SAION
SMART SOLUTIONS

Manual del Sistema de Gestión de Seguridad de la información

Preparado por

Responsable del documento	**Rol en el proyecto/organización**
Eliana Gómez	Coordinadora de Calidad

Historial de cambios

Versión	**Estado**	**Fecha**	**Código**	**Autor**	**Descripción**
1.00	Pendiente		GS-Man.01	Eliana Gómez	Creación del Documento

Aprobado por

Nombre	**Rol en el proyecto/organización**	**Versión aprobada**	**Fecha aprobación**
Vasny Fonnegra	Director Administrativo	1.00	

Tipo y Responsables del Documento

Tipo de Documento	**Propietario**	**Custodio**	**Responsable**
Reservado	Vasny Fonnegra Directora Administrativa y Financiera	Eliana Gómez Coordinadora de Calidad	Jheison Urzola Técnico en Seguridad de la Información

Contenido

1. INTRODUCCIÓN 6
2. PRESENTACIÓN DEL MANUAL 6
   - 2.1 Objetivo del Manual 6
   - 2.2 Alcance del Manual 7
3. CONTEXTO DE LA ORGANIZACIÓN 7
   - 3.1 Reseña histórica 7
   - 3.2 Misión 8
   - 3.3 Visión 8
   - 3.4 Objetivos Estrategicos 8
   - 3.5 Determinación de las partes Interesadas 9
   - 3.6 Objetivos del SGSI 10
   - 3.7 Alcance del SGSI 10
4. TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN 10
5. MARCO LEGAL APLICABLE 12
6. POLITICA DE SEGURIDAD DE LA INFORMACIÓN 13
   - 6.1 Política de Seguridad de la información 14
   - 6.2 Política de Roles y Responsabilidades 14
   - 6.3 Política Contacto con Autoridades 20
   - 6.4 Política de Trabajo Remoto o Teletrabajo 20
   - 6.5 Política de Seguridad del Recurso Humano 21
   - 6.6 Política de Escritorio y pantalla Limpia 22

6.7 Política de Equipos de Usuarios desatendidos 22

6.8 Política de Seguridad de la información con proveedores (Colaboradores de Saion con contrato por prestación de servicios) 22

6.9 Política Protección de la Información y Copias Seguras 23

6.10 Política de Buenas Prácticas de Seguridad de la Información 23

6.11 Política de protección de datos personales 24

7. CAPACITACIÓN DEL PERSONAL EN SEGURIDAD DE LA INFORMACIÓN 24

8. GESTIÓN DE RIESGOS 24

9. CULTURA DE SEGURIDAD DE LA INFORMACIÓN 25

9.1 Plan de Conciencitización 25

9.2 Plan de Comunicaciones 25

10. GESTIÓN Y MANEJO DE LA INFORMACIÓN DOCUMENTADA 26

10.1 Inventario de Activos: 26

10.2 Clasificación de la Información: 26

10.3 Uso y devolución de los activos y activos de información: 26

10.4 Manejo de la información: 27

10.5 Almacenamiento de la Información 28

10.6 Encriptación de la Información 28

10.7 Protección de la Información de Registro 28

10.8 Transferencia de la Información 29

11. ACCESO Y GESTIÓN DE LOS SISTEMAS DE INFORMACIÓN 29

11.1 Asignación de Usuario y Permisos 29

11.2 Acceso a los Sistemas de Información 30

11.3 Disponibilidad y Capacidad de la Organización respecto a Seguridad de la Información 30

11.4 Gestión de Cambios 30

11.5 Gestión de amenazas, Vulnerabilidades e Incidentes de Seguridad de la información ... 30

12. GESTIÓN Y MANTENIMIENTO DE EQUIPOS 31

13. PERÍMETRO DE SEGURIDAD 31

13.1 Controles Áreas de Acceso Seguro 32

14. SEGURIDAD DE LA INFORMACIÓN EN LOS PROYECTOS 32

15. SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL SERVICIO 33

16. IDENTIFICACIÓN DE REQUISITOS LEGALES 33

17. SEGUIMIENTO Y EVALUACIÓN DEL DESEMPEÑO DEL SGSI 33

17.1 Auditoria Interna 34

17.2 Inspecciones de Seguridad a los Sistemas de Información 34

17.3 Tratamiento y Cierre de No Conformidades y Acciones Correctivas 35

17.4 Comité de Seguridad de la Información (SGSI) 35

17.5 Revisión Independiente del SGSI 35

18. MEJORA CONTINUA DEL SGSI 35

1. INTRODUCCIÓN

La creación de este Manual del Sistema de Gestión de la Información responde a la necesidad de la organización de darle un carácter de obligatoriedad al cumplimiento de las directrices, políticas y prácticas contenidas en él, las cuales constituyen parte fundamental del modelo de Seguridad de la información de la organización.

A partir de la divulgación de este manual se pretende realizar planes de sensibilización que conlleven a que colaboradores, contratistas, y terceros que tengan relación contractual o acceso a los activos de información de **SAION SMART SOLUTIONS S.A.S** interioricen estas permitiendo así salvaguardar la confidencialidad, integridad y disponibilidad de la información.

La elaboración de este manual se realizó con base en los controles y requisitos identificados en la norma ISO 27001:2013 y la guía técnica ISO 27001:2015.

2. PRESENTACIÓN DEL MANUAL

2.1 Objetivo del Manual

El objetivo de este manual es describir, establecer y difundir las políticas, procesos, procedimientos, directrices y prácticas con que colaboradores, contratistas, terceros o cualquier persona que tenga una relación contractual o acceda a los activos de información de **SAION SMART SOLUTIONS S.A.S** actúe con el fin de preservar la confidencialidad, integridad y disponibilidad de la información, permitiendo así, implementar y mantener un SGSI eficaz.

Adicional a lo anterior, con este manual se espera suministrar las bases documentales para las auditorias de certificación.

2.2 Alcance del Manual

El presente Manual del Sistema de Gestión Seguridad de la Información pretende describir las políticas, directrices y procesos de la organización orientados a darle cumplimiento al alcance del SGSI, el cual, es la “Gestión de la seguridad de la información y activos del ciclo de vida del servicio de Consultoría, Soporte Técnico y Funcional, Mantenimiento, Mesa de Servicio, Desarrollo y Testing de Software, Automatización de Procesos y Reclutamiento de Personal enfocado en la plataforma SAP Cloud y OnPremise; y que son de obligatorio cumplimiento por parte de colaboradores, contratistas y terceros involucrados.

3. CONTEXTO DE LA ORGANIZACIÓN

3.1 Reseña histórica

Saion Smart Solutions nació en el año 2012 bajo el nombre de Covertixe digital siendo su principal objeto la prestación de servicios en la interfaz gráfica para los clientes y en segundo lugar la Consultoría SAP, comenzó en la sala de su representante legal acompañada de 3 empleados y un contador, en el año 2016 en el mes de febrero se toma la decisión de cambiar el nombre de la compañía por Saion Smart Solutions y fortalecer la prestación de servicios de Consultoría SAP poniéndolo como su principal objeto, para lo cual se formaliza la relación de Partner con SAP, obteniendo el PARTNER EDGE SILVER de SAP. Bajo este objeto se comienza en el 2016 con el primer cliente privado teniendo una gran acogida y abriéndonos paso en licitaciones públicas para lograr ser reconocidos.

