestión de incidentes de seguridad de la información**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Integridad**: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).

- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar.

- **Procedimiento**: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Titulares de la información**: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Transferencia del riesgo**: Compartir con otra de las partes la pérdida o la ganancia de un riesgo. Nota: En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la transferencia del riesgo.

- **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

5. IMPLEMENTACIÓN POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Garantizando la seguridad de los datos y el cumplimiento de las normas legales, la Empresa Girón S.A.S E.S.P. con el propósito de salvaguardar la información de la entidad en todos sus aspectos, ha establecido realizar un Plan de Seguridad y Privacidad de la información asegurando de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos. La seguridad de la información se entiende como la preservación de las siguientes características:

a) Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
b) Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

6. DESCRIPCIÓN DE LAS POLÍTICAS

La empresa Girón S.A.S E.S.P. cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

7. GESTIÓN DE ACTIVOS

7.1. POLÍTICA IDENTIFICACIÓN, CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN

El personal a cargo de los recursos físicos de la entidad con el apoyo del encargado de sistemas tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.

Girón S.A.S E.S.P. realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a las dependencias de TIC y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

8. CONTROL DE ACCESO

8.1. POLÍTICA ACCESO A REDES Y RECURSOS DE RED

Las redes de datos y los recursos de red de la entidad son responsabilidad del área de Sistemas e Informática y la Dirección Administrativa y Jurídica de Girón S.A.S E.S.P., es por esto; que ellos deben apoyar que dichas redes, sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico, para esto se deben cumplir las siguientes modelos:

- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de Girón S.A.S E.S.P. deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
- Los trabajadores y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la entidad, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de Confidencialidad firmado previamente.
- El proceso Gestión de TIC debe asegurar que las redes inalámbricas de la empresa cuenten con métodos de autenticación que evite accesos no autorizados.

8.2. POLÍTICA DE ADMINISTRACIÓN DE ACCESO A USUARIOS

La empresa Girón S.A.S E.S.P., implementará privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los trabajadores y el personal provisto por terceras partes tengan acceso

únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin. Es importante tener en cuenta que el área encargada de las TIC debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo. También Los propietarios de los activos de información deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información

8.3. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y APLICATIVOS

La empresa Girón S.A.S E.S.P., como propietaria de los sistemas de información y aplicativos en arriendo que se contraten y que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada. El Profesional Universitario de Sistemas e Informática como responsable de la administración de dichos sistemas de información y aplicativos, vigilará para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

La entidad proporciona la implantación y vigila por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

8.4. POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS DE CÓMPUTO

La empresa Girón S.A.S E.S.P., para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica, atendiendo los siguientes lineamientos:

- El área de Sistemas e Informática debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.

- El proceso Gestión de TIC debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.
- Se debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.
- Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la empresa Girón S.A.S E.S.P., el usuario responsable debe informar a la dependencia de Sistemas e Informática, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los profesionales universitarios de apoyo al área de Sistemas.
- En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

8.5. POLÍTICA DE USO ADECUADO DEL INTERNET

La empresa Girón S.A.S E.S.P., debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos. A su vez debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos. Se debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet. Por tal motivo No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento. Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores. No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el área de Sistemas e Informática de la entidad.

9. PRIVACIDAD Y CONFIDENCIALIDAD

9.1. POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

Por medio de esta política, Girón S.A.S E.S.P., ha instituido las reglas y principios necesarios para brindarle protección a usted, como titular de los datos personales que se tratan dentro de la organización, de cualquier riesgo de vulneración de sus derechos, con miras a garantizar su Dignidad Humana a partir de la implementación de las medidas necesarias y efectivas para cumplir las obligaciones establecidas en la Ley 1581 de 2012 y su Decreto reglamentario. En tal sentido, le informamos que este documento contiene las directrices generales que tendremos en cuenta para tratar sus datos personales cuando sean recolectados, almacenados, usados, circulados o suprimidos por nosotros.

