1. LINEAMIENTOS GENERALES

EVOL, es una marca que agrupa diversas empresas dedicadas a la consultoría de sistemas, con presencia en Perú (TS NET S.A.), Colombia (TSNET S.A.S.), Costa Rica (TSNET S.A) y México (TSNET GLOBAL MÉXICO SA DE CV), reconoce la importancia de proteger la información como un activo fundamental para la continuidad, confianza y crecimiento del negocio.

El propósito de esta política es proporcionar a todas las partes interesadas los principios, bases conceptuales y acciones necesarias para proteger los activos de información de EVOL, garantizando su confidencialidad, integridad y disponibilidad. Asimismo, busca establecer un marco que permita mitigar los riesgos asociados a accesos no autorizados, pérdida, alteración o divulgación de información crítica, cumpliendo con la normativa vigente y buenas prácticas internacionales.

Los lineamientos que regulan el uso y control de la seguridad de la información de EVOL son:

a) Proteger la confidencialidad, integridad y disponibilidad de la información manejada por EVOL, tanto interna como externamente, asegurando su uso ético, legal y autorizado.

b) Garantizar que el acceso a la información esté restringido únicamente al personal autorizado, conforme a los roles y responsabilidades asignados.

c) Establecer controles físicos, lógicos y administrativos que permitan mitigar riesgos de pérdida, alteración, divulgación no autorizada o uso indebido de la información.

d) Promover una cultura organizacional de seguridad de la información mediante programas de sensibilización, capacitación continua y comunicación efectiva hacia todos los colaboradores y terceros involucrados.

e) Cumplir con la normativa legal vigente, incluidos los requisitos de la Ley de Protección de Datos Personales y otras regulaciones aplicables al tratamiento de información.

f) Asegurar que los sistemas tecnológicos, plataformas digitales y procesos operativos cuenten con medidas de seguridad adecuadas, desde su diseño hasta su operación continua.

g) Establecer mecanismos de control y monitoreo para detectar incidentes de seguridad, respondiendo de manera oportuna y efectiva, y asegurando la trazabilidad de los eventos.

h) Promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), alineado a las buenas prácticas como la norma ISO/IEC 27001.

i) Asegurar que los acuerdos con empleados, proveedores, clientes y aliados estratégicos incluyan cláusulas claras sobre la confidencialidad, protección de datos y manejo seguro de la información.

j) Fomentar el uso responsable de los recursos tecnológicos asignados, garantizando que se utilicen exclusivamente para fines laborales autorizados por EVOL.

k) Definir y aplicar sanciones internas en caso de incumplimiento de las disposiciones establecidas en la presente política, conforme al reglamento interno de trabajo.

2. ALCANCE

Estas políticas de seguridad de la información son aplicables a todos los empleados, contratistas, proveedores y cualquier otra parte interesada que tenga acceso a los sistemas de información, equipos tecnológicos y recursos informáticos de EVOL. Incluye el uso adecuado de contraseñas, software, equipos físicos, redes y la protección de la información tanto en el entorno de trabajo físico como en el teletrabajo.

3. DEFINICIONES

a. **Información restringida:** Datos o información que, debido a su naturaleza o sensibilidad, no debe ser divulgada sin las debidas autorizaciones.
b. **Controles criptográficos:** Técnicas utilizadas para proteger datos mediante el uso de algoritmos y claves de cifrado.
c. **VPN (Red Privada Virtual):** Herramienta que permite la conexión segura a una red privada a través de internet.
d. **Teletrabajo:** Modalidad de trabajo que permite a los empleados realizar sus funciones desde un lugar distinto a las instalaciones de la empresa mediante el uso de tecnología.
e. **Proveedor:** Persona o empresa externa a EVOL que proporciona productos o servicios relacionados con la tecnología o la información.

4. RESPONSABILIDADES DEL TRABAJADOR

a. **Cumplimiento de políticas:** El trabajador es responsable de cumplir con todas las políticas de seguridad de la información, incluyendo las relacionadas con contraseñas, uso de software y equipos, y protección de datos.
b. **Uso adecuado de equipos y recursos:** El trabajador debe utilizar los recursos tecnológicos proporcionados por la empresa de manera responsable, incluyendo el uso de contraseñas seguras y la protección física de equipos.
c. **Confidencialidad:** El trabajador debe mantener la confidencialidad de la información a la que tenga acceso, absteniéndose de divulgarla sin la debida autorización.
d. **Reportar incidentes**: El trabajador tiene la obligación de reportar cualquier incidente de seguridad, como el acceso no autorizado o la sospecha de que un sistema está comprometido, de acuerdo con los procedimientos establecidos por la empresa.
e. **Uso del correo electrónico:** El trabajador debe usar la cuenta de correo electrónico corporativo exclusivamente para actividades laborales y evitar enviar o recibir correos electrónicos no relacionados con su trabajo.

5. DIRECTRICES PARA LA SEGURIDAD DE LA INFORMACIÓN

a) P1. Política de Contraseñas Seguras

Una vez que el personal de EVOL recibe su usuario y contraseña con el cual puede ingresar a su correo electrónico corporativo y directorio activo, debe cambiar en su primer ingreso. Las siguientes son algunas indicaciones que deben seguir para crear contraseñas seguras, con el fin de evitar que personas no autorizadas tengan acceso a los sistemas de información de EVOL.

- Utilizar contraseñas que no sean fáciles de adivinar.
- Crear contraseñas con una longitud mínima de nueve caracteres. Deben incluir obligatoriamente letras mayúsculas, minúsculas, números y caracteres no alfanuméricos.
- Abstener de usar el mismo nombre de usuario como contraseña.
- Memorizar la contraseña. No la escriba.

- Cambiar la contraseña, mínimo cada 90 días o cuando sienta que la misma ha sido comprometida.
- Evitar la reutilización de contraseñas anteriores.
- Evitar el uso de combinaciones obvias de teclado, como por ejemplo "qwerty".

b) P2. Política de Uso de Controles Criptográficos

Se utilizarán controles criptográficos en los siguientes casos:

- Para proteger las credenciales de acceso a sistemas, datos y servicios.
- Para cifrar la información restringida transmitida mediante memorias USB o discos duros fuera del entorno organizacional.
- Para establecer conexiones seguras y encriptadas a internet cuando se acceda desde fuera de las oficinas de EVOL.
- Para la conexión a través de VPN, emplear aplicaciones cliente seguras como FortiClient, utilizando las credenciales de dominio asignadas al personal o las provistas por el cliente.

Los equipos utilizados deben contar con sistemas operativos Microsoft Windows 10 o 11 Professional, o macOS en el caso de dispositivos Apple. Para las aplicaciones de productividad, se debe utilizar Microsoft Office 365, proporcionado por la organización.

c) P3. Política de Seguridad con Sistemas Físicos

El personal de EVOL es responsable de custodiar y proteger tanto los elementos físicos como la información contenida en ellos, teniendo en cuenta las siguientes directivas para proteger dichos activos y su información:

- No dejar descuidados ni desatendidos los equipos de cómputo o cualquier elemento bajo su custodia.
- En caso de contar con un computador portátil asignado, garantizar que su ubicación sea segura y que no pueda ser retirado o sustraído fácilmente. Utilizar el cable de seguridad provisto para este propósito.
- Bloquear la sesión cada vez que se retire del puesto de trabajo.
- Apagar la estación de trabajo al dejar el área o al finalizar la jornada laboral, salvo cuando se requiera acceso remoto autorizado para atender incidencias o emergencias de clientes. En tales casos, coordinar previamente con el equipo de Soporte TI.
- La asignación de celulares para proyectos podrá ser gestionada si se considera necesaria, sin que esta sea de carácter obligatorio. En caso de realizarse dicha asignación, la responsabilidad sobre el uso adecuado, custodia y eventual devolución del equipo recaerá tanto en el usuario asignado como en su jefe inmediato.
- Mantener asegurados los cajones que contengan información o recursos informáticos bajo su responsabilidad.
- Evitar realizar acciones que pongan en riesgo su seguridad física, la integridad de los equipos o la información almacenada, así como evitar trasladar o manipular los equipos en condiciones inseguras que puedan exponerlos a daño o hurto.
- Suspender el uso de cualquier equipo electrónico (computadoras, portátiles, dispositivos móviles, tabletas) ante la detección o sospecha de infección por virus.
- No permitir que personas no autorizadas abran, desarmen, manipulen o modifiquen los equipos.
- Evitar el uso inadecuado o el daño físico a los equipos informáticos.
- Registrar cualquier activo que no forme parte del inventario de EVOL.