En el año 2017, Saion se certifica en el modelo de calidad IT Mark lo cual nos hizo crecer como empresa, ser más visibles en el mercado y entre nuestros competidores por las buenas prácticas de calidad y constancia en nuestros procesos organizacionales, no contentos con esto y teniendo en cuenta uno de nuestros principios, la “mejora continua”, en el año 2019 logramos la certificación en CMMI SVC nivel 3, modelos de calidad reconocido mundialmente, haciendo de Saion una compañía llamativa por su implementación y mantenimiento de los procesos, procedimientos y calidad en la prestación de sus servicios de Consultoría SAP. En el año 2020 Saion motivado por su mejora continua y apoyado de un gran equipo interdisciplinario, logró obtener la calificación CMMI SVC nivel 5, lo cual ha contribuido a mejorar de manera significativa los procesos organizacionales, la calidad en la prestación del servicio, el reconocimiento y buena calificación entre sus clientes y la oportunidad para participar en más procesos de

contratación tanto públicos como privados antes ignorados por no contar con modelos internacionales de calidad.

3.2 Misión

SAION SMART SOLUTIONS S.A.S es una organización de soluciones integrales de tecnología, que a través del uso óptimo de las Tecnologías de la Información y las Comunicaciones (TICs), brinda a los clientes soluciones para el mejoramiento continuo de los procesos y aumento de la productividad, a través de la permanente formación del talento humano, la transparencia, calidad y experiencia.

3.3 Visión

En el 2023 **SAION SMART SOLUTIONS S.A.S** será reconocida por sus clientes y aliados estratégicos como una organización que fomenta:

- La formación del talento humano especializado y de calidad como estrategia de desarrollo profesional y empresarial.
- La implementación y certificación de modelos de calidad reconocidos internacionalmente.
- El desarrollo de productos propios que respondan a las necesidades particulares del sector público y privado.
- La calidad en el servicio como valor agregado.

3.4 Objetivos Estrategicos

- Promover un ambiente de bienestar que favorezca el desarrollo integral de los colaboradores.
- Fomentar el mejoramiento continuo respecto al desempeño laboral, relaciones interpersonales, comunicación, liderazgo, innovación y competencia de los colaboradores.

- Crear y difundir la imagen corporativa a nivel interno.
- Crecer nacionalmente.
- Internacionalizar la prestación de servicios de la organización.
- Posicionar y difundir la identidad corporativa a nivel externo.
- Implementar y certificar modelos calidad reconocidos internacionalmente.
- Entregar soluciones integrales e innovadoras a través del fortalecimiento de las líneas de negocio y la conformación de alianzas estratégicas.
- Mejorar la posición competitiva de la organización respecto a otras del sector.
- Incrementar la percepción de valor en el cliente.
- Incrementar las utilidades de la compañía.
- Maximizar la inversión.
- Incrementar la adopción de controles de seguridad de la información que permitan reducir el impacto y la probabilidad de materialización de los riesgos asociados con amenazas y vulnerabilidades de la confidencialidad, la integridad y la disponibilidad de los activos de la información de **SAION** y sus clientes.

3.5 Determinación de las partes Interesadas

SAION para identificar las partes interesadas internas y externas que intervienen y afectan la consecución de los objetivos previstos del SGSI. Ha determinado que a partir de la estructuración de la matriz DOFA documentada en el formato **Frm_Matriz DOFA** identificó sus debilidades, oportunidades, fortalezas y amenazas concernientes a la organización y en relación con seguridad de la información estableciendo para ello el procedimiento **Prc_ Análisis del Contexto de la Organización.**

3.6 Objetivos del SGSI

- Generar cultura de seguridad de la información en los colaboradores de la organización por medio del levantamiento de buenas prácticas del SGSI para dar un tratamiento de riesgos adecuado a las necesidades de la compañía por medio de estrategias de capacitaciones, revista empresarial, despliegue, entre otros.

- Alinear los esfuerzos del SGSI con los objetivos por medio de actividades orientadas a la norma ISO 27001/IEC:2013 para apalancar la estrategia organizacional por medio del seguimiento de la alta gerencia.

- Aumentar las ventas en un 10% sobre las metas comerciales del año por medio de estrategias de marketing digital que resalten las bondades del cumplimiento de la norma ISO 27001 para aumentar la rentabilidad de la compañía.

- Incrementar la cobertura de activos y de controles de seguridad de la información en los sistemas de gestión humana, ambientes de desarrollo, calidad y productivo que permita reducir el impacto de que se materialicen los riesgos asociados con las amenazas y vulnerabilidades identificadas en los sistemas de información de Saion para aumentar la confianza en colaboradores y clientes.

3.7 Alcance del SGSI

Gestión de la seguridad de la información y activos del ciclo de vida del servicio de Consultoría, Soporte Técnico y Funcional, Mantenimiento, Mesa de Servicio, Desarrollo y Testing de Software, Automatización de Procesos y Reclutamiento de Personal enfocado en la plataforma SAP Cloud y OnPremise. Conforme a la declaración de la aplicabilidad vigente.

4. TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes términos y definiciones están basados en las Referencias Normativas: ISO 27000 aplicados en la ISO27001.

Alta Gerencia: Se entiende como Alta Gerencia al propietario y representante legal de la organización y al director de Proyectos.

Parte Interesada: Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.

Propietario: Se entiende como la alta gerencia quien es la propietaria de toda la información que se procesa sobre la organización.

Custodio: Se entiende como la persona responsable dentro de la organización de administrar y versionar el repositorio de almacenamiento y gestión de la información OneDrive de la organización.

Responsable: Se entiende como la persona responsable de gestionar, actualizar y transferir los activos de información asignados a el proceso del cual es responsable.

Seguridad de información: Preservación de la confidencialidad, integridad y disponibilidad de la información

Amenaza: Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas

Riesgo: Es el efecto (la desviación de lo esperado (negativo o positivo) de la incertidumbre (deficiencia, incluso parcial, de la información relacionada, la comprensión o el conocimiento de un evento, su consecuencia y probabilidad) sobre lo objetivos.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Aceptación de riesgo: Decisión de asumir un riesgo.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

Activo: cualquier elemento que represente valor para la organización.

Integridad: Propiedad de la exactitud y la integridad de la información.

Disponibilidad: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada

Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados

Política: Intenciones y dirección de una organización, según lo expresado formalmente por su alta dirección

Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Gerencia con el objetivo de garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

5. MARCO LEGAL APLICABLE

SAION identifica los requerimientos legales de obligatorio cumplimiento con base en el contexto de la organización y sus sistemas de gestión de información conforme al procedimiento **Prc_ Identificación de Requisitos Legales** y los documenta en el formato **Frm_ Matriz legal Integrada.**

Las leyes y requerimientos legales identificados son:

- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 1915 de 12 de julio de 2018 – Nuevas disposiciones en materia de Propiedad Intelectual - Derechos de Autor.
- Ley 1032 de 2006 - Disposiciones generales para el manejo de información de datos personales (Habeas Data).
- Decreto 1360, de 23 de junio de 1989, por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor.
- Ley 527 de 1999, por 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 2364 de 2012, firma electrónica.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley Estatutaria 1581 de 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de los datos personales.
- Ley 1581 de 2012, "Protección de Datos personales".
- Directiva Presidencial Nº 03 de 15 de marzo de 2021. Lineamientos para el uso de servicios en la nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.

- Ley 1341 de 30 de julio de 2009 - Principios y conceptos sobre la Sociedad de la Información y la Organización de las Tecnologías de la Información y las Comunicaciones.
- Decreto 1078 de 26 de mayo de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

6. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

En **SAION SMART SOLUTIONS S.A.S** se establece el documento **Po_Manejo de Seguridad de la Información** que contiene las políticas de seguridad de la información establecidas por la Alta Gerencia con el fin de demostrar que **estamos comprometidos con la implementación de estrategias y mecanismos de gestión de seguridad de la información, asumiendo la responsabilidad de disminuir el impacto generado sobre sus activos y toda la información sensible de los clientes y de la compañía, manteniendo un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de los mismos, para mejorar la confianza, transparencia y calidad de los servicios prestados en nuestra operación con prácticas estandarizadas y promoviendo la mejora continua.**

Estas políticas serán revisadas por el comité directivo y de SGSI anualmente o cuando se identifiquen cambios significativos que afecten las políticas, se dejará acta de la revisión con las aprobaciones de las políticas si se realiza modificaciones, oportunidades de mejora, entre otros.

Se realizará auditoría interna de manera anual, al sistema de gestión de la seguridad de la información, a sus interesados y activos de información con base en la política de aseguramiento de la calidad PPQA establecida y conforme al plan de auditorías establecido por el área de calidad de la compañía.

Las políticas contenidas en este documento son las siguientes y pueden ser consultadas en su totalidad en el documento **Po_Manejo de Seguridad de la Información**:

- Política de Seguridad de la información
- Política de Roles y Responsabilidades
- Política de Contacto con Autoridades y Grupos de Interés
- Política de Trabajo Remoto o Teletrabajo
- Política de Seguridad del Recurso Humano
- Política de Escritorio y pantalla Limpia
- Política de Equipos de Usuarios Desatendidos

- Política de Seguridad de la información con proveedores (Colaboradores de Saion con contrato por prestación de servicios)
- Política de Copias Seguras
- Política de Buenas Prácticas de Seguridad de la Información
- Po_Manejo Datos Personales (Habeasdata)

6.1 Política de Seguridad de la información

En **SAION** estamos comprometidos con la implementación de estrategias y mecanismos de gestión de seguridad de la información, asumiendo la responsabilidad de disminuir el impacto generado sobre sus activos y toda la información sensible de los clientes y de la compañía, manteniendo un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de los mismos, para mejorar la confianza, transparencia y calidad de los servicios prestados en nuestra operación con prácticas estandarizadas y promoviendo la mejora continua.

6.2 Política de Roles y Responsabilidades

En **SAION** se establece, define y asigna 3 roles para determinar las responsabilidades y autoridades con relación a seguridad de la información. Los cuales son:

- ***Técnico en Seguridad (responsable de la Seguridad de la Información):*** Personal con estudios previos y certificados en seguridad como "Security Fundamentals. El cual vela por que la información, los activos de información y equipos de la compañía estén en óptimas condiciones y en un correcto funcionamiento. Entre sus principales funciones se encuentra:

  - Velar porque cada equipo tenga instalado sistema operativo y software licenciados.
  - Asignación de usuarios único corporativo.
  - Velar por el cumplimiento del mantenimiento de los equipos
  - Verificar la realización e integridad de los backups, entre otras.

- ***Responsable secundario de la seguridad de la información:*** Personal que apoya al Técnico en seguridad de la información, vela por el cumplimiento de las funciones del personal con relación a seguridad de la información y otorga los

permisos de acceso al personal a los sistemas de información de **SAION**. Entre sus principales funciones se encuentra:

- Velar por que los colaboradores estén cumpliendo con sus responsabilidades de seguridad frente al equipo asignado.
- Velar porque se cumpla el mantenimiento de los equipos en la fecha establecida en el inventario y asignación de equipos.
- Realizar los backups de la información contenida en drive.
- Otorgar permisos al personal conforme a las directrices de asignación de permisos por rol contenidas en el formato **Frm AsignaciónPermisos_Rol.**

- ***Colaboradores:*** Personal administrativo y operativo de la organización que tenga asignado un equipo de esta para la ejecución de sus labores y acceso privilegiado o restringido al sistema de información de **SAION**. Entre sus funciones principales se encuentra:

  - Velar por la integridad del equipo asignado por la compañía, y en caso de requerir modificaciones o identificar anomalías en el equipo, reportarlas oportunamente al responsable secundario.
  - Manejo y uso adecuado de la información de la organización y terceros a la que tenga acceso conforme a la política de manejo de seguridad de la información.
  - Reportar eventos, incidentes o anomalías de seguridad de la información al personal autorizado o autoridad competente conforme al procedimiento **Prc_ Reporte de Eventos o Incidentes de Seguridad de la Información**

Las autoridades determinadas por la Alta Gerencia correspondientes a cada rol en la organización son las siguientes:

Cargo	Rol	Responsabilidades	Autoridad
Arquitecto SAP	Técnico en Seguridad Director de Proyectos Consultor Arquitecto SAP	• Velar que cada equipo tenga tanto sistema operativo como hardware y software licenciados. • Asignar usuarios únicos a cada colaborador y consultor de la compañía. • Instalar el antivirus Avast o Windows defender en cada equipo. • Velar que se cumpla el protocolo de no instalar programas no licenciados. • Velar que se cumpla el mantenimiento a los equipos. • Verificar que se realicen los backups establecidos.	• Asignar usuarios • Asignar permisos • Generar directrices sobre buenas prácticas para la seguridad de la información. • Aprobar nuevos productos. • Definir modificaciones al SGSI • Modificar, borrar, añadir carpetas, archivos, formatos, etc. • Definir los recursos y controles requeridos para la gestión de incidentes. • Definir controles para proteger la información. • Definir controles para seguridad física de

		• Participar con la alta dirección en la definición y planeación de controles. • Velar que los colaboradores cumplan con sus responsabilidades de seguridad frente al equipo y activos. • Verificar el estado del equipo que es regresado de nuevo a la compañía.	equipos. • Implementar controles de acceso a la información • Definir personas a contratar. • Tomar acciones en caso de violaciones a la SI.
Director Administrativo y financiero	Responsable secundario de la seguridad de la información.	• Velar por que los colaboradores estén cumpliendo con sus responsabilidades de seguridad frente al equipo asignado. • Velar porque se cumpla el mantenimiento de los equipos. • Solicitar al área administrativa y/o al responsable principal los software o programas cuando estos sean requeridos por los colaboradores. • Realizar los backups de la información contenida en drive. • Informar al área administrativa y al técnico en seguridad cualquier anomalía. • Otorgar permisos en las carpetas que contienen la información de acuerdo con el archivo AsignaciónPermisos_Rol. • Velar porque se llene el registro de retiros de equipos establecido por la compañía conforme a lo establecido en estas políticas, cuando corresponda.	• Asignar permisos de acceso a la información. • Generar directrices sobre buenas prácticas para la seguridad de la información. • Aprobar nuevos productos. • Definir modificaciones al SGSI • Modificar, borrar, añadir carpetas, archivos, formatos, etc. • Interactuar con proveedores (Colaboradores por prestación de servicios), entre otros. • Definir mecanismos para divulgar, sensibilizar y comprometer al personal en la SI. • Definir personas a contratar. • Tomar acciones en caso de violaciones a la SI. •
Directora de Talento Humano	Colaborador administrativo con acceso privilegiado	• Contratación y Selección de personal. • Gestión SGSST. • Cuidado físico del equipo asignado por la compañía. • Manejo adecuado de la información y uso de esta conforme a la política establecida para Manejo de la información. • Transporte del equipo, cuando se requiere movilizar a sitios diferentes del habitual, debe solicitar autorización al responsable de seguridad de la información por medio de los canales dispuestos para la comunicación (Correo electrónico). • No instalar software o programas no licenciado. • Podrá instalar software o programas de uso libre, previa autorización. • Solicitar al técnico en seguridad o al responsable secundario la instalación de cualquier software que requiera adquisición por parte de la compañía. • Informar cuando su equipo es víctima de un virus o el antivirus haya puesto el equipo en cuarentena por una amenaza de virus. • Informar cuando su equipo presente daño físico o de software para su correcto tratamiento y entrega temporal de otro equipo. • Informar si conoce el caso de un acceso no autorizado a la información de Saion o de sus clientes por parte de un tercero o un miembro del equipo que no deba tener acceso a esa	• Generar directrices sobre buenas prácticas para la seguridad de la información. • Búsqueda en base de datos de antecedentes. • Definir mecanismos para sensibilizar y comprometer al personal en la SI. • Ajustar la documentación del SGSI en lo relacionado a la gestión de talento humano. • Definir personas a contratar. • Tomar acciones en caso de violaciones a la SI conforme a lo establecido en el reglamento interno y los acuerdos confidenciales. • Modificar, borrar, añadir carpetas, archivos, formatos, etc en gestión de talento humano.

		información. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (Policía, Bomberos) si se tiene conocimiento de un ataque a las instalaciones de Saion. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (policía, bomberos, ejercito, DAGRD) si se tiene conocimiento o presencia eventos como incendio, inundaciones, derrumbes que ponga en riesgo las instalaciones o bienes de la compañía.	
Coordinadora de Calidad	Colaborador administrativo con acceso privilegiado	• Gestión de procesos empresariales. • Gestión de proceso PPQA • Cuidado físico del equipo asignado por la compañía. • Manejo adecuado de la información y uso de esta conforme a la política establecida para Manejo de la información. • Transporte del equipo, cuando se requiere movilizar a sitios diferentes del habitual, debe solicitar autorización al responsable de seguridad de la información por medio de los canales dispuestos para la comunicación (Correo electrónico). • No instalar software o programas no licenciado. • Podrá instalar software o programas de uso libre, previa autorización. • Solicitar al técnico en seguridad o al responsable secundario la instalación de cualquier software que requiera adquisición por parte de la compañía. • Informar cuando su equipo es víctima de un virus o el antivirus haya puesto el equipo en cuarentena por una amenaza de virus. • Informar cuando su equipo presente daño físico o de software para su correcto tratamiento y entrega temporal de otro equipo. • Informar si conoce el caso de un acceso no autorizado a la información de Saion o de sus clientes por parte de un tercero o un miembro del equipo que no deba tener acceso a esa información. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (Policía, Bomberos) si se tiene conocimiento de un ataque a las instalaciones de Saion. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (policía, bomberos, ejercito, DAGRD) si se tiene conocimiento o presencia eventos como incendio, inundaciones, derrumbes que ponga en riesgo las instalaciones o bienes de la compañía.	• Generar directrices sobre buenas prácticas para la seguridad de la información. • Definir mecanismos para divulgar, sensibilizar y comprometer al personal en la SI. • Ajustar la documentación del SGSI. • Modificar, borrar, añadir carpetas, archivos, formatos, etc en los procesos organizacionales, gestión de calidad, gestión de la seguridad. • Generación de contenido.
Coordinador de Proyectos	Colaborador Administrativo con acceso privilegiado	• Gestión de proyectos. • Cuidado físico del equipo asignado por la compañía. • Manejo adecuado de la información y uso de	• Generar directrices sobre buenas prácticas para la seguridad de la información. • Definir mecanismos para divulgar, sensibilizar y comprometer al personal en la SI.

		esta conforme a la política establecida para Manejo de la información. • Transporte del equipo, cuando se requiere movilizar a sitios diferentes del habitual, debe solicitar autorización al responsable de seguridad de la información por medio de los canales dispuestos para la comunicación (Correo electrónico). • No instalar software o programas no licenciado. • Podrá instalar software o programas de uso libre, previa autorización. • Solicitar al técnico en seguridad o al responsable secundario la instalación de cualquier software que requiera adquisición por parte de la compañía. • Informar cuando su equipo es víctima de un virus o el antivirus haya puesto el equipo en cuarentena por una amenaza de virus. • Informar cuando su equipo presente daño físico o de software para su correcto tratamiento y entrega temporal de otro equipo. • Informar si conoce el caso de un acceso no autorizado a la información de Saion o de sus clientes por parte de un tercero o un miembro del equipo que no deba tener acceso a esa información. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (Policía, Bomberos) si se tiene conocimiento de un ataque a las instalaciones de Saion. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (policía, bomberos, ejercito, DAGRD) si se tiene conocimiento o presencia eventos como incendio, inundaciones, derrumbes que ponga en riesgo las instalaciones o bienes de la compañía.	• Ajustar la documentación del SGSI en la dirección de proyectos. • Modificar, borrar, añadir carpetas, archivos, formatos, etc en los procesos organizacionales, gestión de proyectos, gestión misional
Contadora	Colaborador Administrativo con Acceso privilegiado	• Gestión de procesos financieros. • Emisión de facturas • Cuidado físico del equipo asignado por la compañía. • Manejo adecuado de la información y uso de esta conforme a la política establecida para Manejo de la información. • Transporte del equipo, cuando se requiere movilizar a sitios diferentes del habitual, debe solicitar autorización al responsable de seguridad de la información por medio de los canales dispuestos para la comunicación (Correo electrónico). • No instalar software o programas no licenciado. • Podrá instalar software o programas de uso libre, previa autorización. • Solicitar al técnico en seguridad o al responsable secundario la instalación de cualquier software que requiera adquisición por parte de la compañía. • Informar cuando su equipo es víctima de un virus o el antivirus haya puesto el equipo en	• Generar directrices sobre buenas prácticas para la seguridad de la información del área. • Modificar, borrar, añadir carpetas, archivos, formatos, etc en la gestión financiera. • Presentar información financiera a las entidades que lo soliciten.

		cuarentena por una amenaza de virus. • Informar cuando su equipo presente daño físico o de software para su correcto tratamiento y entrega temporal de otro equipo. • Informar si conoce el caso de un acceso no autorizado a la información de Saion o de sus clientes por parte de un tercero o un miembro del equipo que no deba tener acceso a esa información. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (Policía, Bomberos) si se tiene conocimiento de un ataque a las instalaciones de Saion. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (policía, bomberos, ejercito, DAGRD) si se tiene conocimiento o presencia eventos como incendio, inundaciones, derrumbes que ponga en riesgo las instalaciones o bienes de la compañía.	
Consultores	Colaborador Consultor y operativo con acceso restringido	• Cumplimiento de su asignación o requerimiento en el cliente, conforme a su especialidad. • Cuidado físico del equipo asignado por la compañía. • Manejo adecuado de la información y uso de esta conforme a la política establecida para Manejo de la información. • Transporte del equipo, cuando se requiere movilizar a sitios diferentes del habitual, debe solicitar autorización al responsable de seguridad de la información por medio de los canales dispuestos para la comunicación (Correo electrónico). • No instalar software o programas no licenciado. • Podrá instalar software o programas de uso libre, previa autorización. • Solicitar al técnico en seguridad o al responsable secundario la instalación de cualquier software que requiera adquisición por parte de la compañía. • Informar cuando su equipo es víctima de un virus o el antivirus haya puesto el equipo en cuarentena por una amenaza de virus. • Informar cuando su equipo presente daño físico o de software para su correcto tratamiento y entrega temporal de otro equipo. • Informar si conoce el caso de un acceso no autorizado a la información de Saion o de sus clientes por parte de un tercero o un miembro del equipo que no deba tener acceso a esa información. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (Policía, Bomberos) si se tiene conocimiento de un ataque a las instalaciones de Saion. • Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (policía, bomberos,	• Acceso de lectura a las carpetas asignadas según su rol dentro del repositorio de Saion.

		ejercito, DAGRD) si se tiene conocimiento o presencia eventos como incendio, inundaciones, derrumbes que ponga en riesgo las instalaciones o bienes de la compañía.	

