Normas de Seguridad Corporativas TIC

1. OBJETO

El presente documento tiene como objeto definir las normas de seguridad corporativas en el ámbito de las TIC.

2. ALCANCE

Estas normas aplican a todo el personal y terceros (proveedores, personal subcontratado, colaboradores, etc.) que tengan acceso a información propiedad de APISOL SA.

3. NORMAS DE SEGURIDAD

A continuación, se detallan las normas de seguridad, aplicable a todo el personal y colaboradores que acceden a los sistemas e instalaciones de APISOL SA:

4. ZONAS Y ESPACIOS PROTEGIDOS

En APISOL SA se han identificado cuatro tipos de zonas según su nivel de protección:

- Zonas de acceso público, designadas para zonas de atención y recepción de visitas, desde donde son atendidas e identificadas.
- Zonas de carga y descarga, que incluye tanto las áreas de recepción de material como de almacén.
- Zonas de acceso interno, limitadas al uso de todo el personal interno y terceros autorizados.
- Zonas seguras, de acceso restringido general, habilitado a personal autorizado.

Las entradas y salidas a las instalaciones y distintas zonas de APISOL SA se realizará por los accesos habilitados para ello, definidas en la normativa interna de Seguridad Física, y está restringido al personal interno y externo autorizado. Las visitas deberán permanecer acompañadas por personal interno.

Queda completamente prohibido fumar en la totalidad de las instalaciones de APISOL SA. Asimismo, se debe evitar comer o beber en zonas seguras, especialmente donde se ubiquen activos de especial protección.

La generación voluntaria de cualquier elemento que pueda afectar negativamente al funcionamiento de los equipos, tales como ceniza, polvo, humo, humedad, etc. está terminantemente prohibida salvo que se tomes las debidas medidas de precaución y bajo autorización expresa del Responsable de Instalaciones.

5. USO DE CREDENCIALES

Todo el personal, interno y externo, así como las visitas, deben registrarse a la entrada y salida por los medios implementados (huella digital y registro).

- Las credenciales para el acceso a las instalaciones, equipos, sistemas y/o a la red corporativa son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida.
- La capacidad de acceso está limitada por las credenciales según las necesidades de las funciones del puesto de trabajo. No está permitido acceder, o intentar forzar el acceso, a cualquier recurso donde no se disponga de autorización.

- No se permite compartir ni utilizar las credenciales asignadas a otros usuarios.
- Las credenciales basadas en contraseñas nunca deben anotarse, deben recordarse o almacenarse haciendo uso de administradores de contraseñas, autorizadas por APISOL SA, que permitan su custodia segura de forma cifrada. Asimismo, estas deben ser cambiadas periódicamente, siempre que el sistema lo solicite, o antes, siempre que se considere conveniente o tengamos indicios de que haya podido ser comprometida, en cuyo caso además deberá ser comunicado este hecho mediante la notificación de un incidente de seguridad.
- Las contraseñas serán cambiadas periódicamente, de acuerdo a las políticas de renovación establecidas en cada sistema, y deberán cumplir con los requisitos mínimos de complejidad y robustez establecidas por APISOL SA, definidos en la normativa interna aplicable.
- De acuerdo a la criticidad de los sistemas y zonas, se podrá requerir el uso de doble factor de autenticación para el acceso, basadas en algo que se sabe (contraseñas), algo que se tiene (tarjeta o código enviado a dispositivo móvil), y algo que se es (biometría).

6. EQUIPOS Y DISPOSITIVOS

- Los equipos y dispositivos informáticos única y exclusivamente están puestos a disposición de los usuarios con la finalidad de permitir el desempeño de las funciones y tareas laborales encomendadas, debiendo hacer un uso racional y velar por el cuidado de los mismos.
- No está permitido el almacenamiento de información de carácter distinto al exclusivamente laboral o profesional (esto es, información personal como por ejemplo fotografías, emails, etc.) en dichos dispositivos.
- APISOL SA es responsable de definir la configuración básica de los puestos de trabajo, incluyendo las medidas de seguridad a implementar
- No se permite el uso de usuarios con permisos de administración salvo aquellos casos expresamente autorizados por el Responsable del Área o Departamento.
- No está permitido alterar la configuración física ni el software de los equipos, así como desinstalar o instalar cualquier otro tipo de software distinto a la configuración predefinida, salvo autorización del Responsable del Área o Departamento y para el desempeño de sus funciones.
- Al abandonar el puesto de trabajo, se debe bloquear la sesión del equipo, por lo general mediante la combinación de teclas Win+L, a fin de evitar cualquier posible vulneración de sus credenciales mediante accesos no autorizados.
- A la finalización de la relación laboral con APISOL SA, todo el equipamiento facilitado debe ser devuelto en estado aceptable.
- Los equipos móviles como portátiles, tablets o smartphones, tienen la consideración de puestos de trabajo, y por ello estos también deben implementar medidas de seguridad. Al respecto, únicamente están permitidos el acceso a los recursos de APISOL SA a través de dispositivos móviles corporativos que dispongan de las medidas de seguridad definidas en la normativa interna de seguridad, salvo autorización del Responsable de Seguridad.
- Los equipos y soportes informáticos, que contengan información de APISOL SA, y vayan a ser desechados o reutilizados, deben ser borrados o destruidos de forma segura. Para ello, se deberá comunicar el Area de Sistemas Internos Corporativos.

7. CLASIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

La información en APISOL SA se clasifica, según la necesidad de conocer, en las siguientes categorías:

- Pública, de acceso libre sin restricciones.
- Interna, de acceso libre generalizado a todo el personal interno y externo de APISOL SA.
- Confidencial, de acceso restringido a personal, perfiles o grupos autorizados. Toda la información propiedad de clientes de APISOL SA se considera como confidencial.
- Secreta, de acceso limitado a personal autorizado. Esta clasificación se reserva a información estratégica o con altos requisitos de seguridad.

La documentación es clasificada y etiquetada por el responsable de la información de acuerdo con los criterios establecidos en la normativa interna aplicable. En caso de que por decisión o requisitos internos no se etiquete la documentación, no eximirá la aplicación de las medidas de seguridad necesarias.

La información a la que tienen acceso los usuarios debe ser utilizada única y exclusivamente para fines adecuados, y no desproporcionados, relacionados con el desempeño de sus funciones, garantizando en todo momento el cumplimiento de las medidas de seguridad que sean de aplicación según su nivel de confidencialidad.

El empleado se compromete a guardar el deber de secreto sobre toda la información propiedad de APISOL SA a la que se tenga acceso.

Se prohíbe utilizar, copiar o transmitir información contenida en los sistemas informáticos de APISOL SA para uso personal, de terceros, o cualquier otra finalidad distinta del servicio al que está destinado, salvo autorización expresa del propietario de la información.

Se realizan copias de seguridad de forma automática de la información existente en los sistemas y espacios de almacenamiento corporativo en red. Para garantizar la disponibilidad e integridad de la información, se debe priorizar el uso de estos espacios, evitando en la medida de lo posible almacenar información en entornos locales.

La transmisión de la información está restringida únicamente a las personas, roles o grupos definidos en la lista de distribución.

La impresión de documentación se realizará en las impresoras corporativas habilitadas y haciendo uso de impresión bloqueada por usuario y contraseña.

La documentación que contenga información de carácter confidencial o superior de APISOL SA deberá ser destruida mediante las trituradoras dispuestas para ello.

En APISOL SA se promueve una política de "mesas limpias", porque se debe evitar la acumulación de documentación en las mesas y hacer uso de archivadores y armarios para la custodia ordenada y segura de la información.

Se debe evitar el uso de dispositivos y soportes portátiles extraíbles para el almacenamiento información propiedad de APISOL SA, salvo aquellos autorizados por el

Area de Sistemas Internos Corporativos que incorporen mecanismos de cifrado adecuados. Adicionalmente, el prohíbe el uso de espacios personales o compartidos en la nube no corporativos o autorizados.

8. USO DE LA RED CORPORATIVA

La red corporativa es un recurso, compartido y limitado, dispuesto tanto para el acceso de los usuarios de la organización a internet, a las aplicaciones y servicios corporativos, así como facilitar la comunicación de información. Al respecto:

- No está permitida la conexión de equipos o dispositivos no autorizados a la red corporativa interna.
- El acceso a internet está limitado para el acceso a información y medios corporativos relacionados con el desempeño de las funciones de los usuarios, debiendo evitarse el acceso a otros contenidos que resulten inapropiados.
- Se debe evitar el uso de aplicaciones de uso compartido de contenidos o descargas masivas no autorizadas.
- APISOL SA se reserva el derecho a monitorizar la actividad de la red corporativa para la prevención de malware y usos malintencionados.

9. USO DEL CORREO ELECTRÓNICO

Se considera el correo electrónico como un instrumento de trabajo que la organización pone a disposición de los usuarios para el desempeño de sus funciones en el ámbito laboral. Con ello:

- Se prohíbe su uso con fines particulares, como el intercambio de contenidos personales o subscripciones a boletines discordantes a las actividades desarrolladas
- APISOL SA se reserva el derecho a acceder a las cuentas de correo electrónico en casos de necesidad y excepcionalidad, como el acceso a datos propiedad de la organización a los que no puede accederse por otros medios, o la investigación de actividades sospechosas de uso fraudulento.
- Se deben evitar envíos masivos de correos a los usuarios, o con adjuntos de gran tamaño, limitándose a los mínimos estrictamente necesarios, a fin de evitar saturar la red y los espacios de almacenamiento.
- Se debe evitar abrir anexos de correos o enlaces sospechosos o de los que se desconozca su procedencia.
- Se debe evitar el envío de información de carácter confidencial o superior de forma desprotegida. Para ello, se debe hacer uso de los mecanismos de cifrados habilitados por la organización.

10. ACCESO REMOTO

El acceso a los sistemas de información de APISOL SA, desde fuera de las instalaciones corporativas, únicamente será autorizado mediante el uso de canales seguros de conexión remota habilitados de APISOL SA (VPN) y con los medios corporativos autorizados.

11. GESTIÓN DE INCIDENTES DE SEGURIDAD

Todo el personal de APISOL SA tiene la obligación y el deber de notificar al Responsable de TIC de cualquier actividad de la que tenga constancia y que pueda afectar a la calidad del servicio de los Sistemas de Información corporativos o a la seguridad de los datos tratados por éstos. La comunicación de incidentes se realizará a través del correo electrónico adminti@apisol.es

12. INCUMPLIMIENTO DE LA NORMATIVA

El incumplimiento de cualquiera de las obligaciones que constan en la normativa de APISOL SA, implicaría, en su caso, sanciones disciplinarias según lo previsto en el Estatuto de los Trabajadores y Convenios colectivos aplicables.

En el referido caso de incumplimiento, y sin perjuicio de las demás responsabilidades a que hubiere lugar en derecho, sería responsable de cuantos daños y perjuicios hubiera podido ocasionar tanto a APISOL SA, como a otros licenciatarios como consecuencia del eventual incumplimiento.

Firma del empleado:	Firma de la Dirección de APISOL: