

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024 – 2027

**EMPRESA DE SERVICIOS DE EL RETIRO
- RETIRAR S.A.E.S.P**

El Retiro - Antioquia, 2024

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

Tabla de contenido

1. Introducción	3
2. Justificación	3
3. Alcance	3
4. Objetivos	3
Objetivo General	3
Objetivos específicos	4
5. Análisis de la Situación Actual	4
6. Definiciones	5
7. Marco Normativo	9
8. Fases para Implementar e Instrumentar el Modelo de Seguridad y Privacidad de la Información.	13
9. Guías Modelo de Seguridad y Privacidad de la Información	21
10. Plan de Comunicación.....	21

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

1. Introducción

La nueva Política de Gobierno Digital tiene como uno de sus habilitadores la Seguridad y Privacidad de la información. Esto con el fin de desarrollar y adoptar todos los mecanismos que garanticen salvaguardar los activos de información. El Ministerio de las Tic - MINTIC ha establecido que para proteger los activos de información y garantizar su disponibilidad, integridad y confidencialidad debe adoptarse y aplicarse el Modelo de Seguridad y Privacidad de la información

En el presente documento se desarrolló el Plan de Seguridad y Privacidad de la Información para la EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P, donde se plantean todas las fases que permitan la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI.

2. Justificación

LA EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P, con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la Información con el ánimo de que no se presenten pérdidas, robos y accesos no autorizados.

3. Alcance

Este Plan de Seguridad y Privacidad de la Información, es aplicable a todos los funcionarios de la EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P, a sus recursos, procesos y procedimientos tanto internos como externos y así mismo al personal vinculado a la entidad, que usen activos de información que sean propiedad de la entidad.

El plan esta formulado para que se ejecute durante la vigencia 2024-2027, tiempo necesario para lograr la adopción del Modelo de Seguridad y Privacidad de la Información MSPI y garantizar su continuidad.

4. Objetivos

Objetivo General

Instrumentar el Modelo de Seguridad y Privacidad de la información para fortalecer el aseguramiento de los servicios de TI y la información que se genera y obtiene en la EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P, para preservar la confidencialidad, integridad y disponibilidad de la información.

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

Objetivos específicos

- Fomentar en los procesos de la Entidad, la gestión de riesgos de seguridad de la información, con base en los activos críticos previamente identificados y las acciones para mitigar el riesgo.
- Ejecutar actividades en el marco de una metodología de gestión de la seguridad, para establecer un modelo de madurez aplicable y repetible.
- Definir y socializar políticas, lineamientos, buenas prácticas y recomendaciones para establecer cultura en Seguridad de la Información en la Entidad.

5. Análisis de la Situación Actual

LA EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P, en estos momentos cuenta con diferentes criterios para mantener la seguridad de la información, tales como:

- ☐ El Gateway o puerta de enlace del internet, es un dispositivo Cisco, configurado de tal forma que bloquea cualquier conexión que intente acceder a la entidad y sin haber sido autorizada.
- Los cables que transportar el internet, están instalados, dentro de canaletas
- Se tiene configurado un programa para realizar backup de seguridad de forma automática.
- Se cuenta con al menos 2 discos duros donde se almacenan los backups de seguridad de cada una de las dependencias.

De igual manera, la entidad realizará el diligenciamiento de la Herramienta de Diagnostico, denominada “INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD” brindada por el MINTIC, para medir el porcentaje de avance en la planeación y desarrollo del Modelo de Privacidad y Seguridad de la Información.

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

6. 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.

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 controlar en su calidad de tal.

Archivo: conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización

Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo

Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría

Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software),

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

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, y los datos biométricos. (Decreto 1377 de 2013, art 3).

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

Declaración de aplicabilidad: documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles

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).

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).

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.

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).

Plan de continuidad del negocio: plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

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.

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

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

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 y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos: directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

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.

Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información SGSI: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

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

Tratamiento de Datos Personales: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

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.

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas.

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.

7. Marco Normativo

El Estado colombiano cuenta con normatividad vigente que obliga el adecuado tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

Ley 1437 de 2011, Capítulo IV, “utilización de medios electrónicos en el procedimiento administrativo.”

“Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.”

Ley 1581 de 2012, g) Principio de seguridad

“La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.”

Ley 1581 de 2012, Artículo 17, ítem d

“Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”.