6.3 Política Contacto con Autoridades

En **SAION** se establece el procedimiento **Prc_ Reporte de Eventos o Incidentes de Seguridad de la Información** para el reporte de incidentes o eventos de seguridad de la información donde se describe las directrices a seguir en estos casos, y cual, es el orden de escalamiento respecto de la competencia, si con autoridades internas o entidades competentes externas. Dicho reporte será efectuado por cualquier parte interesada por medio del formato **Reporte de incidente o eventos de Seguridad de la Información**

6.4 Política de Trabajo Remoto o Teletrabajo

SAION ha establecido el teletrabajo para aquellos colaboradores para los cuales así se requiera, esto se establece de acuerdo con lo dispuesto en la Ley 1221 de julio 16 de 2008 reglamentado por el Decreto 0884 del 30 de abril de 2012 respecto al TELETRABAJO. Las disposiciones y desglose de las características del teletrabajo se encuentran consignadas en el reglamento interno de trabajo en el Capítulo 1 – Teletrabajo, en los artículos 90 al 96.

Así mismo **SAION** establece la realización de trabajo remoto (Trabajo en casa) cuando por causas de fuerza mayor propia, del entorno o de orden y/o salud pública no se puedan desplazar a las instalaciones de **SAION** o de sus clientes o por estas mismas causas no se pueda usar dichas instalaciones, se realizará trabajo remoto desde su lugar de residencia hasta nueva orden.

Todo lo relacionado al teletrabajo se encuentra consignado en el **Est_Reglamento Interno de Trabajo**. Adicional se cuentan con el estándar de **Est_Guías para definir Estándares de Entorno de Trabajo** que establece los estándares para el puesto de trabajo en caso de desarrollar trabajo remoto o teletrabajo.

En cuanto al compromiso de promover buenas prácticas de seguridad de la información en caso de desarrollar trabajo remoto o teletrabajo, se estable el estándar **Est_Guía para**

el uso de las TIC's (Vinculados) y **(Contratistas)**, tanto para empleados como para contratistas, con el fin de salvaguardas la integridad, confidencialidad y disponibilidad de la información que es tratada en las estaciones de trabajo remotas.

6.5 Política de Seguridad del Recurso Humano

En **SAION** se establecen directrices para asegurar condiciones seguras en cuanto al manejo y acceso de la información durante el proceso de contratación del nuevo personal de la organización para ellos establece los siguientes parámetros:

Selección: Se establece que durante el proceso de selección de personal se requiera la presentación de antecedentes legales, disciplinarios, judiciales y referencias laborales a los aspirantes con el fin de verificar que el nuevo personal de la organización cumple con el perfil definido para ser parte de esta. Para lo cual, se estableció el procedimiento **Prc_Reclutamiento y Selección de Colaboradores y Contratistas.**

Términos y condiciones de ingreso y retiro de la organización: Se establece que dentro de los documentos contractuales que son leídos, firmados y aceptados por empleados y contratistas con los cuales se pretende dar carácter de obligatoriedad en el cumplimiento las buenas prácticas de seguridad de la información establecidas por **SAION**:

- Declaración de confidencialidad
- Acuerdo de confidencialidad (Contratistas)
- Autorización de tratamiento de datos personales
- Manual de funciones
- Reglamento interno

Adicional en caso de retiro o reasignación de proyecto del personal de **SAION** se aplica lo definido en la política, el proceso de transición del servicio (SST) y con lo establecido en el acuerdo de confidencialidad para el manejo de la información, activos de información y transferencia de esta.

Proceso Disciplinario: **SAION** establece criterios para aplicación del procedimiento disciplinario por motivo de la violación o incumplimiento a los acuerdos, responsabilidades, deberes y obligaciones de los colaboradores relacionadas a la seguridad de la información entre otros. Por lo cual, dentro del Reglamento Interno de Trabajo se describe en los capítulos XV, XVI y XVIII, las faltas y sanciones disciplinarias y

en el procedimiento **Prc Disciplinario** se describen las actividades necesarias para la aplicación de sanciones, entre otras.

6.6 Política de Escritorio y pantalla Limpia

SAION define que cada colaborador debe mantener el escritorio y pantalla libre de elementos que puedan ser susceptibles de pérdida o sustracción de información. El escritorio en el que cada colaborador trabaja debe estar libre de dispositivos extraíbles que contengan información que pueda ser clasificada y sensible. Al igual que la pantalla de su computador debe estar libre de documentos que contenga información de carácter privado, confidencial o reservado. Estos deben estar almacenados conforme al documento **Po_Política de almacenamiento proyectos** y al **Frm_Plan de Administración de la Configuración.**

6.7 Política de Equipos de Usuarios desatendidos

SAION define que cada colaborador debe brindarle la protección necesaria a su equipo cuando este no vaya a ser usado por un tiempo y que no se pueda realizar un apagado total, para esto cada colaborador tanto en teletrabajo, trabajo en casa o presencial, debe realizar el bloqueo de su equipo cuando este vaya a estar solo y sin atención del colaborador, permitiendo así que solo el colaborador pueda activarlo nuevamente por medio del usuario y contraseña o pin, adicional a esto si se realizan transacciones en las que se intercambia información valiosa de la compañía o de los clientes, debe de asegurarse de cerrar cada cesión si no se va a realizar procesos o ejecuciones por un tiempo prolongado o si el colaborador se debe ausentar por un tiempo determinado.

6.8 Política de Seguridad de la información con proveedores (Colaboradores de Saion con contrato por prestación de servicios)

Se define para el manejo y seguridad de la información con los proveedores, que se realizará con base en la clasificación de la información definida por **SAION** y la establecida por sus clientes, se generará soporte contractual de la relación entre las partes con sus obligaciones y acuerdos con respecto a la seguridad de la información a la que se tendrá acceso durante la relación. Las especificaciones de obligatorio cumplimiento sobre seguridad de la información se encuentran contenidas en las

cláusulas y recomendaciones de los documentos **Frm_Contrato de Prestación de Servicios PN,** el **Frm_Declaración de confidencialidad** y **Est_Guía para el uso de las TIC's (Vinculados)** y **(Contratistas)** respectivamente.

6.9 Política Protección de la Información y Copias Seguras

Toda la información que maneja **SAION** está contenida en la nube en la herramienta One Drive; esta herramienta permite realizar el backup en línea de la información registrada y una continua actualización de la información contenida.

Para la información Administrativa se define realizarse los backup's semanalmente en línea y mediante disco externo fuera de la oficina, para garantizar de esta manera que la información pueda ser recuperada en caso de cualquier eventualidad y pérdida de la información.

Las copias se realizan de manera automática en la nube y en el disco externo de manera automática por el Sistema Operativo Windows 10 Profesional. Esta actividad se deja registrada en el **Plan de backups** donde se indica la fecha de la copia, el responsable de la configuración para realizar la copia, ubicación de las copias, fecha de la próxima copia, observaciones si se requiere, fecha de revisión, quien revisa la copia, nombre de la copia y descripción general de la información que contiene.

Adicional, las directrices para la creación y gestión de las copias de forma segura se encuentran contenidas en el documento **Est_Creación y Gestión de Backups.**

6.10 Política de Buenas Prácticas de Seguridad de la Información

En **SAION** en función del compromiso que se tiene con la promoción y adopción de buenas prácticas sobre seguridad de la información por parte de todo su personal (vinculado y contratista) en el manejo previo, durante y posterior de la información de la organización y sus clientes. Define la guía **Est_Guía para el uso de las TIC's (Vinculados)** y **(Contratistas)** de carácter de cumplimiento obligatorio para todos los miembros de la organización con el fin de dar cumplimiento a las buenas prácticas establecidas.

