1. OBJETIVO

La Política de Seguridad de la Información tiene como objetivos:

El. Establecer lineamientos que permitan a los grupos de interés de green4T seguir estándares de conducta deseables y aceptables en materia de seguridad de la información, actuando de acuerdo con la legalidad y las buenas prácticas globales y con el objetivo de mitigar riesgos técnicos, financieros, administrativos, legales y de imagen/reputación.

B. Orientar la definición de procedimientos específicos de Seguridad de la Información, así como la implementación de controles y procesos para su cumplimiento.

w. Preservar la información de green4T en cuanto a confidencialidad, integridad y disponibilidad.

d. Minimizar los riesgos de pérdida financiera, cuota de mercado, confianza de consumidores y socios o cualquier otro impacto negativo en el negocio de green4T, resultante de una o más brechas de seguridad en sus entornos, especialmente en lo que respecta a los datos producidos, almacenados, procesados o tratados por sus profesionales. , ya sea en formato físico o digital.

Esta Política se complementa con procedimientos y documentos adjuntos, clasificados como confidenciales, que brindan las pautas a seguir en la conducción de los procesos relacionados con esta política, y sirven de referencia para los profesionales a cargo de su ejecución.

2. ALCANCE Este

documento se aplica a todos los Departamentos y empresas afiliadas y controladas de green4T y cubre las normas NBR ISO/IEC 27.001 e ISO/IEC 27.002.

3. TÉRMINOS

a) Autenticidad: Propiedad de que la información fue producida, emitida, modificada o destruida por una determinada persona natural, o por un determinado sistema, organismo o entidad. Trae características de no repudio y garantías de solo modificaciones autorizadas y rastreadas.

b) Confidencialidad: Propiedad de que la información no está disponible o revelada a persona, sistema, organismo, entidad no autorizada y acreditada.

c) Disponibilidad: es la garantía de que la información pueda obtenerse cuando sea necesario, es decir, que esté siempre disponible y utilizable para quienes la necesiten en el ejercicio de sus funciones. Cuando la información no está disponible, los procesos que dependen de ella se paralizan.

d) Integridad: es la garantía de que la información almacenada o transferida es correcta y se presenta íntegra a quien la consulta. Significa que en una comunicación, la información no es modificada, suprimida, destruida de forma no autorizada o accidental en medio del camino entre quien envía la información y quien la recibe. Es una característica crítica desde un punto de vista operativo e indispensable, ya que valida todo el proceso de comunicación en green4T. e) Legalidad: es la garantía de que la información se registra de acuerdo con los procedimientos vigentes, es decir, el uso de la tecnología informática y de comunicación que generó la información es conforme a las leyes vigentes en el lugar o país. Trazabilidad (o Auditabilidad): es la posibilidad de rastrear actualizaciones de información sensible para que, en caso de algún problema, sea posible esclarecer exactamente qué pasó con la información. Hay situaciones en las que se necesitan mecanismos capaces de rastrear el proceso hasta su origen.

g) Usuario: Colaborador o representante (prestador de servicios) que hace uso de los recursos tecnológicos pertenecientes a la empresa.

4. RESPONSABILIDADES

4.1. GERENTE DE TECNOLOGÍA DE LA INFORMACIÓN

a) Gestionar el uso de las tecnologías necesarias para el buen funcionamiento de los negocios de green4T, incluidas las acciones preventivas y el manejo de incidentes, con el fin de promover un mayor nivel de seguridad de la información; b) Realizar acciones dirigidas a cuestiones técnicas relacionadas con gestión de la seguridad de la información;

c) Proponer metodologías y procesos específicos para la Seguridad de la Información, junto con el gerente de Seguridad de la Información, tales como Evaluación de Riesgos; d) Apoyar la evaluación y ~~ad~~ecuación de controles específicos de Seguridad de la Información para nuevos sistemas o servicios, en conjunto con el Comité de Seguridad de la Información; e) Tomar medidas inmediatas para remediar cualquier infracción verificada por el área y cesar inmediatamente el riesgo para green4T, informando inmediatamente al RPD sobre la infracción y las medidas implementadas.

4.2. ÁREA DE PERSONAS

a) Entregar la PL.00.34 - POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN al ingreso a todo empleado o prestador de servicios. b) Entregar y recoger la firma de todo empleado o prestador de servicios al ingreso al PL.00.22 - POLÍTICA DE TECNOLOGÍA DE LA INFORMACIÓN; c) Definir con el gerente de área, el gerente de TI y el gerente de seguridad de la información, los recursos de información necesarios para llevar a cabo las actividades para las cuales fue contratado el empleado o proveedor

(hardware y software);
d) Solicitar el bloqueo del acceso a los sistemas de información de la empresa en caso de despido y cambio de área.

4.3. EMPLEADOS Y TERCEROS PROVEEDORES

Todos los empleados y proveedores de green4T:

a) Se comprometen a cumplir fielmente la Política de Seguridad de la Información, las normas y los procedimientos establecidos en el presente documento, asumiendo el compromiso de observarlos y aplicarlos, así como sometiéndose a las sanciones previstas en las políticas internas y en la legislación aplicable;
b) Acuerdan que todas las operaciones y accesos realizados a través de medios magnéticos son registrados y sujetos a verificación en cualquier momento, independientemente de previo aviso, ya que son herramientas de trabajo, y no es necesario hablar de invasión de la privacidad;

c) Son conscientes de que green4T, de acuerdo con su derecho, puede monitorear todos sus ambientes, ya sean físicos o salas de trabajo; lógicos y/o electrónicos, incluyendo: correo electrónico corporativo, red interna, Internet y Extranet y otros sistemas, almacenando los datos de acceso de cada usuario;

d) Están de acuerdo y reconocen que, en caso de cualquier violación a los términos y condiciones de esta Política, se sujetará a las normas internas y la legislación vigente. También podrá dar lugar al despido por justa causa, de conformidad con lo dispuesto en el artículo 482, inciso “g”, de la Recopilación de Leyes del Trabajo, sin perjuicio de las demás sanciones legales aplicables; e) Son conscientes de que, al término de su relación laboral, o en cualquier momento a solicitud de green4T, deben devolver todos y cada uno de los materiales proporcionados o que contengan Información producida como resultado del contrato de trabajo;

f) Son conscientes de que está prohibida la reproducción de documentos para uso exclusivo de green4T, para cualquier fin, caracterizándose tal actitud como divulgación no autorizada de información confidencial y producción ilícita de prueba;
g) Deben buscar la orientación del gerente de seguridad de la información cuando existan dudas relacionadas con la Seguridad de la Información; h) Deben utilizar una contraseña segura, y deben cambiarla, como periodicidad determinada por green4T;
i) Deben suscribir la PL.00.22 - POLÍTICA DE TECNOLOGÍA DE LA INFORMACIÓN, formalizando la ciencia de la Política y Normas de Seguridad de la Información, así como asumiendo la responsabilidad por su cumplimiento;

j) Debe proteger la información contra el acceso, modificación, divulgación o destrucción no autorizada por parte de green4T;
k) Deben velar por que los recursos tecnológicos se utilicen únicamente

para fines profesionales aprobados y en interés de green4T; l)
Deberán notificar inmediatamente al responsable de seguridad de la información cualquier incumplimiento o violación de esta Política y/o sus Normas y Procedimientos relacionados.

4.4. RESPONSABLE DE

ÁREA Es responsabilidad de todo responsable de área de green4T:

a) Conocer y gestionar los accesos concedidos a los subordinados, siendo, por tanto, indirectamente responsable del mal uso de los mismos.
ellos mismos;
b) Revisar periódicamente a los usuarios con acceso a transacciones críticas bajo su responsabilidad, informando al área de Personas cualquier cambio en el acceso o autorización; c) Tener una actitud ejemplar en relación
con la Seguridad de la Información, sirviendo de modelo de conducta para los empleados a su cargo; d) Cumplir y hacer cumplir esta Política, las Normas y Procedimientos para
Seguridad de la Información;
e) Asegurar que sus equipos tengan acceso y conozcan esta Política, así como las Normas y Procedimientos relacionados con la Seguridad de los
Información;
f) Atribuir en la fase de contratación de terceros y socios, cuando necesiten tener contacto con información de la empresa, la inserción de una cláusula de responsabilidad, conocimiento de la Política de Seguridad de la Empresa
Información, que requiere la transferencia de obligaciones a sus empleados responsables de la prestación de servicios dentro de green4T; g)
Especificar y solicitar previamente el permiso de acceso, enumerando los activos de información para los empleados en general que no estén contratados;