Ley 1712 de 2014, “principio de transparencia”

“Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.”

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

Ley 1712 de 2014, artículo 7: “Disponibilidad de la información”

“En virtud de los principios señalados, deberá estar a disposición del público la Información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.”

Ley 1712 de 2014 -Título III “Excepciones acceso a la información”

“Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito.”

Decreto 2573 de 2014

“Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea” donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.

Decreto 1413 de 2017, artículo 2.2.17.6.6, “Seguridad de la información.”

“Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.”

Decreto 1413 de 2017, artículo 2.2.17.6.1, “Responsable y encargado del tratamiento”:

“Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen.”

Decreto 1413 de 2017, artículo 2.2.17.6.3. “Responsabilidad demostrada y programa integral de gestión de datos.”

Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto,

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.

Decreto 1413 de 2007, artículo 2.2.17.6.5, “Privacidad por diseño y por defecto”

“Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador”

Decreto 1413 de 2017, artículo 2.2.17.5.10, “Derechos de los usuarios de los servicios ciudadanos digitales”

Los usuarios de los servicios ciudadanos digitales tendrán derecho a:

- Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador.
- Aceptar, actualizar y revocar las autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales.
- Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre.
- Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales.
- Elegir y cambiar libremente el operador de servicios ciudadanos digitales
- Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en cuyo caso podrá descargar su información a un medio de almacenamiento propio.

Decreto 1413 de 2017, artículo 2.2.17.2.1.1 “Descripción de los servicios ciudadanos digitales.”

Los servicios ciudadanos digitales se clasifican en básicos y especiales.

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

1. Servicios ciudadanos digitales básicos. Son servicios ciudadanos digitales básicos los siguientes:

- **Servicio de autenticación biométrica.** Es aquel que permite verificar y validar la identidad de un ciudadano colombiano por medio de huellas dactilares contra la base de datos biométrica y biográfica de la Registraduría Nacional del Estado Civil, dando pleno cumplimiento a la Resolución 5633 de 2016 emitida por la Registraduría Nacional del Estado Civil o cualquier otra norma que la adicione, modifique, aclare, sustituye o derogue.
- **Servicio de autenticación con cédula digital.** Es aquel que permite la validación de la identidad de los ciudadanos colombianos por medios electrónicos, a través de la cédula de ciudadanía digital que para tal efecto expida la Registraduría Nacional del Estado Civil.
- **Servicio de autenticación electrónica.** Es aquel que permite validar a los usuarios por medios electrónicos, en relación con un mensaje de datos y provee los mecanismos necesarios para firmarlos electrónicamente, en los términos de la Ley 527 de 1999 y sus normas reglamentarias sin perjuicio de la autenticación notarial.
- **Servicio de carpeta ciudadana.** Es aquel que permite el almacenamiento y conservación electrónica de mensajes de datos en la nube para las personas naturales o jurídicas, en donde éstas pueden recibir, custodiar y compartir de manera segura y confiable la información generada en su relación con el Estado a nivel de trámites y servicios. En ningún caso la carpeta ciudadana hará las veces de sistema de gestión de documentos electrónicos de archivo.
- **Servicio de interoperabilidad.** Es aquel que brinda las capacidades necesarias para garantizar el adecuado flujo de información y de interacción entre los sistemas de información de las entidades del Estado, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad.

2. Servicios ciudadanos digitales especiales. Se consideran servicios ciudadanos digitales especiales aquellos adicionales a los servicios ciudadanos digitales básicos, tales como el desarrollo de aplicaciones o soluciones informáticas que puedan ser de interés para la administración o cualquier interesado en el marco de la prestación de los servicios ciudadanos digitales básicos, que aplicarán, entre

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

otros, para los casos descritos en el artículo 45 de la Ley 1753 de 2015 o aquellas normas que la sustituyan, modifiquen o deroguen, para cuyo efecto, el Ministerio de las Tecnologías de la Información y las Comunicaciones definirá y reglamentará en coordinación con las entidades responsables de cada uno de los trámites y servicios los estándares, protocolos y modelos que aplicarán en cada caso.

Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicas cuando lo requieran.”

Decreto 612 de 2018, artículo 1.

“Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web.”

Conpes 3854 de 2016

Objetivo general “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país”.