6.11 Política Manejo Datos Personales (Habeasdata)

En **SAION** con el fin de dar cumplimiento a la a la Ley 1581 de 2012 sobre el tratamiento de datos personales, se define y establece la política de **Po_Manejo Datos Personales (Habeasdata)** para indicarle a los interesados la forma como la organización dará tratamiento adecuado a los datos personales que sean otorgados a la organización motivo de la relación contractual que se establezca con las partes interesadas.

Adicionalmente, se establece que los interesados que nos proporcionen datos personales debido a labores o servicios prestados a la organización motivo del ejercicio del negocio, autorizarán la utilización y los términos de uso y protección que se le darán a sus datos, firmando el formato **Frm_Autorización de tratamiento de datos personales.**

7. CAPACITACIÓN DEL PERSONAL EN SEGURIDAD DE LA INFORMACIÓN

Se establece que conforme al proceso **Capacitación organizacional (OT)** se definen las necesidades de capacitación del personal de **SAION**, entre ellas, la formación idónea en seguridad de la información al personal encargado de gestionar el SGSI para la correcta ejecución de las labores propias de este. Adicional, la formación a todo el personal, sobre buenas prácticas de seguridad de la información dentro de la ejecución de sus labores con el fin de desarrollar una cultura organizacional orientada a salvaguardar la integridad, confidencialidad y disponibilidad de la información de la organización y clientes.

8. GESTIÓN DE RIESGOS

En **SAION** al momento de planificar el SGSI se prioriza la identificación, análisis y valoración de los riesgos asociados a seguridad de la información relacionados con el contexto de la organización y las expectativas internas y externas. Así mismo, se estructura, establece y valora las estrategias para su reducción, transferencia o mitigación. Con el fin de lograr lo anterior, la organización define el estándar **Est_Estandar Guía para la gestión del Riesgo,** el cual, contiene la descripción detallada de la metodología empleada por la organización para la gestión de los riesgos. Y esta

metodología es documentada en el formato **Frm_Plan de Administración de Riesgos. (e**ste formato se aplica tanto a nivel organizacional como en los proyectos por separado).

Adicional a la gestión de los riesgos asociados a la seguridad de la información, también la organización, identifica, analiza y valora los riesgos relacionados con los activos de información base en el mismo estándar **Est_Estandar Guía para la gestión del Riesgo** y documentada su aplicación en la Matriz **Frm_Matriz de Activos de Información.**

9. CULTURA DE SEGURIDAD DE LA INFORMACIÓN

9.1 Plan de Conciencitización

En **SAION** estamos comprometidos con el desarrollo de una cultura organizacional que incluya buenas prácticas de seguridad de la información en el actuar diario de nuestros miembros. Por lo tanto, la organización ha definido un plan de concientización basado en la capacitación, sensibilización e importancia que la adopción de buenas prácticas de seguridad de la información nos aporta como organización y a cada miembro de está en su vida personal.

El plan de concientización se planifica y ejecuta anualmente y consiste en la elaboración de cartillas, publicación de información de interés, actualidad y directrices de la organización en la revista interna, socialización de políticas, estándares y directrices en los sprint review organizacionales, impartir capacitaciones internas y externas sobre seguridad de la información, ciberseguridad, entre otros temas relacionados. El cual se encuentra documentando en la estándar **Est_Plan de concientización.**

9.2 Plan de Comunicaciones

SAION ha definido un plan de comunicaciones para establecer las directrices adecuadas para la transferencia de información de forma interna y externa con base en la asignación de permisos por rol en el repositorio, las autoridades delegadas por la alta gerencia en el manejo de la información de **SAION** y el enfoque de salvaguardar la integridad, confidencialidad y disponibilidad de la información que se determinó debe ser comunicada a las partes interesadas, tanto de manera organizacional como en los proyectos.

Para ello, se estableció el estándar **Est_Estandar Plan de Comunicación Organizacional,** que contienen las directrices de cómo se define qué, quién y por qué medio se comunica la información. Adicional se establecieron los formatos **Frm_Plan de**

Comunicación Organizacional y **Frm_Plan de Comunicación Proyectos** para documentar las necesidades de comunicación correspondientes.

10. GESTIÓN Y MANEJO DE LA INFORMACIÓN DOCUMENTADA

En **SAION** se identifica los activos de información y se clasifican conforme a su naturaleza e importancia para la organización. Así mismo se asignan las responsabilidades respecto al cuidado y manejo de cada uno de ellos.

Para tal efecto se define lo siguiente:

10.1 Inventario de Activos:

Se elabora un inventario de activos en el formato **Frm_ Matriz de Activos de Información** de acuerdo con el tipo o naturaleza del activo (documento, equipo, licencia, entre otros) y se le asigna las responsabilidades respecto a este (propietario, custodio y responsable) conforme al formato de **Frm_Plan de Administración de la Configuración.**

10.2 Clasificación de la Información:

Se define la clasificación de la información conforme a su condición de disponibilidad e importancia para la organización y considerando las reglamentaciones legales y normativas para el cuidado y protección de información de terceros que se capta en la organización. Para tal fin, en el formato **Frm Plan de Administración de la Configuración** se describen los criterios para clasificar la información (Pública, reservada, confidencial y privada); y se cuenta con el formato **Frm_Listado maestro de documentos** en el cual se documenta por activo de información (artefacto y productos de procesos) la clasificación de cada activo de información bajo los anteriores criterios.

10.3 Uso y devolución de los activos y activos de información:

Todo equipo y activo de información deberá ser utilizado para el desarrollo del objeto del negocio bajo las políticas establecidas para equipos y manejo de información que se establecen en este documento. Todo equipo y activo de información al finalizar contrato se debe realizar la respectiva devolución al jefe inmediato o director de talento humano a si mismo al finalizar contrato se realizará el respectivo bloqueo a los permisos asignados.

10.4 Manejo de la información:

SAION define para la información digital que sea almacenada en la nube en drive (sistema de información), a la cual se accede por medio usuarios únicos asignados "correo electrónico único corporativo" con la clave segura asignada por cada uno de los usuarios y a través de claves asignadas por el responsable de seguridad del área a los archivos que contengan información clasificada como privada. Los protocolos para la creación de contraseñas de acceso seguro a la nube se definieron en el procedimiento **Prc_ Gestión de información secreta para la autenticación de usuarios** y los definidos por el mismo sistema de información de Microsoft OneDrive.

Para el manejo de la información una vez autorizado el acceso a esta, se define la guía **Est_Guía para el uso de las TIC's (Vinculados)** y **(Contratistas)** que contiene las buenas prácticas de seguridad de la información que tanto vinculados y contratista deben acatar para dar cumplimiento al compromiso del SGSI de salvaguardar la integridad, confidencialidad y disponibilidad de la información.

Adicional cada colaborador tiene asignadas las siguientes funciones frente a su equipo y los activos de información, las cuales se encuentran también descritas en su manual de funciones:

- Manejo adecuado de la información y uso de esta conforme a la política establecida para Manejo de la información.
- Informar al técnico en seguridad de la información y representante legal si conoce el caso de un acceso no autorizado a la información de **SAION** o de sus clientes por parte de un tercero o un miembro del equipo que no deba tener acceso a esa información.
- Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (Policía, Bomberos) si se tiene conocimiento de un ataque a las instalaciones de **SAION**.
- Informar al técnico en seguridad de la información o comunicarse directamente con las autoridades de control (policía, bomberos, ejercito, DAGRD) si se tiene conocimiento o presencia eventos como incendio, inundaciones, derrumbes que ponga en riesgo las instalaciones o bienes de la compañía.