h) Asistir al responsable de seguridad de la Información en la adecuación de las Normas, Procesos, Procedimientos y sistemas bajo su responsabilidad para cumplir con la presente Política de Seguridad de la Información; i) Comunicar de
inmediato al responsable de seguridad de la información, a través de un Canal específico (dpo@green4t.com), cualquier vulneración de la Seguridad de la Información, la cual se desencadenará y trabajará en conjunto con el equipo de Seguridad de la Información.

4.5. GERENTE DE CUMPLIMIENTO

a) Realizar pruebas de seguimiento sobre el cumplimiento de las normas establecidas en esta política; b) Asistir al DPO en
la adecuación de la empresa green4T a la ley 13.709/18 (Ley General de Protección de Datos - LGPD), las normas ISO/IEC 27.001, ISO/IEC 27.002 e ISO/IEC 27.701, definiendo las mejoras de controles internos a ser implementados por el área de tecnologías de la información y demás requisitos descritos en la ley.

4.6. ÁREA DE SEGURIDAD DE LA INFORMACIÓN

El equipo de seguridad de la información de green4T es responsable de:

a) Presentar al Comité de Seguridad de la Información y LGPD las versiones de la Política y estándares de seguridad de la información, y luego de su aprobación, publicarlos y promoverlos en la intranet de green4T; b) Proponer y apoyar iniciativas encaminadas a asegurar los bienes de información de green4T;

c) Promover, junto con el área de Personas, la concientización de los empleados y colaboradores sobre la importancia de la Seguridad de la Información para los negocios de green4T, a través de campañas, charlas, capacitaciones y otros medios;

d) Analizar críticamente los incidentes, con el apoyo del equipo de TI, si es necesario; e) Mantener una comunicación efectiva con el Comité de Seguridad de la Información y LGPD, con el fin de mantenerlos adecuadamente informados sobre asuntos relacionados con el tema, que afecten o tengan el potencial de afectar a green4T; f) Recibir denuncias sobre violaciones a la Política y Normas, luego de culminadas las investigaciones realizadas, debiendo promover el tratamiento de la información, identificación del plan de acción, mitigación de riesgos, activación del Comité de Seguridad de la Información y LGPD y aplicación de las correspondientes sanción (Sanciones).

4.7 ÁREA JURÍDICA

a) Brindar orientación sobre la mejor manera de recolectar y preservar evidencia electrónica, a fin de mantener su efectividad para uso en la corte, cuando sea necesario; y b) Elaborar y revisar documentos legales relacionados con la Seguridad de la Información, principalmente de protección de datos definidos por la LGPD y asegurando cláusulas que mitiguen los riesgos legales.

4.8 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN El Comité de Seguridad de la Información y LGPD está integrado por directivos de las principales áreas de Green4T, quienes deben cumplir con las siguientes responsabilidades dentro de la organización.

a) Asegurar la disponibilidad de recursos para todas las acciones de Seguridad de la Información; b) Mantener el enfoque y promover la Seguridad de la Información en green4T, aprobando políticas que reflejen su función descrita anteriormente mediante la aprobación del material presentado por el gerente de Seguridad de la Información. Información;

c) Asegurar que los riesgos para la Seguridad de la Información sean identificados, evaluados, categorizados y gestionados por el gerente de Seguridad de la Información Información responsable de eso; d) Aprobar acciones rentables para gestionar los riesgos y monitorear su implementación; e) Dirigir, revisar y actualizar la estrategia de Seguridad de la

Información que garantice que su Política, reglas y procedimientos se actualicen adecuadamente y sean continuamente relevantes para el escenario green4T;

f) Velar por que se imparta formación y concienciación sobre Seguridad de la Información a los empleados y, en su caso, a terceros, proveedores y clientes.