Por lo anterior, La EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P deben emprender acciones orientadas a la protección de la información que gestiona, realizando la identificación y tratamiento de riesgos de la información de los activos críticos que la soportan, de manera que se establecen y realiza el seguimiento a dichas acciones en el marco del plan de acción y del Sistema Integrado de Gestión.

8. Fases para Implementar e Instrumentar el Modelo de Seguridad y Privacidad de la Información.

Las fases que se requieren para instrumentar el Modelo son:

- Fase de diagnóstico - etapas previas a la implementación
- Fase de planificación.
- Fase de implementación
- Fase de evaluación de desempeño.
- Fase de mejora continua.

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

Cronograma de Actividades Fase de Diagnostico

En esta fase se pretende identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información. Para esto se utilizará la Herramienta de Diagnostico brindada por el MINTIC.

Diagnostico		
Actividad	Responsable	Fecha
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, Utilizando la Herramienta de Diagnostico brindada por el MINTIC.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad, Utilizando la Herramienta de Diagnostico brindada por el MINTIC.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación Utilizando la Herramienta de Diagnostico brindada por el MINTIC.	Gerencia Dirección Administrativa y Financiera Encargado TI	

Objetivos del diagnostico

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

Fase de Planificación

La entidad, utilizara los resultados obtenidos en la fase de diagnóstico para proceder a elaborar el Plan de Seguridad de la Información

En la fase de planificación del MSPI en EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P se pretende alcanzar las siguientes metas:

- **Meta 1:** Política de seguridad y privacidad de la información.
- **Meta 2:** Procedimientos de Seguridad de la información.
- **Meta 3:** Roles y Responsabilidades de Seguridad y Privacidad de la Información.
- **Meta 4:** Inventario de activos de información.
- **Meta 5:** Integración del MSPI con el Sistema de Gestión documental.
- **Meta 6:** Identificación, Valoración Y Tratamiento de Riesgos.
- **Meta 7:** Plan de Comunicaciones.
- **Meta 8:** Plan de Transición de IPv4 a IPv6.

Actividad	Responsable	Fecha
Crear la Política de General Seguridad y Privacidad de la Información, basada en la Guía No. 2 Política General MSPI.	Gerencia Dirección Administrativa y Financiera Encargado TI	

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

Crear las Políticas Específicas de Seguridad y privacidad de la información, de acuerdo la Guía No. 2 Política General MSPI.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Establecer y documentar los Procedimientos de seguridad de la información, teniendo como referencia la Guía No. 3 Procedimientos de Seguridad y Privacidad de la Información.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Definir Roles y responsabilidades de seguridad y privacidad de la información, de acuerdo a la Guía 4 Roles y Responsabilidades	Gerencia Dirección Administrativa y Financiera Encargado TI	
Levantar el Inventario de activos de información, de acuerdo a la Guía No. 5 Gestión de Activos y la Guía No. 20 Transición de IPV4 a IPV6 .	Gerencia Dirección Administrativa y Financiera Encargado TI	
Realizar la Integración del MSPI con el Sistema de Gestión documental, tomando como referencia la Guía No. 6- Gestión Documental.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Realizar la Identificación, Valoración y tratamiento de riesgo. Según la Guía No. 7 Gestión de Riesgos	Gerencia Dirección Administrativa y Financiera	

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

y la Guía No. Controles de seguridad.	Encargado TI	
Elaboración del plan de tratamiento de Riesgos.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Establecer el Plan de Comunicaciones. Siguiendo los lineamientos dados en la Guía No. 14. Plan de Comunicación, Sensibilización y capacitación.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Crear un Plan de diagnóstico de IPv4 a IPv6, como lo indica la Guía No. 20. Transición IPv4 a IPv6.	Gerencia Dirección Administrativa y Financiera Encargado TI	

Fase de implementación

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa de Planificación y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad.

En la fase de implementación se realizan las siguientes metas de acuerdo al resultado de la planeación.

