Rotoplas más y mejor agua	**Política de Seguridad de la Información**	Código: GR-EAI-POL-014 Fecha de emisión: Abril 2021 Fecha de revisión: Junio 2021 N° de revisión: 01

ELABORA	**REVISA**	**AUTORIZA**
Nombre: Christian Sánchez Domínguez Puesto: Gerente Seguridad de la Información y TI	Nombre: Juan Fernando Gómez Collada Puesto: Gerente Sr. De Sistemas Nombre: Ma. del Carmen Garcia Romero Puesto: Gerente Sr. Contraloría MX, CA & LATAM	Nombre: Diego Fernando Ponce García Puesto: VP Transformación Nombre: Suraj Shinde Puesto: Director Digital y TI Nombre: Luis Humberto Maya Márquez Puesto: Director de Contraloría

Objetivo

- Definir un marco para normar y establecer las reglas y los lineamientos para gestionar la información y los recursos tecnológicos en Grupo Rotoplas, que garanticen la integridad, confidencialidad y disponibilidad.
- Alinear la continuidad de los servicios y actividades del negocio relacionadas con la seguridad de la información
- Dar confianza a los clientes, colaboradores, socios y proveedores, accionistas y autoridades disponiendo de un sistema de información confiable y seguro.
- Cumplir con las obligaciones contractuales, legales y normativas.
- Alinear con la estrategia del negocio para apoyar en la misión y visión del Grupo Rotoplas.
- Establecer y mantener una cultura en Seguridad de la Información sólida y sostenible en el tiempo.
- Gestionar continuamente los riesgos de seguridad de la información, promoviendo el constante monitoreo de nuevos riesgos y hacer seguimiento a los planes de mitigación respectivos.
- Evaluar la eficacia de los controles implementados para proteger la información que gestiona el negocio de acuerdo con sus riesgos asociados respecto a la confidencialidad, integridad y disponibilidad.
- Mitigar el impacto de los incidentes relacionados con la seguridad de la información en la organización.

Alcance

Esta política es de aplicación general para todo el personal de Grupo Rotoplas que labore o preste servicios, inversionistas y Empresas Subsidiarias, misma que deberá cumplirse con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información.

Descripción

Grupo Rotoplas es una empresa fundada en 1978 que se dedica a crear soluciones para almacenar, conducir, purificar y tratar agua en tu hogar y trabajo.
En Rotoplas tenemos como misión llevar más y mejor agua a las personas, por eso desde hace cuatro décadas nos esforzamos día con día a crear soluciones para almacenar, conducir, purificar y tratar el agua en tu hogar y trabajo. Somos una compañía líder de origen mexicano, con una tradición que nos impulsa a crecer sostenidamente en América y a traspasar fronteras para llevar nuestras soluciones a otros países.

Grupo Rotoplas ha tomado la decisión de robustecer la seguridad de Información para proteger los activos de la organización alineados a las mejores prácticas.

Grupo Rotoplas reconoce que los activos de información que se tienen y que son soportados en la infraestructura tecnológica son esenciales para el desarrollo de la estrategia y la continuidad del negocio, para el cumplimiento de su misión y visión.

Grupo Rotoplas se compromete al cumplimiento de los requisitos aplicables en temas de Seguridad de la Información teniendo en cuenta la Confidencialidad, Integridad y Disponibilidad.

Grupo Rotoplas se compromete a implantar, operar, monitorear, revisar, mantener y mejorar continuamente la Gestión de Seguridad de la Información para que los controles seleccionados protejan los activos de información y den confianza a los clientes, proveedores, empleados, accionistas, autoridades y demás interesados.

Términos y Glosario

- Activo de información
  Cualquier herramienta, artefacto, programa, que personas que manejan datos o contiene información de valor para GRUPO ROTOPLAS.
- Confidencialidad:
  Propiedad que impide la divulgación de información a personas o sistemas no autorizados. Asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.
- Control:
  Capacidad para ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan.
- Disponibilidad:
  Es la característica, cualidad o condición de la información de encontrarse a disposición de quien debe acceder a ella, ya sean personas, procesos o aplicaciones. Es el acceso a la información por personas autorizadas en el momento que así lo requieran.
- Estrategia:
  Conjunto de decisiones que se toman para determinar políticas, misión, visión y objetivo. Información
- Información
  Datos organizados resultado del uso de las soluciones de negocio. Información escrita como procedimientos, manuales, contratos, etc.
- Integridad:
  Propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.
- Norma:
  Forma en que se realiza un procedimiento o proceso.
- Riesgo:
  Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias.
- Seguridad de Información:
  Preservación de la confidencialidad, integridad y accesibilidad de la información.
- Usuario:
  Empleado de Grupo Rotoplas o persona que presta servicios que por sus funciones mantiene autorización a acceder y hacer uso de las diferentes soluciones tecnológicas.

Objetivos de Control Interno

- Reporte Financiero –Confiabilidad de la información

- Operaciones – Continuidad en las operaciones de la organización
- Cumplimiento – con las normas internas, leyes y reglamentos que afectan a la organización.

