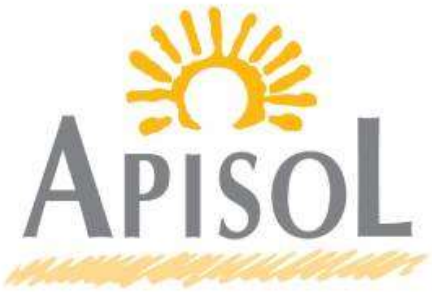

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

APROBACIÓN Y ENTRADA EN VIGOR:

El presente texto ha sido aprobado el día 1 de Septiembre de 2020 por la Dirección de Apisol SA.

Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación y hasta que la misma sea reemplazada por la aprobación de una nueva Política.

1. Introducción

APISOL SA para alcanzar sus objetivos en el normal desarrollo de su actividad, depende de los sistemas TIC (Tecnologías de Información y Comunicaciones). Estos sistemas deben ser administrados con la debida diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad, así como autenticidad y trazabilidad de la información tratada o los servicios que se prestan.

El fin único de la seguridad de la información, y por ende el de la presente política, es garantizar la calidad de la información y la prestación continuada de los servicios, actuando de forma preventiva, supervisando las actividades diarias que se desarrollan en la organización y reaccionando con celeridad frente a los incidentes que puedan ocurrir.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial suficiente para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y de los servicios. Es necesario que para defenderse o prevenir estas amenazas, se implemente una estrategia que se adapte a cualquier cambio, en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto significa que todos los departamentos deben de aplicar al menos las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS) y a nivel de buenas prácticas las establecidas en la Norma ISO/IEC 27001, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos y áreas de la organización deben cerciorarse de que la seguridad TIC es una parte integral de cada una de las etapas del ciclo de vida del sistema. Los departamentos y áreas deben estar preparados para prevenir, detectar, reaccionar y recuperarse de los posibles incidentes, en sus sistemas de información.

2. Prevención, detección, reacción y recuperación:

APISOL SA pone a disposición los recursos para evitar que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos y áreas deben implementar las aplicar al menos las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), a nivel de buenas prácticas las establecidas en la Norma ISO/IEC 27001 así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, Los departamentos y áreas deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Dado que, debido a incidentes, los servicios pueden verse rápidamente degradados, éstos deben de monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia; se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Para garantizar la disponibilidad de los servicios, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. Alcance:

La presente política se aplica a todos los sistemas TIC de APISOL SA y a todas las personas de la organización.

4. Propósito y Misión:

El propósito de Apisol se fundamenta en aportar a la sociedad productos saludables, sostenibles y que enamoren.

En Apisol tenemos la aspiración de aportar productos que enamoren y contribuyan a mantener una vida saludable utilizando ingredientes naturales. También aspiramos a trabajar de forma sostenible, siendo respetuosos con el medio ambiente, utilizando materiales 100% reciclables, y cuidando a nuestros apicultores/agricultores, ya que ellos son los grandes protagonistas.

Con el fin de garantizar la protección efectiva de los recursos corporativos necesarios para el correcto funcionamiento de la organización, tanto de amenazas externas como internas y definiendo dicha protección en términos de calidad, se establecen los siguientes objetivos y principios básicos:

1. Cumplir los requisitos legales y contractuales aplicables al desarrollo de sus funciones, en especial, y a efectos de la presente Política, en las materias relacionadas con la seguridad de la información.
2. Difundir entre todo el personal y hacer cumplir los procesos y normativa aplicables en materia de seguridad de la información, individualmente en función de sus tareas dentro de la organización.

3. Garantizar la protección de la información, mediante la correcta aplicación de las medidas de seguridad, el correcto uso de los sistemas que la procesan que son responsabilidad de la organización, y la limitación de accesos según la necesidad de conocer de las personas.
4. Mantener el secreto respecto a la información y no divulgarla a terceros, salvo que las comunicaciones formen parte de la relación laboral y en cumplimiento de las debidas garantías de confidencialidad.

5. Marco normativo y legal:

Esta Política se desarrollará conforme al marco normativo y legal aplicable en materia de seguridad, concretamente:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales y lo relativo a los mismos en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- En materia de protección de datos de carácter personal, APISOL SA cumple con los dispuesto en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Normas de la Autoridad Nacional para la Protección de la Información Clasificada.
- UNE-EN ISO/IEC 27001, tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la Información y requisitos. Que contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

6. Normativa interna:

La presente política se desarrollará en los siguientes ámbitos de aplicación.:

- Clasificación y etiquetado de la Información.
- Seguridad en Explotación.
- Seguridad en las Comunicaciones.
- Gestión de Auditoria Interna de Seguridad.
- Mejora Continua del Sistema de Gestión.

- Gestión de la Seguridad en las Relaciones con Terceros.
- Gestión de Activos y Soportes.
- Análisis y Gestión de Riesgos.
- Gestión de la Documentación del Sistema de Gestión.
- Gestión de Copias de Seguridad y Restauración.
- Gestión de Incidentes de Seguridad.
- Gestión de Acceso Lógico de la Información.
- Seguridad física y del entorno.
- Adquisición, Desarrollo y Mantenimiento de Sistemas.
- Gestión de la Continuidad del Servicio.
- Gestión de Supervisión de Sistemas.
- Firma electrónica, certificados y controles criptográficos.
- Gestión de la seguridad en la relación con las personas.

La normativa de seguridad estará a disposición de todos los miembros de la Organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

7. Organización de la seguridad:

a. Comité:

Con el fin de facilitar la gestión de la seguridad en Apisol SA, mediante la aprobación de la presente política, se aprueba también la formación de un Comité de Seguridad de la Información orientado a la gestión de la seguridad en la organización.

Este comité tiene la función de coordinar todas las funciones de seguridad de Apisol SA, vela por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial. Asimismo, este comité se encarga de velar por el alineamiento de las actividades de seguridad y los objetivos de la organización.

El comité lo formarán el Director General y el Responsable de TIC en APISOL SA.

b. Roles y responsabilidades:

En el marco de cumplimiento del ENS y la IS027001, y a fin de conformar la estructura de responsables en materia de seguridad, se han determinado los siguientes roles principales:

- Responsable de la Seguridad de la Información, representado por el Director General de Apisol SA.
- Responsable de Servicio, representado por el Responsable de TIC.

c. Procedimientos de designación:

Los roles y responsabilidades en materia de seguridad de la información serán designados por la Dirección General de APISOL y/o el Responsable de Seguridad de la Información, según la relación jerárquica de los perfiles afectados.

8. Gestión de riesgos:

Todos los sistemas sujetos a la presente Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Cuando exista un cambio significativo en los sistemas de información.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

9. Obligaciones del personal:

Todas las PERSONAS de Apisol SA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad que la desarrolla, siendo responsabilidad del Comité de Dirección disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un plan de concienciación continua, en materia de seguridad de la información, para atender a todas las personas de Apisol SA según su grado de responsabilidad.

Firma del empleado:	Firma de la Dirección de APISOL: