



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Publico

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

1.	Introducción.....	2
2.	Alcance/Aplicabilidad	2
3.	Nivel de cumplimiento.....	3
4.	Glosario.....	3
4.1	Activos de información:	3
4.2	Confidencialidad:.....	3
4.3	Disponibilidad:.....	3
4.4	Integridad:	3
4.5	Riesgo:	3
4.6	SGSI:.....	3
4.7	Vulnerabilidad:	3
5.	Objetivos	4
6.	Uso Aceptable de Recursos Tecnológicos.....	5
6.1	Se considera uso no aceptable de recursos tecnológicos:.....	6
7.	Uso de Internet	7
7.1	No está permitido en Internet	7
8.	Uso del Correo Electrónico.....	8
9.	Control de Acceso Físico.....	9
10.	Segregación de Tareas	9
11.	Controles Contra el Código Malicioso	10
12.	Copias de Seguridad de la Información.....	10
13.	Gestión de medios extraíbles	10
14.	Gestión de contraseñas de usuario	10
15.	Controles Criptográficos	11
16.	Política de puesto de trabajo despejado y protección de pantalla ..	11
17.	Notificación de Incidentes	11
18.	Sanciones para las violaciones a las Políticas de Seguridad de la Información	12
19.	VIGENCIA	13



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Publico

1. Introducción

La dirección de **Smart Data & Automation SAS**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para **Smart Data & Automation SAS**, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

Los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Smart Data & Automation SAS
- Garantizar la continuidad del negocio frente a incidentes.

2. Alcance/Aplicabilidad

El SGSI debe cubrir todos los activos de información, plataformas tecnológicas y procesos en **Smart Data & Automation SAS**. Buscando la preservación de los activos de información asociados al desarrollo de aplicaciones automatizadas, y el desarrollo a la medida, con presencia a nivel LATAM de acuerdo con la declaración de aplicabilidad aprobada el 23 de septiembre d 2021.



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Publico

Esta política aplica a toda la compañía, sus empleados, terceros, aprendices, practicantes y proveedores sin excepción.

3. Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento en un 100% de la política.

4. Glosario

4.1 Activos de información: bases de datos, documentación física y digital, software, hardware, equipos de comunicación, servicios informáticos y de comunicaciones, infraestructura (iluminación, energía, aire acondicionado, etc.) y las personas (son quienes generan, transmiten y destruyen información).

4.2 Confidencialidad: La propiedad de que esa información esté disponible y no sea divulgada a individuos, entidades o procesos no autorizados.

4.3 Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

4.4 Integridad: Propiedad de la información relativa a su exactitud y completitud.

4.5 Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

4.6 SGSI: Sistema de Gestión de la Seguridad de la Información

4.7 Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

5. Objetivos

Smart Data & Automation SAS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Dentro de las temáticas que se tocan en la política se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, copias de seguridad, infraestructura en la nube y acceso a la información, lo cual estableció como principios necesarios e importantes los siguientes conceptos:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- **Smart Data & Automation SAS** protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en Outsourcing.
- **Smart Data & Automation SAS** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- **Smart Data & Automation SAS** protegerá su información de las amenazas originadas por parte del personal.
- **Smart Data & Automation SAS** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- **Smart Data & Automation SAS** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- **Smart Data & Automation SAS** implementará control de acceso a la información, sistemas y recursos de red.
- **Smart Data & Automation SAS** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Publico

- **Smart Data & Automation SAS** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- **Smart Data & Automation SAS** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- **Smart Data & Automation SAS** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6. Uso Aceptable de Recursos Tecnológicos

- Se considera uso adecuado de los recursos, la utilización legal y ética de estos para apoyar las labores propias de los empleados de acuerdo con la misión y visión de la compañía.
- Deben ser usados racionalmente evitando el uso ineficiente de los mismos.
- Los empleados de **Smart Data & Automation SAS** utilizarán los recursos tecnológicos para tratamiento de la información requerida para el desempeño de las labores asignadas.
- Los datos e información creada, relacionada con las operaciones propias de la compañía deberán ser almacenados de manera estricta en dispositivos y sistemas de información pertenecientes a **Smart Data & Automation SAS**.
- Todos los datos e información, sin importar su clasificación, relacionados con las operaciones propias de la compañía, son de propiedad exclusiva de **Smart Data & Automation SAS** y deberá solicitarse permiso por medio formal cuando se requiera realizar operaciones de manipulación de estos y que se extralimiten de las líneas base de las operaciones propias de las labores asignadas a cada colaborador.
- Los procesos que requieran la generación de documentación deberán ser realizados, de manera estricta, teniendo en cuenta que la información privada del cliente pertenece de forma exclusiva al cliente, por lo cual no se deben incluir dentro de la documentación compartida con terceros, información que haga



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Publico

referencia a temas tecnológicos, comerciales o administrativos que sean propios de la operación de los clientes.

- El uso de los recursos de la compañía tiene el único propósito de apoyar los procesos asignadas a cada empleado de **Smart Data & Automation SAS**.