Por otro lado, se establece el estándar **Est_Guia de instalación y uso del software Keepass para la gestión segura de contraseñas** con el fin de utilizar el software de uso libre **keepass_2** para mantener encriptada las contraseñas de los usuarios únicos

asignados para cada miembro de la organización, y disminuir el acceso no autorizado a los sistemas de información del SAION por mal manejo y guardado de las contraseñas.

10.5 Almacenamiento de la Información

En **SAION** la mayoría de su documentación se almacena de manera digital en el OneDrive. Sin embargo, la documentación física se encuentra almacenada en azetas y bajo llave; dependiendo de su contenido es custodiada por la Directora de Talento Humano, Contadora o la Directora Administrativa y Financiera.

Las directrices para el almacenamiento de la información también dependen de su contenido. Para el área de proyectos se cuenta con el documento **Po_Política_de almacenamiento_proyectos** y para el resto de la información se cuenta con el documento **Frm_Plan de Administración de la Configuración.**

10.6 Encriptación de la Información

En **SAION** se define que la información propia de la organización contenida como copias de seguridad en los discos externos será encriptada para salvaguardar la integridad y confidencialidad de esta. El proceso de encriptación se realizará de acuerdo con las directrices contenidas en la **Est_Creación y Gestión de Backup's.**

Por otro lado, para la información de nuestros clientes se realizará el proceso de encriptación a petición de cada uno de ellos y según lo que se estipule en el acuerdo de nivel de servicio.

10.7 Protección de la Información de Registro

SAION define el procedimiento **Prc_ Protección de la información de registro** con el fin de salvaguardar la información de registro de los Sistemas de información de **SAION** contra alteraciones y accesos no autorizados.

Por otro lado, se establece el estándar **Est_Guia_de_instalación_y_uso_del_sofware Keepass para la gestión segura de contraseñas** con el fin de utilizar el software de uso libre **keepass_2** para mantener encriptada las contraseñas de los usuarios únicos

asignados para cada miembro de la organización, y disminuir el acceso no autorizado a los sistemas de información del SAION por mal manejo y guardado de las contraseñas.

10.8 Transferencia de la Información

En **SAION** se define que la transferencia de información entre la organización con terceros (clientes, proveedores y contratistas) se realizará únicamente por medio de Office 365 y sus aplicaciones asociadas (teams, outlook, AzureDevos, sharepoint, entre otras) bajo los protocolos y políticas de seguridad y cifrado de información establecidos por Microsoft para este servicio.

Adicional, para la firma y legalización de documentos tales como contratos, acuerdos, entre otros con personal interno y terceros (clientes, proveedores y contratistas) se utilizará únicamente el servicio de Abode Sign el cual está certificado de acuerdo con la ISO 27001, SSAE SOC 2 Tipo 2, FedRAMP Tailored y PCI DSS. Además, Adobe Sign se puede configurar o usar de manera que permita a las organizaciones cumplir con los requisitos normativos específicos del sector, como HIPAA, FERPA, GLBA y FDA 21 CFR Parte 11.

11. ACCESO Y GESTIÓN DE LOS SISTEMAS DE INFORMACIÓN

11.1 Asignación de Usuario y Permisos

En **SAION** los accesos y permisos a la información están establecidos teniendo en cuenta el rol y la clasificación de la información, estos permisos se encuentran consignados en el formato **Frm AsignaciónPermisos Rol.** Estos accesos al sistema de información de **SAION** OneDrive son asignados por el Técnico en Seguridad y el responsable secundario, y son retirados al finalizar el contrato de la persona que tenga el acceso o ajustado si este pasa a otro cliente o área conforme al procedimiento **Prc Registro y cancelación del registro de usuarios**.

11.2 Acceso a los Sistemas de Información

En **SAION** se les otorga un usuario único asignado por el Técnico en Seguridad de la información a empleados, contratistas y proveedores que lo requieran conforme al **Prc Gestión de usuarios.** Con este usuario podrán ingresar al repositorio OneDrive y demás aplicaciones asociadas a Office 365 (Outlook, teams, AzureDevops, Planner, entre otras), donde podrán disponer de toda la información necesaria para la prestación de su servicio o labor de forma segura y adecuada a su rol de acuerdo con lo definido en el procedimiento de **Prc Gestión de información secreta para la autenticación de usuarios.**

11.3 Disponibilidad y Capacidad de la Organización respecto a Seguridad de la Información

En **SAION** se define la estrategia de Disponibilidad y Capacidad de la organización en el formato **Frm_Estrategia de Capacidad y Disponibilidad Organizacional,** conforme al proceso **Gestión de capacidad y disponibilidad (CAM).** Mediante el cual se detalla las estrategias y recursos de los que se dispone la organización para atender las interrupciones que impacten la ejecución de las actividades del SGSI o incidentes de seguridad sobre los sistemas de información de Saion.

11.4 Gestión de Cambios

Se define para la gestión de cambios, que este sea realizado bajo los parámetros, procesos y procedimientos adoptados por la compañía para la continuidad del servicio, entre los cuales se encuentra, continuidad del servicio, plan de transición, gestión de cambios, entre otros, para asegurar el paso de la información de manera segura, la continuidad de la prestación del servicio y disminución en los impactos generados por los cambios efectuados.

11.5 Gestión de amenazas, Vulnerabilidades e Incidentes de Seguridad de la información

En **SAION** se define que por medio del formulario **Reporte de incidente o eventos de Seguridad de la Información** que estará disponible a través de la página web de Saion, los colaboradores, proveedores, contratistas o clientes podrán reportar las amenazas, vulnerabilidades e incidentes de seguridad de la información que sean identificados dentro

de los sistemas de información de SAION. Este formulario será recibido conforme a lo establecido en el procedimiento **Prc_ Reporte de Eventos o Incidentes de Seguridad de la Información** y revisado por el comité de SGSI quien analizará y evaluará la situación reportada conforme a lo establecido en el proceso **Resolución y prevención de incidencias (IRP),** documentando la gestión y resolución del evento en el formato **Frm_Reporte de Incidencias.**

12. GESTIÓN Y MANTENIMIENTO DE EQUIPOS

SAION tiene activos los cuales están identificados y asignados a los colaboradores como se encuentra documentado en el formato **Frm_ Matriz de Activos de Información.**

Para la gestión de los activos Saion ha definido la guía **Est_Gestión de Equipos** en la cual establece los parámetros para gestionar los equipos tales como:

- Codificación de los equipos
- Ubicación
- Alimentación Ininterrumpida
- Mantenimiento y Actualización
- Retiro de equipos
- Reutilización y Eliminación de equipos

13. PERÍMETRO DE SEGURIDAD

Se establece para las instalaciones de **SAION**, que estas contarán con estándares de seguridad en vigilancia, monitoreo, controles de acceso entre otros para brindar amplio margen de seguridad a los activos físicos que se encuentren en las instalaciones.

Adicional a esto también cuenta con cámaras de seguridad en portería, en el perímetro externo, en las zonas comunes como parque y zonas de tránsito vehicular dentro de la unidad las cuales son monitoreadas constantemente por el personal de vigilancia.

También se encuentra conectado con el cuadrante 20 de la policía metropolitana con los números de contacto 3005612133 – 3006173177.

13.1 Controles Áreas de Acceso Seguro

Se establece para el ingreso a las instalaciones de SAION, controles de acceso físico que se debe aplicar a cada visitante antes de ser aprobado su ingreso. Por ello se cuenta con portería con servicio 7/24 donde los visitantes deben anunciar su ingreso para ser aprobado por SAION, adicional se maneja una bitácora donde se registra los datos personales del visitante que ha sido anunciado y aprobado para su ingreso.

Dentro de las instalaciones de SAION se cuentan con servidores para la ejecución de las actividades del área administrativas los cuales son accedidos remotamente por medio de claves y VPNs seguras y archivero con llave para el almacenamiento de la información física de la organización.

