## POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de proporcionar a todos las partes interesadas de **TSNET S.A.**, las bases conceptuales, los principios y acciones que deben conocer, entender y cumplir con el fin de proteger los activos y recursos informáticos para mitigar el riesgo de fuga y/o pérdida de Información restringida a continuación se presentan las políticas de seguridad de la información:

DS La

DS TM

DS

### P1. Política de Control de Acceso

Una vez que el personal de TSNET S.A. 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 TSNET S.A.:

- Utilice contraseñas que no sean fáciles de adivinar.
- Construya contraseñas con una longitud mínima de nueve caracteres. Deben incluir obligatoriamente letras mayúsculas, minúsculas, números y caracteres no alfanuméricos.
- Absténgase de usar el mismo nombre de usuario como contraseña.
- Memorice la contraseña. No la escriba.
- Cambie la contraseña, mínimo cada 90 días o cuando sienta que la misma ha sido comprometida.
- Evite reutilizar contraseñas anteriores.
- Absténgase de usar combinaciones obvias de teclado, como por ejemplo "qwerty".

### P2. Política de Uso de Controles Criptográficos

Se utilizarán controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión en memorias USB o discos duros de información restringida, fuera del ámbito de la organización.
- Para la conexión segura y encriptada a internet fuera de la oficina de **TSNET S.A.**
- Para la conexión a través de VPN se utilizarán aplicaciones clientes seguras como: FortiClient, con las credenciales de dominio asignadas al personal o las que utilice el cliente.

Debe utilizarse equipos con licencias de Microsoft Windows Professional que ya viene instalado en los equipos con Windows 10 y aplicaciones de productividad Microsoft Office 365 que provee la organización.

### P3. Política de Seguridad con Sistemas Físicos

El personal de **TSNET S.A.** 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:

- Absténgase de dejar descuidados y/o desatendidos los equipos de cómputo o elementos que estén bajo su custodia.
- Si tiene asignado un computador portátil, utilícelo teniendo en cuenta que su ubicación sea realmente segura y que no pueda ser retirado o sustraído fácilmente. Use el cable de seguridad que se le ha proporcionado para este fin.
- Cada vez que se retire de su puesto de trabajo bloquee la sesión.

- Al dejar su área de trabajo o al final del día apague su estación de trabajo. A menos que necesitan conectarse remotamente a su equipo para atender incidencias (Emergencias) de clientes que pueden presentarse de último momento. Consulte con el equipo de Soporte TI la aplicación de acceso remoto autorizado.
- Asegure los cajones que contengan información o recursos informáticos asignados a su cargo.
- Absténgase de realizar acciones riesgosas o inadecuadas tanto para su seguridad física como para la del elemento y la información contenida en él y de trasladar o mover los equipos en condiciones no seguras, exponiéndolos a daño o hurto.
- Absténgase de continuar utilizando el equipo de cómputo, portátil, dispositivo móvil, tableta o cualquier otro elemento electrónico cuando se detecte o sospeche que el mismo se encuentre infectado por un virus.
- Abrir directamente o permitir a personas no autorizadas a desarmar los equipos, extraer, manipular y/o cambiar sus partes.
- No golpear o utilizar de forma inadecuada los equipos informáticos.
- El ingreso al edificio por el personal estará regido por un control biométrico y a su vez por personal de seguridad para el control de las visitas y registro de estas. Sólo podrá ingresar personal autorizado.

**P4. Política de Uso de Software Legal**

Los empleados de **TSNET S.A.** 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 **TSNET S.A.**
- No está permitido realizar modificaciones a los paquetes de software.