6.1 Se considera uso no aceptable de recursos tecnológicos:

- El uso de los activos tecnológicos con fines personales, lúdicos o de lucro para el usuario.
- La transmisión de contenido que resulte incómodo para los otros empleados o que atente contra los valores y la ética de la compañía.
- La transmisión de cualquier información difamatoria que afecte tanto el contexto interno como externo de la compañía.
- El uso y la transmisión de material electrónico violando derechos de propiedad intelectual.
- El inicio de sesión en activos con credenciales de autenticación ajenas.
- El uso excesivo de los recursos, para fines no relacionados con las labores asignadas causando lentitud en los objetivos misionales.
- El uso de software malicioso para generar degradación de los activos de información de la compañía o de terceros.
- El uso de software licenciado no autorizado en los equipos de la compañía.
- El uso de equipos personales en la red de la compañía sin previa autorización.
- El uso de tecnologías de almacenamiento externo, sin la debida autorización de los empleados a cargo del SGSI de la compañía.
- Las acciones que causen detrimentos en las funciones y tareas de otros usuarios de la compañía o de terceros.



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Publico

- El proporcionar usuarios, contraseñas o cualquier otro tipo de credenciales de accesos a personal no autorizado por la compañía.
- Cualquier acción vandálica que cause degradación en los activos de información de la compañía.
- La reubicación de activos, así como conexión o desconexión de estos sin autorización de la Gerencia Técnica y de Proyectos.
- La modificación de los equipos de escritorio, portátiles y/o dispositivos móviles a nivel sistema operativo, sin autorización de la Gerencia Técnica y de Proyectos.
- La manipulación de las bases de datos internas o pertenecientes a los clientes sin autorización de la Gerencia Técnica y de Proyectos.

7. Uso de Internet

Internet es un recurso que apoya la ejecución de las labores propias de los empleados de **Smart Data & Automation SAS**.

7.1 No está permitido en Internet

- El acceso a todo tipo de páginas que vayan en contravía de los valores y la ética de la compañía como son páginas pornográficas, drogas y alcohol, páginas de hackeo y plataformas de ataques cibernéticos, así como cualquier otra página que vaya en contra de la legislación en general y en especial de las leyes colombianas y/o del país en donde se encuentre laborando.
- El uso de cualquier tipo de software de mensajería instantánea o red social para el intercambio de información (credenciales, información confidencial altamente sensitiva) relacionada con las actividades propias del negocio y de propiedad exclusiva de **Smart Data & Automation SAS** y/o de sus clientes.
- La descarga de todo tipo de material que atente contra la propiedad intelectual como juegos, películas, música, software licenciado, entre otros.



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Público

- El uso e instalación de software licenciado o gratuito que no esté autorizado por la Gerencia Técnica y de Proyectos, al igual que el software licenciado o gratuito que no apoye las labores propias del colaborador, relacionadas con los objetivos misionales de la compañía.
- La instalación y uso de programas P2P (peer-to-peer) para compartir o descargar archivos de internet como son emule, ares, kazaa, entre otros.
- Cada usuario es responsable del uso adecuado de este recurso y no puede ser utilizado para la participación en actividades ilegales o criminales.
- Ningún colaborador puede utilizar el nombre de la compañía a título personal para emitir opiniones en redes sociales, blogs y sitios de opinión similares.

8. Uso del Correo Electrónico

A continuación, se mencionan las directrices para el uso adecuado del correo electrónico:

- El correo corporativo no tiene un carácter privado, la información contenida dentro del buzón es de propiedad de **Smart Data & Automation SAS** y sólo debe conservarse la información relacionada con las funciones propias de cada usuario.
- **Smart Data & Automation SAS** realizará revisiones periódicas del uso del correo corporativo y podrá realizar auditoria del mismo sin previo aviso y cuando lo estime conveniente.
- El correo es de uso corporativo para las labores propias asignadas a cada colaborador de **Smart Data & Automation SAS** y podrá ser utilizado para fines personales siempre que se haga de manera ética y responsable y legal.
- Está prohibido el envío de correo con contenido religioso, político, racista, pornográfico o que vaya en contra de los valores de la compañía, así como cadenas de correo que atenten contra la productividad y el buen nombre de la compañía o de terceros.

- El envío de archivos de video, música y en general cualquier tipo de archivo multimedia, debe estar relacionado con las labores propias de los empleados y siempre respetando los derechos de autor (Copyrigh).
- Cuando exista la necesidad del envío de correos masivos, deben realizarse a través de una cuenta genérica a nombre de un proceso y no a través de la cuenta personal de un usuario y deben ir ocultas las cuentas de correo a las que van dirigidas.
- Está prohibido el envío de credenciales de autenticación, así como de información confidencial altamente sensitiva, en texto plano, este tipo de contenido debe ser enviado de manera cifrada y en formatos no editables.
- El envío de correos y la información contenida en los mismos debe realizarse conservando la identidad corporativa, para lo cual deben utilizarse los diferentes formatos creados por la Control Interno para estos fines y conservando el mensaje legal y de confidencialidad.