- Reportar cualquier incidente al equipo de Soporte TI de manera inmediata, en el momento de ocurrencia y no de forma posterior.
- El ingreso al edificio estará controlado y supervisado directamente por el personal de seguridad, quien gestionará el acceso y registro de visitantes. Solo el personal autorizado podrá ingresar.

d) P4. Política de Uso de Software Legal

Los empleados de EVOL solo podrán utilizar software legalmente adquirido y/o autorizado por la Empresa. Se puede hacer copia o duplicación de software licenciado por parte del personal, sólo cuando está explícitamente permitido en los términos y condiciones de la licencia. Si una persona requiere instalar un software específico, debe tener la aprobación formal del área de tecnología, área que analizará las implicaciones a nivel de licencia y uso que este software pueda tener en la infraestructura de TI y soluciones de información.

De acuerdo con lo anterior el usuario del software, debe abstenerse de:

- Copiar, vender, regalar o distribuir el software sin permiso del autor.
- Estimular, permitir, obligar o presionar al personal de Soporte de TI a crear o utilizar copias no autorizadas.
- Prestar los programas para que sean copiados.
- Utilizar hardware o software de monitoreo de actividades (analizadores de protocolos, software catalogado como "hacking", etc.) sin la debida autorización.
- Utilizar aplicaciones que no estén debidamente autorizadas por el área de Soporte TI.
- Utilizar software o servicios de red que permitan el intercambio de información sin el debido aval y autorización por parte del área de Soporte TI.
- Utilizar software que permita el control remoto sobre cualquier tipo de equipo conectado en la red de datos sin la debida autorización.
- Usar software o hardware que permita vulnerar o evadir los controles establecidos por EVOL
- No está permitido realizar modificaciones a los paquetes de software.D.
- Descargar o instalar nuevo software o aplicaciones sin informar y solicitar la autorización previa correspondiente.

e) P5. Política de Intercambio y de Confidencialidad de la información

El acceso a Internet es una herramienta que entrega **EVOL** a su personal para adelantar exclusivamente las labores propias de sus cargos y debe ser utilizada de manera austera y eficiente. Por ello, los siguientes son los lineamientos del buen uso de esta herramienta:

- Está prohibido ejecutar herramientas de hacking.
- Queda prohibido colocar información de EVOL, en cualquiera de sus formatos (Word, Excel, PowerPoint, PDF, AVI, MP3, MP4 o cualquier otro formato actual o futuro), en sitios de internet, discos, carpetas virtuales o cualquier sistema de publicación de documentos, dentro o fuera de las instalaciones de EVOL, excepto en los repositorios en nube autorizados por la empresa: OneDrive y SharePoint.
- Se prohíbe publicar material que pueda considerarse inapropiado, ofensivo, racial, sexual o irrespetuoso hacia otros, así como acceder a dicho tipo de contenido.
- Se prohíbe el acceso a portales de internet con contenido inapropiado, los cuales serán monitoreados; es responsabilidad de cada empleado no ingresar a páginas web con fines distintos a los laborales.