**P5- Política de Intercambio y de Confidencialidad de la información**

El acceso a Internet es una herramienta que entrega **TSNET S.A.** 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:

- Abstenerse de ejecutar herramientas de hacking.
- Abstenerse de colocar información de **TSNET S.A.** independientemente de su formato (Word, Excel, Power Point, pdf, avi, mp3, mp4 o cualquier otro formato actual o futuro) en sitios de internet o los denominados discos, carpetas virtuales o cualquier sistema de publicación de documentos, actual o futuro dentro o fuera de las instalaciones de **TSNET S.A.** que no sean los repositorios en nube autorizados por la empresa: OneDrive y SHAREPOINT.
- Abstenerse de publicar material que pueda ser considerado como inapropiado, ofensivo, racial, sexual o irrespetuoso a otros, y de igual manera no acceder a dicho tipo de material.

- El acceso a cualquier portal de internet con contenido inapropiado se encuentra prohibido y es monitoreado, por lo cual es responsabilidad de cada empleado abstenerse de ingresar a páginas web para fines diferentes a los laborales.

Todo el personal de **TSNET S.A.** 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 personal es para uso exclusivo de las labores propias del cargo. Por lo mismo, no está recomendado el reenvío de correos electrónicos ni de agendas del buzón de **TSNET S.A.** a cuentas de correo públicas como Gmail, Hotmail u otras. Recuerde que el uso de cuentas de correo público no está asegurado y la información que intercambie a través de este medio puede ser accedida por personas no autorizadas.
- No está permitido usar el correo electrónico para el envío de propagandas, ofertas, negocios personales, avisos publicitarios o cualquier otra información ajena a las labores que desempeña en su cargo.
- No está permitido el envío de correos con mensajes difamatorios, discriminatorios, de acoso o intimidación, imágenes o videos con contenido ilegal, racista, ofensivo, indecente, obsceno o con material sexual explícito.
- No está permitido el envío de correos masivos sin autorización.
- Todo correo electrónico de procedencia desconocida, llamado SPAM que sea recibido en los buzones de correo de **TSNET S.A.** debe ser eliminado, ignorado y reportado al área de soporte técnico con el fin de evitar posibles infecciones por código malicioso o virus. **TSNET S.A.** puede aplicar controles técnicos que prevengan la recepción de correos provenientes de estos individuos u organizaciones. Es responsabilidad de los usuarios la no propagación de dichos correos a cuentas corporativas o personales.
- Antes de responder un correo electrónico, valide si requiere incluir el historial del mismo. Enviar este historial sin validar si el remitente requiere o no tener conocimiento del mismo puede estar exponiendo información restringida a personas no autorizadas.
- Absténgase de usar el correo electrónico como una herramienta de mensajería instantánea.
- Recuerde que los mensajes de correo electrónico revisten la misma fuerza probatoria ante la Ley como la tienen los documentos impresos.

**P6. Política de escritorio y pantalla limpia**

**TSNET S.A.** 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.

**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 **TSNET S.A.** 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.
- Escritorio Virtual: 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 TSNET S.A.

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 **TSNET S.A.** 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 es permitido que la sesión establecida con la empresa sea utilizada por una persona diferente al colaborador autorizado.
- No hacerlo desde un sitio de acceso público como un Café Internet, Aeropuerto y Restaurante, entre otros y en caso de hacerlo es obligación el uso de VPN.
- Cumplir con las condiciones establecidas en el formato de autorización de alta de usuarios (Contratación).
- Se deben considerar los requerimientos de seguridad definidos en Seguridad de la Información para los activos de información involucrados, es decir aplicar todas las restricciones y protecciones para la confidencialidad, integridad y disponibilidad definidas.
- Reportar cualquier evento anormal aplicando el procedimiento asociado.
- Si bien **TSNET S.A.** no requiere el uso de telefonía móvil por parte de la empresa, se recomienda que el personal utilice dichos dispositivos de manera responsable, contando con un PIN o Patrón de acceso, no uso de información sensible y en caso de ser necesario, asegurarse de su correcta eliminación luego del uso.

**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.

**ALBERTO MANRIQUE MEDINA**

**GERENTE GENERAL**