POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI)

Tandem

Política Para La Seguridad De La Información
2021

ELABORÓ		REVISÓ		APROBÓ	
Nombre:	Jose Dueñas Medina	**Nombre:**	Sandra Paez	**Nombre:**	Jose Dueñas Medina
Cargo:	Director de Informática	**Cargo:**	Coordinador Comercial y Adm. Del SGC	**Cargo:**	Director de Informática
Fecha:	30/Jul/2021	**Fecha:**	30/Jul/2021	**Fecha:**	30/Jul/2021

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com

En virtud del fuerte compromiso de Tandem con el adecuado tratamiento de datos personales, garantizando además de la salvaguarda y seguridad de la información, en ejercicio del Habeas Data, la empresa establece la presente Política aplicable para la seguridad de la información en la organización.

DEFINICIONES

- **Requerimiento:** Documento que describe detalladamente el alcance de lo solicitado por el cliente interno en lo relacionado con sus necesidades de almacenamiento de información en los servidores de Tandem y/o cualquier equipo de cómputo de Tandem.
- **Objeto:** Nombre genérico con el que se puede referenciar un archivo electrónico de cualquier tipo. Ej. Archivos de tipo Word, Excel, Video, Sonido, Fotografías, imágenes Tiff, etc
- **SGC:** Sistema de gestión de calidad
- **Software:** Conjunto de programas o instrucciones de computador que permiten la automatización de operaciones y/o funciones para ejecutarse en el computador.
- **Software Autorizado:** Programas instalados en el servidor y/o estaciones cliente (PC´s) cuya licencia está en poder y a nombre de Tandem; Cuenta con la autorización del área de informática de Tandem y/o el vicepresidente de Tecnología y Proyectos para ser instalados y usados en los equipos de cómputo de Tandem.
- **Hardware:** Conjunto de elementos físicos que pueden hacer parte de la solución tecnológica (PC, Servidor)
- **Versión:** muestra el estado de los documentos en términos de actualidad
- **Solicitante:** Es el cliente interno o Externo que realiza la solicitud. El cliente interno puede ser el área comercial que entrega las especificaciones de un contrato a ejecutar.
- **Freeware:** Es aquel software que se distribuye sin cargo (sin costo), puede estar acompañado de su código fuente o no.
- **Shareware:** Es aquel software que se distribuye sin cargo (sin costo) por un período determinado, luego del cual el usuario deberá optar entre pagar su licencia o desinstalarlo del o los computadores donde esté funcionando.
- **Donaware:** Es aquel software que se distribuye sin obligación de cargo (sin costo) pero que solicita una contribución a cambio de su uso.
- **Payware:** un término que no suele usarse ya que se refiere al software licenciado y por lo cual siempre se deberá pagar para utilizarlo.
- **Encriptación:** (Cifrado, codificación). La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros.
- **Equipo Activo:** Equipo Informático asignado a un proyecto de implementación.

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com

- **Backup:** Copia de seguridad o respaldo que se realiza con el objeto de contar con los medios e información fuente de un sistema, que facilite su recuperación en caso de un incidente de falla o recuperación ante un desastre.

1. OBJETIVO

La presente Política establece las directrices generales para la Seguridad de la Información al interior de Tandem, con el objetivo de brindar las condiciones de seguridad necesarias que impidan la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a la información que es tratada por Tandem.

2. ALCANCE

Esta Política de Seguridad de la Información será aplicada en todos los aspectos administrativos, de gestión, logísticos y de control fijados por la empresa, que deben ser cumplidos por los directivos, funcionarios, contratistas, terceros que presten sus servicios, empleados de terceros proveedores que estén regulados por términos contractuales, y en general todas aquellas personas que tengan algún tipo de relación con la manipulación de información en Tandem.

3. POLÍTICAS ESPECÍFICAS PARA EL TRATAMIENTO DE DATOS PERSONALES.

3.1 INSTALACIÓN DE SOFTWARE

Propósito: Minimizar el riesgo de exposición y de infección por malware, evitando a su vez posibles sanciones por el uso de software sin licenciar.

Política

Es responsabilidad de cada usuario de equipo de cómputo velar por la NO instalación de software no autorizado; es decir, no está permitido instalar software, herramientas Windows o Web (Ej. Google Search), protectores de pantalla, mensajería instantánea, software libre (en cualquiera de sus modalidades), así como software de cámaras o dispositivos como celulares o periféricos que no sean de Tandem y que no tengan una relación directa y justificada con alguno de proyectos o actividad que realiza el usuario.

Los trabajadores no deben instalar software en los dispositivos de la compañía sin la respectiva autorización. Las peticiones de instalación de software deben ser aprobadas por el administrador de la red y el proceso de instalación debe ser realizado por personal calificado de la compañía.

Todo software que sea instalado debe tener licenciamiento comercial, ser de licenciamiento libre (open source, free, trial), o en su defecto la licencia debe provenir del departamento de tecnología.

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com

3.2 USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

Propósito: Minimizar el riesgo de exposición de información de la empresa o de infección por malware contenido en dispositivos externos de almacenamiento (Discos Duros externos, USBs, CDs, Diskettes, Teléfonos Celulares, Reproductores Multimedia, etc).

Política

Está prohibido el uso de dispositivos de almacenamiento personales físicos o en la nube (Google Drive, OneDrive o similares) sin verificar y confirmar la autenticidad y seguridad que provee el repositorio que usará y sin aplicar la encriptación de los datos que almacenará en esos repositorios ya sea desde de la infraestructura tecnológica de la compañía o fuera de ella. En caso de requerirse alguno de estos dispositivos, se debe obtener la aprobación de uso por el vicepresidente de Tecnología y Proyectos o el Director de Informática indicando la razón o necesidad y el proyecto o actividad relacionado con dicha necesidad.

Todo requerimiento de instalación de software y/o periféricos debe ser autorizado por el director de informática y/o vicepresidencia de tecnología y proyectos. Se excluye de la necesidad de obtener la aprobación a los funcionarios de informática siempre y cuando el software o el periférico estén relacionados con el proyecto, especialidad y/o actividad asignada.

Solo los directores, vicepresidentes y funcionarios de informática, están autorizados para el uso y transferencia de información mediante dispositivos removibles como USBs, CDs o DVDs. Si un Director o Vicepresidente requiere autorizar a un funcionario para el uso de estos dispositivos, debe formalizar su solicitud mediante el procedimiento de soporte técnico e informático dirigido al Director de informática.

3.3 USO DEL INTERNET EMPRESARIAL Y POLÍTICA DE MONITOREO

Propósito: El propósito de esta política es definir los estándares para el monitoreo y limitación de la navegación por Internet desde cualquier dispositivo en la red empresarial. Estos estándares están diseñados para asegurar que los empleados utilicen el Internet de forma segura y responsable.

Política

La gerencia está en potestad de monitorear todas las comunicaciones entrantes y salientes dentro de la red de la organización. Esto incluye conocer la IP de origen, la fecha, la hora, el protocolo, el servidor o dirección de destino y los datos comunicados.

La gerencia puede bloquear los sitios de Internet que se consideren inapropiados para el ambiente empresarial. Se considera una falta disciplinaria bajo cualquier circunstancia el acceso a páginas y sitios web de contenido sexual explícito, sitios de juegos o apuestas, sitios relacionados con sustancias ilícitas, sitios de citas y redes sociales, sitios de fraude, contenidos SPAM o en relación a

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com

delitos tipificados por la ley colombiana, contenido racista o de alguna forma ofensivo y discriminatorio, contenido violento, y todo contenido que no esté relacionado con el desarrollo de las finalidades de la empresa sin que medie previa autorización.

Así mismo está totalmente prohibido el uso de la infraestructura empresarial para acceder a sitios de mensajería o correo personal, realizar ataques informáticos o similares. Además, está prohibido el uso del Internet en horas no autorizadas para acceder a contenido multimedia no asociado a la labor del empleado.

Cualquier intento por evadir los controles técnicos impuestos, será considerado en sí mismo una falta disciplinaria.

3.4 MANEJO DE CLAVES

Propósito: El propósito de esta política es establecer un estándar de generación de contraseñas seguras, la protección de dichas contraseñas y su frecuencia de cambio.

Política

Todas las contraseñas de nivel de sistema (root, administrador de servidores Windows), deben ser cambiadas al menos cada tres meses.

Todas las contraseñas de nivel de usuario Windows, deben ser cambiadas al menos 42 días.

Todas las contraseñas utilizadas deben seguir las condiciones descritas a continuación: Contener al menos tres de los siguientes caracteres: Minúsculas, Mayúsculas, Números, Caracteres especiales (e.g. #$%&/(“!.;), la longitud de la contraseña debe ser de al menos 7 caracteres, la contraseña no debe estar compuesta únicamente de palabras de diccionario o contener parte de la cuenta del usuario, se deben evitar contraseñas tradicionales como password, 123456, qwerty, asdfg, etc.