Todo el personal de EVOL debe tener en cuenta los siguientes lineamientos frente al uso de su cuenta de correo electrónico corporativa:

- La cuenta de correo corporativo asignada a cada colaborador es para uso exclusivo de las labores propias de su cargo. Se recomienda evitar el reenvío de correos electrónicos o agendas del buzón de EVOL a cuentas públicas como Gmail, Hotmail u otras, ya que estas no garantizan la seguridad de la información y pueden ser accesibles a personas no autorizadas.
- Queda prohibido el uso del correo electrónico para el envío de propaganda, ofertas, negocios personales, avisos publicitarios o cualquier información ajena a las actividades laborales.
- Está prohibido enviar correos con mensajes difamatorios, discriminatorios, de acoso o intimidación, así como imágenes o videos con contenido ilegal, racista, ofensivo, indecente, obsceno o sexualmente explícito.
- No se permite el envío de correos masivos sin la debida autorización.
- Todo correo electrónico de procedencia desconocida (SPAM) recibido en los buzones corporativos debe ser eliminado, ignorado y reportado al área de soporte técnico para evitar posibles infecciones por código malicioso o virus. EVOL implementará controles técnicos para prevenir la recepción de correos provenientes de estas fuentes. Es responsabilidad de los usuarios evitar la propagación de estos correos en cuentas corporativas o personales.
- Antes de responder un correo electrónico, se debe verificar si es necesario incluir el historial del mensaje. Enviar el historial sin confirmar si el destinatario debe conocerlo puede exponer información restringida a personas no autorizadas.
- El correo electrónico no debe ser utilizado como herramienta de mensajería instantánea.
- Los mensajes de correo electrónico tienen la misma validez legal que los documentos impresos y pueden ser utilizados como prueba ante la ley.

f) P6. Política de escritorio y pantalla limpia

EVOL exige que los colaboradores y partes interesadas, que tengan acceso a las instalaciones físicas de la empresa, sistemas de información y equipos de cómputos, mantengan sus escritorios libres de documentos o dispositivos de almacenamiento, guardándolos en sitios seguros, después de la jornada laboral o cuando no estén siendo utilizados.

No se permite tener accesos directos de información sensible en el escritorio del computador y el usuario debe bloquear sesión cuando se ausente de su puesto de trabajo y/o deje el equipo desatendido, para proteger el acceso a la documentación digital, aplicaciones y servicios de la empresa.

La información relacionada a su actividad laboral debe estar almacenada en los sitios seguros que ha habilitado la organización: OneDrive y SHAREPOINT.

g) P7. Política de disposición móviles y teletrabajo

Con el fin de garantizar la Integridad, Confidencialidad Y Disponibilidad de la información en un entorno de teletrabajo, se establece que EVOL debe proveer a los teletrabajadores los recursos necesarios para realizar su labor en su sitio en la que lo desarrollen y de acuerdo con las normas vigentes establecidas.

El equipo utilizado para el Teletrabajo puede ser:

- Computador asignado por la empresa, provisto con el licenciamiento para todo el software utilizado.
- VMWARE: software que permite el acceso a los datos de un servidor desde un equipo que únicamente brinda la interfaz requerida.
- Cliente de VPN proporcionado por EVOL.

La selección depende de los recursos disponibles y de las funciones que se vayan a ejecutar, lo cual será discrecional del responsable del área correspondiente.

La Actividad de Teletrabajo se realiza mediante conexión remota a los equipos de **EVOL.** La conexión remota a la red de área local de la empresa debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por el Área de Soporte TI.

Se recomienda que mientras se haga uso de VPN desde un equipo personal, éste tenga instalado y actualizado el antivirus y que el sistema operativo cuente con las actualizaciones de seguridad.