Política

Las responsabilidades de la Seguridad de la Información y de los sistemas que la tratan, almacenan o transmiten se extiende a todos los niveles y funciones del Grupo Rotoplas.

La alta Dirección define y asegura que los objetivos de Seguridad de la Información se cumplan con lo establecido en la estrategia de Seguridad de la Información para la organización.

Comité de Seguridad de la información

El Comité de Seguridad de la Información de la compañía será el órgano que se encargará de tomar las decisiones orientadas a la Estrategia de Seguridad de la Información del Grupo Rotoplas.

Este Comité se reunirá por lo menos una vez al año o cuando se requiera por algún acontecimiento excepcional.

Estará integrado como mínimo por los siguientes:

Directores de las partes interesadas
Dirección Digital y TI
Gerencia Sr de TI
Gerente de Seguridad de la información y TI
Gerente de Infraestructura.
Gerente Sr Contraloría
Gerente Sr Seguridad Corporativa

Responsabilidad de Seguridad de la Información

El responsable de Seguridad de la Información del Grupo Rotoplas deberá considerar:

Implementar una estrategia de Seguridad de la Información que vele por el cumplimiento de los principios básicos de esta Política y tendrá la encomienda de liderar la protección de los activos de información, permear la cultura de seguridad de la información como gestor del Sistema de Gestión de Seguridad de la Información (SGSI) en conjunto con todos los colaboradores.

Se establece un modelo de gobierno de responsabilidades del control que se muestra en los siguientes roles:

- Responsable del Proceso: Persona que ha sido nombrada el encargado de garantizar que el proceso total sea efectivo y eficiente.
- Responsable del Control: Persona que ha sido nombrada para ejecutar el control o actividad de un proceso.

Responsabilidad de los colaboradores

Es responsabilidad de cada colaborador conocer y apegarse a las políticas, procedimientos y Código de Ética; cualquier incumplimiento se actuará bajo los lineamientos descritos en el Código de Ética y la legislación aplicable.

- Todos los colaboradores que prestan servicios al Grupo Rotoplas deberán de conocer, asumir y cumplir la Política, estando obligados a mantener el secreto profesional y la confidencialidad de la información manejada en su entorno laboral.
- Cada uno de los colaboradores es responsable de la seguridad de la información alineado a su rol.
- Deben comunicar, con carácter de urgencia y según los procedimientos establecidos, las posibles incidencias o problemas de seguridad que se detecten.

Concientización, educación y capacitación

- Deberán participar en los cursos asignados por el Grupo Rotoplas
- Todos los colaboradores del Grupo Rotoplas y los usuarios terceros que presten servicio deberán participar en las actividades de concientización, educación y capacitación periódica en materia de Seguridad de la Información.
- Los colaboradores del Grupo Rotoplas deberán conocer y certificarse en la política de Seguridad de la Información.
- Los terceros que presten servicio deberán conocer y apegarse a los lineamientos de la política de Seguridad de la Información.

Uso de Activos

- Se deberá hacer buen uso y manejo de los activos. Esto con el fin de evitar cualquier divulgación, modificación, retiro o destrucción de información no autorizada.
- El colaborador está obligado a cuidar los activos que se le hayan asignado como responsable o que se le haya otorgado acceso a los mismos.
- El colaborador deberá de conectar sus herramientas de trabajo en redes seguras.
- Todos los colaboradores y usuarios externos deberán devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
- Toda la información relacionada con la operación en la organización se debe almacenar, manipular, compartir y comunicar solo desde las herramientas institucionales asignadas y autorizadas por el Grupo Rotoplas.

Control de accesos y uso de contraseñas

- Todo lo que ocurra con el usuario y contraseña es responsabilidad del dueño de las credenciales.
- Los colaboradores que tengan acceso a los sistemas deberán tener un usuario único y personalizado.
- Cada usuario deberá ser autorizado y accederá a los recursos con el mínimo de privilegios que le permita llevar a cabo las acciones necesarias para sus funciones de trabajo.
- Las cuentas y contraseñas de acceso deberán de ser custodiadas de forma estricta por el responsable y no deberán ser compartidas.
- El usuario debe cambiar la contraseña al conectarse por primera vez cuando ésta haya sido asignada por un tercero.
- Si el usuario entiende que su contraseña pudiera estar comprometida debe sustituirla por otra, de manera inmediata.
- Las contraseñas deben de tratarse como información confidencial y privilegiada.
- Las contraseñas no deben incluirse en ningún tipo de comunicación electrónica e impresa.
- No escriba su contraseña en documentos, etiquetas físicas, equipos públicos, compartidos o aquellos en que se desconozcan su nivel de seguridad.

- Evitar la opción de “recordar contraseña” que ofrecen los navegadores, especialmente cuando se traten de equipos compartidos.
- Las contraseñas deben cumplir las normas que se exponen a continuación:
  - Contraseñas compuestas de ocho caracteres como mínimo.
  - Renovación de las contraseñas cada tres meses.
  - Utilizar en una misma contraseña números, letras, una mayúscula y caracteres especiales.
  - Al cambiar la contraseña se prohíbe utilizar una de las cinco últimas contraseñas.