9. Control de Acceso Físico

ISO 27001:2013 Anexo A 11.1.2

Las áreas en donde se encuentran ubicados los activos de soporte destinadas al almacenamiento y procesamiento de la información son consideradas como áreas de acceso restringidas. Serán aplicados controles de acceso físico, así como procedimientos que permitan llevar registro de las acciones realizadas sobre estos activos con el fin de prevenir accesos no autorizados o degradación de la información.

10. Segregación de Tareas

ISO 27001:2013 Anexo A 6.1.2

Smart Data & Automation SAS realizará la definición clara de los roles y el nivel de acceso a la información y a los activos de información de acuerdo con las actividades y responsabilidades asignadas a cada colaborador, como son administración, operación, negocios, mantenimiento, auditoria, entre otros. Los niveles con perfil administrador deberán contar con esquema AAA de autenticación.

11. Controles Contra el Código Malicioso

ISO 27001:2013 Anexo A 12.2.1

Todos los activos de información, tanto de infraestructura como sistemas de información deben estar protegidos contra la instalación o intentos de ataques de código malicioso, a través de software antivirus, antimalware, spybot y otros que permitan la prevención, detección y contención de código malicioso. Sólo la Gerencia Técnica y de Proyectos está autorizada para desinstalación o deshabilitación de este tipo de software de protección.

12. Copias de Seguridad de la Información

ISO 27001:2013 Anexo A 12.3.1

La información sensible, definida por cada área, será respaldada a través de copias de seguridad, realizadas periódicamente, estas copias serán sujetas de pruebas de restauración para garantizar que el proceso de respaldo se realice correctamente. Cuando la información sea responsabilidad compartida con terceros, estos deben garantizar la recuperación de esta en caso de que se presente un evento de seguridad de la información.

13. Gestión de medios extraíbles

ISO 27001:2013 Anexo A 8.3.1

Se permite el uso de dispositivos extraíbles a los funcionarios cuyos roles y responsabilidades requieran hacer uso de estos recursos y previa autorización de la Gerencia Técnica y de Proyectos, así mismo el funcionario se compromete a salvaguardar lógica y físicamente el dispositivo. **Smart Data & Automation SAS** establecerá procedimientos para endurecer el uso de estos dispositivos con el fin de disminuir el riesgo de fuga de información por acceso no autorizado o pérdida de estos.

14. Gestión de contraseñas de usuario

ISO 27001:2013 Anexo A 9.4.3



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Publico

Todos los funcionarios o terceros que requieran hacer uso de los recursos de información de **Smart Data & Automation SAS** deberán acceder a través de credenciales de autenticación (Usuario y contraseña) asignados por los administradores de las diferentes plataformas. Cada funcionario o tercero es responsable del buen uso y las tareas ejecutadas bajo sus credenciales.

15. Controles Criptográficos

ISO 27001:2013 Anexo A 10.1

Todos los funcionarios o terceros que requieran hacer uso de información o intercambiar información con **Smart Data & Automation SAS** deberán asegurar su confidencialidad, integridad, autenticidad con el uso adecuado y eficaz de técnicas criptográficas.

16. Política de puesto de trabajo despejado y protección de pantalla

ISO 27001:2013 Anexo A 11.2.9

Todos los funcionarios de **Smart Data & Automation SAS** deben estar comprometidos con la protección de la información sensible a su cargo tanto física como lógica, para lo cual deberán bloquear lógicamente los dispositivos cuando estos se encuentren desatendidos.

Todos los funcionarios deben bloquear las pantallas de sus dispositivos cuando se retiren de ellos, al finalizar la jornada laboral deben cerrar todas las aplicaciones y apagar las estaciones de trabajo.

Todos los dispositivos deben estar programados para bloqueo automático de pantalla máximo cinco minutos después de inactividad.

17. Notificación de Incidentes



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Publico

Toda violación de estas políticas se deberá notificar jefe de seguridad de la información, inmediatamente, a través de la cuenta sgsi@smartdataautormacion.com

Se deberán notificar situaciones tales como:

- Personas ajenas de la organización en centros de cómputo o sistemas informáticos sin la debida autorización.
- Correos con virus, phishing o malware.
- Reinicio de los equipos de cómputo o enrutadores.
- Mala utilización de recursos.
- Uso ilegal del software.
- Mal uso de información corporativa.
- Alteración de información, etc.

18. Sanciones para las violaciones a las Políticas de Seguridad de la Información

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de **Smart Data & Automation SAS**. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información.

Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

El incumplimiento a la Política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: JSI003-1-21

Versión: 01

Fecha: 30 AGOSTO DE 2021

Nivel de Confidencialidad: Publico

19. VIGENCIA

La presente Política rige a partir del 25 de septiembre de 2021.

Versión:1	Elaborado por:	Revisado Por:	Aprobado por:
Firma			
Nombre	Diego Raul Martinez Cetina	Wilmer Humberto Montero	Christian Pérez
Cargo	Jefe de Seguridad de la Información	Gerente de Proyectos y Tecnología	CEO

CONTROL DE CAMBIOS

Fecha	Versión	Descripción
25-09-2021	1	Se publica la primera versión de la Política de Seguridad de la Información para Smart Data & Automation SAS.