9.2. PRINCIPIOS RELACIONADOS CON LA RECOLECCIÓN DE DATOS

La recolección y tratamiento de datos personales debe realizarse para fines lícitos respetando las normas generales, especiales y la autorización dada por el Titular sobre los mismos. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Dichos datos serán tratados de forma leal y lícita. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

9.3. PRINCIPIOS RELACIONADOS CON EL USO DE DATOS PERSONALES

- **PRINCIPIO DE FINALIDAD**: Los datos personales deben ser procesados con un propósito específico y explícito, el cual debe ser autorizado por el Titular o permitido por la ley. Se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y, por tanto, no podrán recopilarse datos sin una finalidad específica.
- **PRINCIPIO DE TEMPORALIDAD**: Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir la finalidad del tratamiento y las exigencias legales o instrucciones de las autoridades de vigilancia y control u otras autoridades competentes. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Para determinar el término del tratamiento se considerarán las normas aplicables a cada finalidad y los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

- **PRINCIPIO DE NO DISCRIMINACIÓN**: Queda prohibido realizar cualquier acto de discriminación por las informaciones recaudadas en las bases de datos o archivos.

9.4. PRINCIPIOS RELACIONADOS CON LA CALIDAD DE LA INFORMACIÓN

- **PRINCIPIO DE VERACIDAD O CALIDAD**: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error. Se deberán adoptar medidas razonables para asegurar que los datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando la Organización así lo determine, sean actualizados, rectificados o suprimidos cuando sea procedente.

9.5. PRINCIPIOS RELACIONADOS CON LA PROTECCIÓN, EL ACCESO Y LA CIRCULACIÓN DE DATOS PERSONALES

- **PRINCIPIO DE SEGURIDAD**: Cada miembro de la Organización deberá cumplir las medidas técnicas, humanas y administrativas que establezca la misma para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- **PRINCIPIO DE TRANSPARENCIA**: En el tratamiento de datos personales debe garantizarse el derecho del Titular a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

9.6. CANALES DE COMUNICACIÓN

Los titulares de datos personales, sus representantes legales, apoderados o herederos, todos estos debidamente acreditados, podrán ejercer los derechos a los que se refiere la Ley 1581 de 2012 y demás normas concordantes, y en general para la atención de P.Q.R. asociadas a datos personales, únicamente mediante los siguientes canales de comunicación: gironesp.com/pqr, info@gironesp.com, Calle 29 No 25-31 Girón Centro, www.gironesp.com.

9.7. AVISO DE PRIVACIDAD

Para todos los efectos legales, Girón S.A.S E.S.P. manifiesta haber cumplido con el Aviso de Privacidad de que trata el Decreto 1377 de 2013. Los titulares de datos personales que deseen consultarlo podrán hacerlo a través de los canales de atención presentados en este documento. Esta Política de Tratamiento de Información – PTI fue aprobada por Girón S.A.S E.S.P.; Se ha dado a conocer mediante aviso de privacidad elaborado conforme a la ley e inicia su vigencia a

partir de la fecha de su publicación. Para conocimiento de los titulares y terceros interesados puede ser consultada en www.gironesp.com.

9.8. DISPONIBILIDAD DEL SERVICIO DE INFORMACIÓN

La empresa Girón S.A.S E.S.P., con el fin de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, creará una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

9.9. POLÍTICA DE CONTINUIDAD, CONTINGENCIA Y RECUPERACIÓN DE LA INFORMACIÓN

La empresa Girón S.A.S E.S.P., proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

9.10. COPIAS DE SEGURIDAD

La empresa Girón S.A.S E.S.P., efectuará con toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo con los procedimientos documentados por el área de Sistemas e Informática. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros. El área debe proveer las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad. La (el) profesional especializado con funciones de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad. La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

10. SEGUIMIENTO Y MONITOREO

La empresa Girón S.A.S E.S.P., evaluará el desempeño del Plan de Seguridad y Privacidad de la Información a través de la revisión de las acciones que se están llevando a cabo y evaluará la eficiencia en su implementación, adelantando verificaciones y seguimientos al menos una vez al año o cuando sea necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo al Plan de Seguridad y Privacidad de la Información debe estar a cargo del Control Interno, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo.

11. BIBLIOGRAFÍA

- https://www.funcionpublica.gov.co/web/mipg
- https://www.gironsantander.gov.co/Transparencia/Paginas/Planeacion-Gestion-y-Control.aspx
- https://www.funcionpublica.gov.co/planeacion-sectorialinstitucional