5. LINEAMIENTOS DE ESTA POLÍTICA

5.1. REGLAS GENERALES

La información producida o recibida por los profesionales de green4T debe ser utilizada con sentido de responsabilidad y de forma ética y segura, en beneficio exclusivo del negocio empresarial y con base en los siguientes principios de integridad, disponibilidad y confidencialidad. En green4T, la información se considera el activo más valioso. Sin confidencialidad se pierde ventaja competitiva, sin integridad se pierde rentabilidad y sin disponibilidad se pierde la capacidad de operar. Además de los tres atributos mencionados, también se consideran la autenticidad, la legalidad y la trazabilidad, ya que sin autenticidad se pierde la confianza en el origen confiable de la información, sin legalidad se corre el riesgo de no apego a las normas regulatorias internas y externas y sin trazabilidad, pierde el control de las actualizaciones de los datos confidenciales.

La Seguridad de la Información en la organización establece los principales lineamientos y controles para la protección de la información:

El. La información propiedad de green4T debe ser tratada de manera ética, confidencial y legal y siempre atendiendo a los términos acordados con empleados, clientes y socios, evitando así el mal uso y exposición indebida de dicha información;

B. La información debe ser utilizada de manera transparente, únicamente para el fin para el cual fue designada y por el tiempo necesario para lograr su finalidad;

w. Todo usuario se compromete a utilizar la Información únicamente en el desempeño de sus funciones y debidamente clasificada según los criterios de clasificación definidos por la organización;

d. Durante su relación laboral o sociedad con green4T, e incluso después de que finalice, el usuario no podrá publicar, revelar o poner a disposición de ningún tercero cualquier Información clasificada como Restringida o Confidencial Restringida, excepto: (i) cuando esté expresamente autorizado en escrito por green4T, o (ii) a otros empleados activos que se sabe que están autorizados a recibir

Información confidencial y la necesidad de conocerla para poder utilizarla para satisfacer las necesidades comerciales;

Es. Todos los usuarios de la información son conscientes y se comprometen a actuar con toda la diligencia necesaria para proteger la integridad y el secreto de la información propiedad de green4T, quedando prohibida la sustracción o sustracción, en cualquier forma, de cualquier material, salvo lo necesario en razón de normas o leyes vigentes;

F. Todas las personas dentro de las instalaciones físicas de Green4T deben estar identificadas mediante distintivos visibles (u otros medios visuales de identificación). La identificación (gafete, login, contraseña, etc.) de cada empleado es única, personal e intransferible, calificándolo como civil y penalmente responsable por las acciones realizadas;

gramo. La contraseña de acceso es de uso personal e intransferible y debe ser mantenida en forma confidencial, quedando expresamente prohibida su divulgación, salvo en los casos previamente aprobados por las áreas de Seguridad de la Información;

h Todos los riesgos identificados en relación con la información de green4T deberán ser comunicados al equipo de seguridad de la información a través de un canal específico (dpo@green4t.com), a fin de que se puedan tomar las medidas necesarias para evaluar y mitigar el riesgo eventualmente identificado. Además de todos los incidentes que afecten a la seguridad de la información, también deberán ser comunicados al equipo de seguridad de la información a través de un canal específico (dpo@green4t.com), que analizará el incidente y elaborará el informe;

i. Todo procedimiento seguirá los lineamientos y normas para incidentes de seguridad y, en su caso, elevará el informe al directorio para que se apliquen las sanciones correspondientes a los involucrados;

j. El control de acceso de los usuarios a los activos de información deberá ser debidamente aprobado por el responsable de la información, ya sea para su simple consulta o para su alteración. Toda la información relativa a la solicitud, aprobación y otorgamiento efectivo del acceso deberá almacenarse en un Drive seguro, con control de acceso configurado por los responsables de cada área;

k. El uso del correo electrónico corporativo puesto a disposición por green4T es de su propiedad y será permitido a los usuarios únicamente para fines corporativos y por un período de tiempo determinado, definido por la gerencia del área solicitante. En cuanto a la transmisión de datos, esta función debe utilizarse para garantizar la privacidad en la comunicación de datos;

yo Todos los requisitos de seguridad de la información, incluida la necesidad de planes de continuidad del negocio, deben identificarse en la fase de definición del alcance de un proyecto o sistema. Estos requisitos deben ser justificados, acordados, documentados, implementados y probados durante la fase de ejecución;

metro. Las reglas para el desarrollo seguro de sistemas y software deben establecerse y aplicarse a los desarrollos realizados dentro o fuera de la organización, sujeto a la evaluación de la adecuación y aprobación del equipo de Seguridad de la Información. En caso de desarrollo fuera de green4T, el sistema debe contener herramientas que permitan realizar auditorías de seguridad en cuanto a: autodeterminación informativa de los titulares de datos, pistas de auditoría, políticas de acceso (autenticación, autorización y trazabilidad) y análisis de códigos fuente;

norte. La concesión de acceso remoto a los sistemas y Drives de green4T a empleados, socios y proveedores debe ser autorizada formalmente. La solicitud debe ser enviada al área de TI, por el responsable del área solicitante, momento en el cual se debe indicar el tipo de acceso, permiso e información a acceder. Todo trámite deberá ser presentado al responsable de seguridad de la información para que tenga conocimiento de las autorizaciones;

o El uso del entorno de Internet en green4T está permitido únicamente con fines profesionales, donde los empleados deben conocer los sitios a los que acceden y saber que serán monitoreados;

PAG. Debe crearse un conjunto de reglas para garantizar la estandarización de las técnicas criptográficas, su correcta aplicación y las responsabilidades para mantener la seguridad en el transporte o almacenamiento de la información, independientemente del medio utilizado. La responsabilidad de las reglas recae en el gerente de TI en colaboración con el gerente de seguridad de la información;

q. El entorno de desarrollo, aprobación y producción debe estar segregado y debidamente controlado. El uso de datos personales reales y datos personales confidenciales no está permitido en el entorno de prueba;

R. Un proceso de gestión del cambio asegura que los controles y modificaciones a los sistemas o recursos de procesamiento de información se realicen con planificación, a fin de no provocar fallas operativas o de seguridad en el entorno productivo de la organización;

s. Los riesgos se identifican a través de un proceso establecido de análisis de vulnerabilidades, amenazas e impactos en los procesos en materia de seguridad de la información (confidencialidad, integridad y disponibilidad);

t. Toda la información que se encuentre en el medio físico (papel) debe ser clasificada con el mismo contenido, almacenada en lugar seguro, bajo llave, protegida contra riesgos naturales, voluntarios e involuntarios, con control de acceso formal por parte de los usuarios con miras a posibles pistas de auditoría;

tu Cuando razones tecnológicas o determinaciones superiores imposibiliten la aplicación de los requisitos establecidos en esta Política, el responsable y/o solicitante deberá informarlos de inmediato al gerente de seguridad de la información, a fin de que éste posibilite la adopción de medidas alternativas que mitigar los riesgos, así como un plan de acción para corregirlos, mitigarlos, monitorearlos o eliminarlos;

v. Todos los empleados de green4T deben recibir formación y concienciación periódica sobre los procedimientos de seguridad y el uso correcto de los activos puestos a disposición por green4T, con el fin de minimizar los posibles riesgos de seguridad, explicar sus responsabilidades y comunicar los procedimientos para reportar incidentes;

w. Todos los empleados de green4T deben asegurarse de que se conserven los
tú derechos de propiedad intelectual, tales como proyectos, marcas registradas, patentes y que el uso de los productos de software propietario cumpla con la respectiva licencia de uso;

X. Todos los empleados de green4T deben velar por el cumplimiento de la “Política de mesa limpia, pantalla limpia y basura limpia”, cuyo objetivo es evitar:
1) papeles y medios de almacenamiento extraíbles encima de los escritorios;
2) papeleras que contengan información confidencial legible; 3)
pantallas con información de sesiones activas o sesiones ya desactivadas.

Este cuidado se extiende a las zonas comunes, como pasillos, armarios, zonas de almacenamiento de material, salas de reuniones, zonas de espera, zonas comunes (despensa, cocina, ocio, etc.).

5.2. DIVULGACIÓN

La Política de Seguridad de la Información es conocida por todos los usuarios y se divulga de la siguiente manera:

a) A través de campañas periódicas de Seguridad de la Información; y
b) Por medios digitales, a través de la intranet corporativa.

La política está disponible en un lugar de fácil acceso para los empleados y está protegida contra cambios no autorizados.

Todos los empleados, además de los prestadores de servicios, socios y proveedores que accedan o manipulen información (digital o física) de cualquier forma o utilicen los recursos tecnológicos de green4T, deberán adherirse formalmente a la "POL.00.22 - POLÍTICA DE TECNOLOGÍAS DE LA INFORMACIÓN", comprometiéndose a actuar de conformidad con las reglas allí descritas. (Material disponible como uno de los tomos de la Política de Seguridad de la Información).

PL.00.34 - La Política de Seguridad de la Información es revisada y actualizada periódicamente, por lo menos cada 01 (un) año y/o cada vez que ocurra algún hecho o evento relevante que motive su revisión anticipada, de acuerdo con el análisis y decisión del Comité de Seguridad de la Información y LGPD.

5.3. SUPERVISIÓN

green4T, a través de su área de Seguridad de la Información, monitorea y registra todo el uso de la información generada, almacenada o transmitida en el mismo, la cual se reserva el derecho de:

a) Implementar sistemas de monitoreo de acceso a estaciones de trabajo, servidores internos y externos, correo electrónico, Internet, dispositivos móviles o inalámbricos y demás componentes de la red. La información generada por estos sistemas de monitoreo podrá ser utilizada para identificar a los usuarios y sus respectivos accesos.

b) Inspeccionar cualquier archivo que se encuentre en la red, en el disco local de la estación o en cualquier otro entorno, a fin de asegurar el estricto cumplimiento de esta Política de Seguridad de la Información.

c) Instalar sistemas de protección y detección de intrusos para garantizar la seguridad de la información y perímetros de acceso.

d) Vigilar las instalaciones físicas a través de cámaras.

5.4. DIRECTRICES PARA LA LGPD

Las empresas de Green4T han definido e implementado los controles internos necesarios para cumplir con la LGPD, en lo que respecta a la protección de datos de clientes, empleados, proveedores u otros que involucren datos de personas físicas, en la forma prevista en la ley 13.709/18.

5.5. PENALIZACIONES

Cuando se considere necesario y pertinente, el equipo de Seguridad de la Información someterá al directorio las violaciones a la Política de Seguridad de la Información y los Estándares de Seguridad de la Información, así como el resultado de la verificación validada a través del comité de seguridad de la información y la LGPD y demás áreas pertinentes, de conformidad con Política de investigación de quejas de green4T.

Al sospechoso de cometer violaciones a la Política y Reglamento de Seguridad de la Información se le debe garantizar un trato justo y correcto, y todas y cada una de las medidas que resulten de su infracción se deben aplicar proporcionalmente a la ocurrencia con base en el Reglamento de Infracciones y Sanciones.

green4T se exime de cualquier y toda responsabilidad derivada del uso indebido, negligente o temerario de los recursos y servicios otorgados a sus empleados, reservándose el derecho de sancionar a los infractores, analizar datos y evidencias para obtener pruebas para ser utilizadas en procesos de investigación y adoptar las medidas legales apropiadas. medidas

6. DOCUMENTOS DE REFERENCIA

P.12.01 - Backup_green4T
P.12.04 - Shutdowns_green4T
P.00.22 – Política de Tecnologías de la Información_green4T
P.00.31 – Política de Privacidad Interna_green4T
P.00.32 – Política de Privacidad Externa_green4T

7. CONTROL DE REGISTROS

NA.

8. HISTORIAL DE REVISIÓN

Revisión	Fecha	Descripción de Cambio	Aprobado por el Gerente	Aprobado por Certificaciones
00	30/05/2022	Emisión	Eduardo marino	Adriana Moisés
01	15/08/2023	Revisión general de la política, modificado el ítem 5.1.f	Comité LGPD: Claudio (DPO), Alan Baldo, Eduardo Rasi y Thais Almeida	