Como base del correcto manejo de claves y contraseñas se presentan una serie de recomendaciones para el manejo correcto de las mismas:

- Siempre utilice contraseñas diferentes para los servicios de la compañía y sus cuentas personales no relacionadas al ámbito laboral.
- No comparta sus contraseñas con ningún tercero, incluso si este pertenece a la organización.
- Las contraseñas nunca deben estar escritas en texto plano (jamás archivos llamados claves.txt y en el escritorio).
- No revele las contraseñas por medios de comunicación desprotegidos como correo, mensajería instantánea, SMS, etc.
- Evite utilizar la opción de recordar contraseña en navegadores y programas internos.

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com

3.5 USO DE CORREO ELECTRÓNICO Y COMUNICACIONES PERSONALES

Propósito: Prevenir daños y perjuicios en la imagen y/o el nombre de la organización por el manejo incorrecto de los servicios de comunicación.

Política

Los diferentes medios de comunicación a disposición de los trabajadores no deben ser utilizados para la distribución de mensajes con contenido ofensivo, racista, discriminatorio, pornográfico, sexual, político, etc. Los empleados que reciban comunicaciones con este contenido deben eliminarlo inmediatamente y reportar el incidente si es de origen interno.

Utilizar los correos empresariales para comunicaciones personales está prohibido. En especial si es para la distribución de mensajes cadena, spam o de alguna forma comerciales y/o para suministrar información de carácter confidencial o no, de propiedad de la empresa y/o que le empresa esté usando dentro del desarrollo de sus actividades comerciales o en razón de su objeto social.

Los empleados no deben esperar privacidad alguna en contenido que almacenen o envíen como parte de los servicios de comunicación de la compañía. El no cumplimiento de las condiciones mencionadas anteriormente es considerado una falta disciplinaria y puede ser objeto de sanción.

3.6 CONFIDENCIALIDAD CON TERCEROS

Propósito: Establecer los requerimientos de confidencialidad en las relaciones con proveedores, contratistas, en particular con empleados y los terceros en general.

Política

Para el desarrollo de las relaciones contractuales, comerciales y laborales, se debe exigir a los terceros la aceptación de los acuerdos de confidencialidad definidos por la organización. En dichos acuerdos se debe establecer el compromiso de salvaguardar la información, velar por su correcto uso, impedir el uso no autorizado de dicha información y guardar reserva. Se debe estipular a su vez la información que es objeto de protección dentro del acuerdo y su temporalidad.

Los acuerdos deben incluirse dentro de los contratos celebrados entre la organización y terceros, como parte integral del contrato o firmarse como un acuerdo independiente.
La aceptación de las condiciones de confidencialidad es indispensable para conceder al tercero el acceso a la información protegida.

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com

3.7 LA SEGURIDAD FÍSICA Y AMBIENTAL

Propósito: Evitar el acceso físico no autorizado, daños e interferencia para la información de la organización y/o información custodiada en razón de su actividad comercial y las instalaciones de procesamiento y almacenamiento de información.

Política

Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado. El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos. El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la intercepción, interferencia o daños. Los equipos de cómputo deben tener un correcto mantenimiento para asegurar su continua disponibilidad e integridad.

Los equipos, la información o el software no se sacarán de las instalaciones de la empresa sin la previa autorización. Se aplicará seguridad a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Todos los elementos del equipo que contienen los medios de almacenamiento deberán ser verificados para garantizar que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Los usuarios deberán asegurarse de que el equipo que no cuenta con vigilancia tenga la protección adecuada.

Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador este desatendido deberá bloquearse la pantalla.

Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.

Solo el personal autorizado tiene acceso a las áreas de almacenamiento de documentación e información física de la empresa y áreas de custodia asignadas a información de nuestros clientes.

3.8 REQUISITOS PARA EL CONTROL DE ACCESO

Propósito: Limitar el acceso de la información y a las instalaciones de procesamiento de la información.

Política

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com

Los colaboradores responsables de las áreas seguras de la empresa tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- Las áreas de producción se catalogan como seguras y deben permanecer cerradas y custodiadas.
- El acceso a áreas seguras donde se procesa o almacena información confidencial y restringida, es limitado únicamente a personas autorizadas.
- El acceso a áreas seguras requiere esquemas de control de acceso, como tarjetas, llaves o candados.
- El responsable de un área segura debe asegurar que no ingresen cámaras fotográficas, videos, teléfonos móviles con cámaras, salvo se tenga una autorización expresa.
- Se utilizan planillas para registrar la entrada y salida del personal.
- Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.