En general se deben aplicar todas las políticas de seguridad de la información de la empresa que sean pertinentes, y se hace énfasis en los siguientes aspectos:

- No está permitido que la sesión establecida con la empresa sea utilizada por una persona distinta al colaborador autorizado.
- Evitar conectarse desde sitios de acceso público, como cafés internet, aeropuertos, restaurantes, entre otros; en caso de hacerlo, es obligatorio el uso de una VPN para garantizar la seguridad de la conexión.
- Cumplir estrictamente con las condiciones establecidas en el formato de autorización para el alta de usuarios (contratación).
- Aplicar todos los requerimientos de seguridad definidos en la política de Seguridad de la Información para los activos involucrados, garantizando las restricciones y protecciones necesarias para la confidencialidad, integridad y disponibilidad de la información.
- Reportar cualquier evento anómalo siguiendo el procedimiento establecido para tal fin.
- Aunque EVOL no exige el uso de telefonía móvil corporativa, se recomienda que el personal utilice estos dispositivos de forma responsable, asegurando el uso de PIN o patrón de acceso, evitando almacenar información sensible y, en caso de ser necesario, garantizando la correcta eliminación de dicha información después de su uso.
- Cumplir con los lineamientos relativos a pantalla limpia y escritorio despejado, tal como se establece en el punto P6 de este documento.
- Mantener la seguridad física de los equipos en el lugar y entorno donde se realice teletrabajo.

h) P8. Política de Seguridad de la Información en las relaciones con los Proveedores

Mantener la Seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de Calidad y de Seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las Políticas de Seguridad de la Información de la empresa, las cuales deben se divulgadas por los responsables de la realización y/o firma de contratos o convenios. En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las Políticas de Seguridad de la Información. Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por la empresa. El Área de Soporte TI

deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información de la empresa.

i) P9. Política de Gestión de Accesos

El acceso a los sistemas informáticos de EVOL está regulado para garantizar la seguridad de los datos y servicios institucionales. Los accesos serán habilitados, modificados o deshabilitados bajo las siguientes condiciones:

i. Habilitación de accesos

- El área de Recursos Humanos (RRHH) es responsable de solicitar la creación de usuarios para nuevo personal, con copia al jefe inmediato, con un mínimo de 2 días hábiles de anticipación (48 horas) a la fecha de ingreso del trabajador.
- La solicitud se realiza vía correo, con copia al jefe inmediato, considerando la siguiente información:
  - Nombre completo del colaborador.
  - Fecha de ingreso.
  - Cargo y área.
  - Herramientas o sistemas a los que debe acceder.
  - Ubicación física (Lima o provincia).

ii. Modificación o restricción temporal de accesos

- En casos de vacaciones, descansos médicos o licencias prolongadas, el área de RRHH deberá notificar a Soporte TI la suspensión temporal de los accesos, con al menos 1 día hábil de anticipación, incluyendo en copia al jefe inmediato.
- La solicitud debe indicar claramente el periodo de suspensión y fecha tentativa de reactivación.

iii. Deshabilitación de accesos

- En caso de cese de personal, el área de Recursos Humanos debe informar al área de Soporte TI con al menos cinco (5) días hábiles de anticipación, con copia al jefe inmediato del colaborador. Esta comunicación anticipada es necesaria para gestionar la revocación oportuna de accesos (correo electrónico, dominio, aplicaciones, entre otros), así como para coordinar la devolución de activos asignados.

Firmado por:
Antonio Cadillo
E7A640B63BCE45C...

DocuSigned by:
Ticiano Muñoz
2924D98A0106464...

DocuSigned by:
Alberto Manrique
79EBC8D5EC3E454...

ALBERTO MANRIQUE MEDINA
GERENTE GENERAL

6. VIGENCIA DEL DOCUMENTO

El presente documento mantiene su vigencia mientras no se realicen modificaciones. En caso de actualizarse, la nueva versión entra en vigencia una vez sea aprobada formalmente mediante la firma del CEO.

7. CONTROL DE CAMBIOS

NÚMERO DE VERSIÓN	FECHA DE ACTUALIZACIÓN	RESPONSABLE	DESCRIPCIÓN DEL CAMBIO
01	20/06/2023	Leandro Alfonzo	Establecimiento inicial del documento. Se colocaron las Directrices de SI
02	09/06/2025	Josué Reyes	Se modificó el formato de la política. Se generaron los siguientes cambios: • Se agregó, vigencia del documento, Finalidad, Alcance, Definiciones, Lineamientos Generales y responsabilidades del trabajador • Se agregó la P9. Gestión de Accesos.