Transferencia de la información y uso de medios móviles

- Realizar un uso adecuado de la red de internet proveída para el uso especifico relacionado con las funciones del usuario.
- Queda prohibido la conexión o instalación de dispositivos y software no autorizados por el Grupo Rotoplas.
- Queda prohibido la utilización de dispositivos de almacenamiento móvil como son: quemadores de CD/DVD discos y memorias de almacenamiento con interfaces de USB, SD, MMC, Micro SD, etc. De manera enunciativa pero no limitativa, que ponga en riesgo la confidencialidad y disponibilidad de los activos.
- En los equipos móviles asignado por el Grupo Rotoplas solo debe almacenarse información de la compañía de acuerdo con las atribuciones y funciones del puesto del colaborador.

Seguridad física en las instalaciones

- Los accesos a las instalaciones deberán ser registrados y autorizados.
- Las visitas, proveedores, personal externo deberán ser autorizados y acompañados por el colaborador responsable del Grupo Rotoplas.
- Evitar la ejecución de trabajos por parte de terceros sin supervisión de colaboradores del Grupo Rotoplas.
- Las zonas restringidas, cuyo acceso debe limitarse únicamente a las personas autorizadas por las personas responsables.
- Controles de entradas/Salidas
  - Se deberán de registrar los accesos a las oficinas, plantas e instalaciones del Grupo Rotoplas de personas ajenas (nombre, apellidos, horas de llegada y salida, etc.) y se acompañarán a los visitantes durante su estancia hasta su salida.

Seguir los controles que marca el área de Seguridad Corporativa y cualquier otro control de acceso contenido en los procedimientos de seguridad del Manual de Operaciones y consignas para el personal en planta.

Seguridad relacionada con la operación

- Queda prohibido el uso de software no autorizado.
- Evitar abrir corros electrónicos y enlaces URL de remitentes desconocidos.
- Asegurar que los equipos de terceros que son autorizados para conectarse a la red tengan antivirus y cuenten con las medidas de seguridad apropiadas.

Escritorio limpio y equipo desatendido

- Debes considerar que, en tu lugar de trabajo, pantallas del equipo de cómputo, estaciones de trabajo y medios de almacenamiento, no queden expuestos los documento físico y digitales con información confidencial y/o privilegiada.
- No dejes desatendido tu equipo de cómputo y bloquea tu sesión.

Respuestas a incidentes y anomalías en materia de Seguridad de la Información

- El colaborador deberá de informar al correo infosec@rotoplas.com cualquier comportamiento violatorio identificado y que atente contra la seguridad de la información

Todos los colaboradores y partes externas deberán seguir esta Política y el anexo de la política de seguridad de la Información donde se definen los controles que se deben implementar y cumplir para garantizar la confidencialidad, integridad y disponibilidad de los siguientes temas:

A. Políticas de seguridad de la información
B. Organización de la seguridad de la información
C. Seguridad relativa a los recursos humanos
D. Gestión de activos
E. Control de acceso
F. Criptografía
G. Seguridad física y del entorno
H. Seguridad de las operaciones.
I. Seguridad de las comunicaciones
J. Adquisición, desarrollo y mantenimiento de los sistemas de información
K. Relación con proveedores
L. Gestión de incidentes de seguridad de la información
M. Aspectos de seguridad de la información para la gestión de la continuidad de negocio
N. Cumplimiento

Sanciones

- El Comité de Ética de Grupo Rotoplas será el encargado de valorar y sancionar la participación de las y los colaboradores en incidentes y/o infracciones de seguridad de la información relacionados en esta política alineados al Código de Ética y de Conducta.

Excepciones

- Cualquier excepción a esta política deberá ser solicitada formalmente por el Director del área solicitante, autorizada por el Director de Contraloría, el Director de Digital Y TI y Gestionada por el responsable de Seguridad de la Información.

El presente documento debe ser revisado y actualizado al menos una vez al año o cuando se realicen cambios significativos en la infraestructura u operación crítica del Grupo Rotoplas

Fuentes de Información y referencias

Esta Política de Seguridad de la Información se basa en la norma ISO 27001 y NIST.

Formatos/Anexos

- GR-EAI-POL-010 Política para Gestión de Contraseñas
- GR-EAI-POL-011 Política Uso Aceptable de Activos y Actuación sobre Comunicaciones Empresariales
- GR-EAI-POL-013 Política Utilización de Equipo de Cómputo, Comunicación y Redes Sociales
- GR-EAI-POL-016 Política Uso de Cuentas SAP para Consultores Externos
- GR-EAI-MAN-003 Manual de Principios Específicos de Seguridad de la Información
- GR-CAP-PRO-003 Evaluación de proveedores

HISTORIAL DE CAMBIOS		
Número de Revisión	**Fecha de Revisión**	**Descripción del Cambio**
00	20.Abril.2021	Creación de documento
01	25.Junio.2021	Cambio en cuadro de autorización/ título de la Política/ redacción de la política más general/ agrego los lineamientos de las contraseñas.