3.9 COPIAS DE SEGURIDAD

Propósito: Evitar la pérdida de información de la empresa mediante la implementación de algún medio de respaldo que pueda ser utilizado con el objeto de contar con los medios e información que facilite su recuperación en caso de un incidente de falla o recuperación ante un desastre.

Política

Las copias de seguridad de la información se ejecutarán cada fin de semana, las cuales se almacenarán en medios magnéticos y serán custodiadas por Tandem.
También será posible ejecutar copias de seguridad con frecuencia diferente o en eventos que ameriten obtener copias de respaldo en fechas y horas no definidas dentro de esta política, al igual que su almacenamiento y conservación en medios adecuados diferentes a los aquí descritos.

Los funcionarios responsables de la gestión del almacenamiento y respaldo de la información deberán proveer los recursos necesarios para garantizar el correcto tratamiento de la misma.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben definir las estrategias para la correcta y adecuada generación y rotación de las copias de respaldo de la información. Tandem cuenta con medios de almacenamiento magnético a usar en sus copias de seguridad o respaldo para mantener un ciclo durante dos semanas adicional al último backup realizado.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben velar por el cumplimiento de los procedimientos de respaldo de la información.

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com

3.10 REGISTRO DE ACTIVIDAD Y SUPERVISIÓN

Propósito: Registrar eventos y generar evidencia.

Política

Se producirán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Los registros de información se protegerán contra la manipulación y el acceso no autorizado. Las actividades del administrador del sistema y de la red serán registradas.

Estos registros serán protegidos y regularmente revisados.

Los relojes de todos los sistemas de informática relevantes serán sincronizados a una fuente de tiempo de referencia única.

3.11 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Propósito: Garantizar que la seguridad informática sea implementada y aplicada de acuerdo con las políticas y procedimientos de la organización.

Política

Los sistemas de información son revisados regularmente a través de Auditorias para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de la entidad.

El área de informática, sin previo aviso, podrá eliminar y remover todo software, periférico y objetos que encuentre instalado en cualquier equipo de cómputo de Tandem que no tenga la debida autorización y no puede responder por información, perjuicios, daños y/o retrasos en las actividades propias de cada usuario causadas por no seguir estas recomendaciones.

4. PROCESO PARA LA ATENCIÓN DE INCIDENTES

Toda vez que se presente algún incidente con la seguridad de la información tratada por Tandem deberá adelantarse el siguiente procedimiento:

1). **Reporte del Incidente:** Ocurrido el incidente de seguridad, la primera persona que tenga conocimiento del mismo y en el menor tiempo posible, deberá presentar un informe detallado del mismo, dirigido al área o persona encargada de la seguridad de la información en la dirección de informática.

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com

2). **Comunicación del Incidente ante la SIC:** Todo incidente de seguridad de la información, deberá ser reportado ante la Superintendencia de Industria y Comercio, específicamente ante el Registro Nacional de Bases de Datos -RNBD-.

3). **Reunión del comité de Seguridad de la información:** El área o persona encargada de la seguridad de la información en la dirección de informática conformara de forma extraordinaria la una reunión de un Comité para la seguridad de la información, en el cual se desarrollarán los siguientes ítems.

   a. **Emisión del concepto técnico:** Evaluados los Hechos del caso se deberá dar un concepto técnico que determina todas las contingencias surgidas en el caso en concreto.
   b. **Identificación de la falencia:** Como resultado del concepto técnico, se deberá identificar plenamente la falencia que dio paso al incidente de seguridad de la información.
   c. **Toma de Medidas:** El comité deberá tomar las medias y los correctivos necesarios para evitar futuros incidentes.

5. MODIFICACIÓN DE LAS POLÍTICAS

Tandem se reserva el derecho de modificar la presente Política de Seguridad de la información en cualquier momento, comunicando de forma oportuna a todas aquellas personas que estén relacionadas o que participen en la manipulación de la información de la empresa para su correcta implementación.

Tandem S.A.S
Teléfonos: (57)(1) 311 1099 - (57)(1) 311 3884
Dir: Cra. 65 # 81 - 81 / Bogotá D.C
www.tandemweb.com