- **Meta 1:** Planificación y Control Operacional

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

- **Meta 2:** Implementación del plan de tratamiento de riesgos
- **Meta 3:** indicadores De Gestión
- **Meta 4:** Plan de Transición de IPv4 a IPv6

Actividad	Responsable	Fecha
Realizar la Planificación y Control Operacional. Para esto se debe realizar de acuerdo a la Guía No 9 - Indicadores de Gestión.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Implementar el plan de tratamiento de riesgos en la entidad., de acuerdo a la Guía No 9 - Indicadores de Gestión.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Generar Indicadores De Gestión. Teniendo como base la Guía No 9 - Indicadores de Gestión.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Implementar el Plan de Transición de IPv4 a IPv6, siguiendo los lineamientos de la Guía de Transición de IPv4 a IPv6 para Colombia” y “Guía de Aseguramiento del Protocolo IPv6	Gerencia Dirección Administrativa y Financiera Encargado TI	

Fase de Evaluación y Desempeño

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

Las metas para esta fase de evaluación del desempeño se realizan las siguientes metas:

- **Meta 1:** Plan de revisión y seguimiento a la implementación del MSPI.
- **Meta 2:** Plan de Ejecución de Auditorias.

Actividad	Responsable	Fecha
Hacer el Plan de revisión y seguimiento, a la implementación del MSPI.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Siguiendo los lineamientos de la Guía No 16 – Evaluación del desempeño.	Gerencia Dirección Administrativa y Financiera Encargado TI	
Realizar el Plan de Ejecución de Auditorias, con base en la Guía No 15 – Guía de Auditoría.	Gerencia Dirección Administrativa y Financiera Encargado TI	

Fase de Mejora Continua

En esta fase la entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

En esta fase es importante que la entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
- Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

Actividad	Responsable	Fecha
Crear el Plan de mejora continua, con base en los resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua	Gerencia Dirección Administrativa y Financiera Encargado TI	
Realizar el Plan de Ejecución de Auditorías, con base en la Guía No 15 – Guía de Auditoría.	Gerencia Dirección Administrativa y Financiera Encargado TI	

Adopción del Protocolo IPV6

La EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P saben que para cumplir el objetivo de innovación tecnológica debe iniciar el proceso de transición del protocolo IPv4 al nuevo protocolo IPv6, para esto se debe revisar que la infraestructura con la que cuenta actualmente soporte el protocolo IPv6, en caso de no ser así realizar cambio de ella. Garantizar que todos los equipos de telecomunicaciones acepten en un 100% este protocolo. Además, en lo relacionado con los proveedores de servicios de conectividad deben proveerlo con total compatibilidad a IPv6. La infraestructura nueva debe estar diseñada para coexistir con el protocolo IPv4.

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5 Versión: 1
---	---	---

9. Guías Modelo de Seguridad y Privacidad de la Información

Los siguientes documentos brindados por el MINTIC serán tenidos en cuenta en la implementación del Modelo de Seguridad y Privacidad de la Información en la EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P

Modelo de Seguridad y Privacidad de la Información

Instructivo Herramienta de Diagnostico

Herramienta de Diagnostico

Guía Mi pymes

Guía 1	Metodología de pruebas de efectividad
Guía 2	Política General MSPI v1
Guía 3	Procedimientos de Seguridad y Privacidad de la Información
Guía 4	Roles y responsabilidades de seguridad y privacidad de la información
Guía 5	Gestión de Activos
Guía 6	Gestión Documental
Guía 7	Gestión de Riesgos
Guía 8	Controles de Seguridad
Guía 9	Indicadores Gestión SI
Guía 10	Continuidad de TI
Guía 11	Impacto Negocio
Guía 12	Seguridad en la Nube
Guía 13	Guía De Evidencia Digital
Guía 14	Plan de comunicación, sensibilización y capacitación
Guía 15	Auditoria
Guía 16	Evaluación del Desempeño
Guía 17	Mejora Continua
Guía 18	Lineamientos terminales de áreas financieras entidades públicas
Guía 19	Aseguramiento del protocolo IPV6
Guía 20	Transición IPv4 IPv6
Guía 21	Gestión de Incidentes

10. Plan de Comunicación

El Plan de seguridad y privacidad de la información, será comunicado a todos los funcionarios de EMPRESA DE SERVICIO EL RETIRO – RETIRAR S.A.E.S.P a través de

	EMPRESA DE SERVICIOS DE EL RETIRO RETIRAR S.A. E.S.P. NIT 811028985-3.	Código: G - 300.05.5.5
		Versión: 1

los mecanismos como son página web de la entidad, donde se publicará en el ítem de transparencia y derecho de acceso a la información pública para que todos los usuarios puedan acceder, se enviara a través de correo electrónico, grupo interno de WhatsApp y capacitación de socialización a todos los funcionarios de la entidad.