14. SEGURIDAD DE LA INFORMACIÓN EN LOS PROYECTOS

En **SAION** estamos comprometidos con gestionar la seguridad de la información como parte del alcance de los proyectos a partir de la gestión de riesgos y el establecimiento de controles de seguridad que nos permitan salvaguardar la integridad, confidencialidad y disponibilidad de la información de la organización y sus clientes. Para ello establece el procedimiento **Prc_Guía Seguridad Información Gestión de Proyectos** que contiene las directrices para la adopción de buenas prácticas de seguridad de la información en el desarrollo de los proyectos.

Adicional se implementa controles de seguridad desde el área de Talento Humano que son de obligatorio cumplimiento por parte de vinculados y contratistas que prestan servicios a nuestros clientes, como son los documentos, **Frm Declaración de confidencialidad** respectivamente que contiene cláusulas de confidencialidad y medidas sancionatorias en caso de incumplimiento de las cláusulas anteriores.

Como último medio de control para promover buenas prácticas de seguridad de la información entre nuestros colaboradores (vinculados y contratistas) se define la guía **Est_Guía para el uso de las TIC's (Vinculados)** y **(Contratistas),** la cual contiene buenas prácticas de seguridad de la información que deben ser consideradas en la ejecución de las labores de todo nuestro personal.

15. SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL SERVICIO

En Saion de cuenta con el proceso **Pro_Continuidad del Servicio** y el estándar **Est_Guías para definir el Plan de Continuidad del Negocio** analizar y determinar los planes de continuidad del Servicio respecto a las funciones, procesos y activos de información críticos para la operación del negocio. Estos planes son documentados en el formato **Frm_Plan de Continuidad del Negocio**

Para realizar un análisis adecuado se cuenta con el procedimiento **Prc_Análisis de Impacto del Negocio**, por medio del cual se establecen las directrices pertinentes para identificar las funciones, procesos y activos de información críticos para la operación del negocio, el nivel de criticidad, los riesgos implícitos, la determinación de los tiempos de recuperación, recursos y procesos alternos que permitan darle continuidad a la operación del negocio de manera segura. Este análisis es documentado en el formato **Frm_Análisis de Impacto del Negocio.**

Posteriormente a la definición de los planes de continuidad en los proyectos y a nivel organizacional estos se evalúan a través del formato **Frm_Plan de Pruebas Plan de Contingencia,** para determinar su nivel de efectividad, recoger lecciones aprendidas y realizar los ajustes necesarios para asegurar la continuidad del servicio y operación del negocio.

16. IDENTIFICACIÓN DE REQUISITOS LEGALES

En Saion se define el procedimiento **Prc_ Identificación de Requisitos Legales** para analizar, evaluar y definir las leyes, normativas y reglamentaciones en materia seguridad de la información en Colombia que nos apliquen conforme al contexto de la organización. Con el fin de ser adoptadas y dar cumplimiento a los requisitos legales exigidos. Lo anterior, se documenta en la **Frm_Matriz Legal Integrada.**

17. SEGUIMIENTO Y EVALUACIÓN DEL DESEMPEÑO DEL SGSI

Se establece para la evaluación del desempeño del SGSI realizar monitoreo a través del proceso **OPP (Desempeño del Proceso Organizacional)**, mediante el cual se realiza seguimiento al desempeño de la organización estableciendo indicadores de desempeño de las diferentes áreas y sistemas de gestión que se encuentran establecidos en la organización; que en materia de seguridad de la información, se realiza seguimiento a los indicadores organizacionales enfocados en seguridad de la información de manera mensual a través de los sprint organizacionales y se documenta ello en el formato **Frm Informe de Monitoreo Áreas Proceso Organizacionales**. Adicional, semestralmente el líder del SGSI presenta a la Alta gerencia un informe de monitoreo detallado sobre el desempeño del SGSI el cual se documenta en el formato **Informe de Monitoreo SGSI**.

17.1 Auditoria Interna

Se define que anualmente se realizará auditoría conforme al proceso **Pro Aseguramiento de la Calidad** y el procedimiento **Prc Plan de Aseguramiento de la Calidad**, con el fin de verificar el cumplimiento de las actividades propias del SGSI y el nivel de adherencia a las buenas prácticas de seguridad de la información establecidas por el SGSI.

17.2 Inspecciones de Seguridad a los Sistemas de Información

Se define y establece que las inspecciones a los sistemas de información de **SAION** son realizadas por el proveedor Microsoft al Sistema de información Office 365, como parte de sus procesos de calidad internos. Por lo cual, la organización se acoge a estos protocolos de pruebas de estrés, inspecciones y verificaciones que garanticen el correcto funcionamiento de la nube y la efectividad y eficiencia de los controles de seguridad implementados por el proveedor.

Estas inspecciones y pruebas de seguridad son consultadas mensualmente en la página:

https://bit.ly/3pr2KsJ

Se realizarán algunas pruebas de seguridad previamente aprobadas según la necesidad por el comité del SGSI atendiendo los siguientes protocolos:

https://bit.ly/3vrd1c8

17.3 Tratamiento y Cierre de No Conformidades y Acciones Correctivas

SAION define que mediante el proceso **Pro_Aseguramiento de la Calidad** y el procedimiento de **Prc_Seguimiento y Cierre de No Conformidades y Acciones Correctivas** se realizará el seguimiento y se les dará el tratamiento adecuado a las No conformidades identificados en las auditorías internas.

17.4 Comité de Seguridad de la Información (SGSI)

SAION establece la creación formal del Comité de SGSI mediante el acta **Frm_Acta Constitución Comité Seguridad de la Información**; con el fin de disponer de un equipo interdisciplinario que apoye el cumplimiento, realice seguimiento, verifique el rendimiento del SGSI.

Así mismo realice la evaluación y defina los tratamientos que se les dará a los eventos de seguridad de la información que presencié la organización.

Para definir el alcance del comité y su proceder la Alta Gerencia estableció el reglamento **Est_Reglamento Comité Seguridad de la Información**, donde se describen las lineamientos, responsabilidades y autoridades respecto al funcionamiento del comité.

17.5 Revisión Independiente del SGSI

SAION define que anualmente realizará auditoría externa con la institución ICONTEC para verificar el cumplimiento de los lineamientos de la norma ISO 27001 y su guía técnica ISO 25002, con el fin de mantener un sistema de Seguridad de la información certificado y actualizado.

18. MEJORA CONTINUA DEL SGSI

En la organización contamos con un proceso para realizar monitoreo y desempeño de los procesos, como **OPP (Desempeño del Proceso Organizacional)** mediante el cual se está verificando la consecución de los **QPPO'S (Objetivos establecidos de desempeño del proceso)** y así identificar las desviaciones negativas que se presentan durante el

desarrollo de los procesos y poder establecer los planes de acción necesarios para encaminar los resultados de los procesos a los resultados esperados de estos.

Por otro lado, se dispone del **proceso CAR (Análisis Causal y Resolución)** cuando las desviaciones negativas impactan considerablemente el desempeño del proceso, área o la prestación de los servicios de la organización. Por medio de este proceso se realiza la evaluación de las desviaciones basada en metodologías y estrategias enfocadas en encontrar la causa raíz de la desviación y así poder mitigarla o eliminar con el fin de evitar su repetición.

Adicional, se tiene establecido el proceso **OPF (Enfoque en procesos de la organización)** mediante el cual, se están recogiendo lecciones aprendidas y buenas prácticas con el fin de estar en la continua identificación de mejoras a los procesos organizacionales y sistemas de gestión establecidos en la organización, y de esta manera, asegurar la continua mejora de todos los procesos.