PHOENIX TOWER
INTERNATIONAL

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE PHOENIX TOWER INTERNATIONAL

EN VIGOR A PARTIR DEL 15 DE AGOSTO DE 2023

OBJETIVO

Phoenix Tower US Holdings, LP y sus subsidiarias y filiales en todo el mundo (colectivamente, "PTI", "Phoenix Tower" o "Empresa") están comprometidas con la protección de la seguridad de la información, el aprendizaje y la mejora continuos, tal y como se establece en esta Política de Seguridad de la Información (la "Política"). El alcance de esta Política pretende ser exhaustivo e incluirá las obligaciones de la Empresa en materia de seguridad y protección de los activos de PTI, incluida la Información de Identificación Personal ("PII"), de toda la Empresa y de sus proveedores autorizados, tanto dentro como fuera de sus instalaciones. Todos los empleados deben revisar y respetar la información contenida en esta Política.

ÁMBITO DE APLICACIÓN

Esta Política se aplica a todos los empleados y proveedores de Phoenix Tower que respaldan a Phoenix Tower y sus activos de información o que interactúan con ellos. Cada sección de esta Política se aplica a aspectos específicos del programa de seguridad de la información de PTI.

DEFINICIONES

- **Información confidencial: Incluye, entre otros,** toda la información material, no pública, relacionada con el negocio, los derechos de propiedad intelectual, los secretos comerciales, los conocimientos comerciales, ya sea en forma escrita u oral, estén indicados o no como tal, relacionados con asuntos como la estrategia comercial, los procesos, las finanzas, los planes de marketing, los contratos y/o la tecnología. A continuación figuran algunos ejemplos:
    - contratos, tanto ejecutados como en borrador;
    - material de marketing en desarrollo; o
    - previsiones de ventas o ingresos.
- **Seguridad de la información:** Los procesos y metodologías que se diseñan y aplican para proteger la información o los datos, impresos, electrónicos o de cualquier otro tipo, confidenciales, privados o sensibles del acceso, uso, uso indebido, divulgación, destrucción, modificación o interrupción no autorizados.
- **Empleado:** Persona física identificada o identificable que actúa como director, funcionario, miembro del equipo, empleado, contratista o asesor de PTI, ya sea a tiempo completo o parcial, de forma temporal o indefinida.
- **Dispositivos orientados al usuario final:** Cualquier herramienta o dispositivo tecnológico utilizado por un empleado de PTI para almacenar información o acceder a los sistemas de PTI, incluido el correo electrónico. Entre los ejemplos de dispositivos orientados al usuario final, se incluyen los ordenadores, portátiles, teléfonos inteligentes, discos duros externos y almacenamiento USB.
- **Información de Identificación Personal ("PII"):** Cualquier dato que pueda identificar a una persona concreta, como nombre, dirección, correo electrónico,

información financiera, número de seguridad social, pasaporte, etc.

SUPERVISIÓN POLÍTICA

Phoenix Tower considera la seguridad de la información uno de los aspectos más importantes de su actividad.

- La alta dirección de Phoenix Tower predicará con el ejemplo al garantizar que la seguridad de la información sea de alta prioridad en todas las actividades e iniciativas comerciales actuales y futuras.
- El Director Jurídico Global revisará esta Política y cada uno de sus apéndices anualmente con el fin de garantizar que sean oportunos y estén actualizados, y se revisarán, cuando sea necesario, para comprobar que sean adecuados a la luz de las obligaciones legales, la tecnología y las necesidades empresariales.
- La dirección transmitirá las correspondientes revisiones de esta política a todo el personal por diversos medios, como actualizaciones electrónicas, sesiones informativas, formación, boletines, etc.

Para cumplir o superar estos objetivos, se han puesto en marcha las siguientes prácticas:

- Los empleados firman un aviso de recepción, revisión y aceptación de la Política de Seguridad de la Información cuando son contratados o se renueva su contrato.
- El personal recibirá un refuerzo de formación periódicamente para que la seguridad de la información siga siendo prioritaria.
- La formación en seguridad de la información es preceptiva desde el primer momento, empezando por la incorporación de los empleados. Toda formación técnica debe ser pertinente para las responsabilidades de la función laboral. Cuando los miembros del personal cambian de puesto de trabajo o de funciones, sus necesidades de seguridad de la información deben reevaluarse, y debe impartirse nueva formación de forma prioritaria.

1. ORGANIZACIÓN DE SEGURIDAD

1.1 DEFINICIÓN DE FUNCIONES Y RESPONSABILIDADES

En PTI se establecen las siguientes funciones relacionadas con la Seguridad de la Información:

FUNCIONES	RESPONSABILIDADES
Director de Tecnología de la Información	Determinar los requisitos de seguridad de los servicios prestados, evaluando el impacto de un incidente que pueda afectar a la seguridad de los servicios en detrimento de

	la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.
Director de Tecnología de la Información	Determinar los requisitos de seguridad de la información tratada, evaluando el impacto de un incidente que pueda afectar a la seguridad de los servicios en detrimento de la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.
Director de Tecnología de la Información	Determinar las decisiones para cumplir con los requisitos de seguridad de la información y los servicios, supervisando la aplicación de las medidas necesarias e informando sobre estas cuestiones.
Gerente Sénior de Tecnología de la Información	Responsable de desarrollar el modo específico de implementar la seguridad de los sistemas y de supervisar su funcionamiento diario, pudiendo delegarlo en los administradores u operadores bajo su responsabilidad.
Gerente Sénior de Tecnología de la Información	Responsable de las tareas técnicas de seguridad y de quién las ejecuta.

2. INFORMACIÓN DE IDENTIFICACIÓN PERSONAL

Este apartado tiene por objeto orientar en la protección de la PII de propietarios, inquilinos, clientes potenciales y empleados, y ayudará a estos últimos a determinar qué información puede ser revelada a terceros, así como respecto a la sensibilidad relativa de la información que no se revelará a entidades ajenas a Phoenix Tower sin la debida autorización.

2.1 Definiciones

Phoenix Tower reconoce la necesidad de mantener la confidencialidad de la PII y entiende que dicha información es única para cada persona y que, generalmente, se limita a los datos pertinentes y necesarios para sus fines. La PII amparada por esta Política puede provenir de diferentes tipos de personas que realizan tareas en nombre de la Empresa, y que incluyen a empleados, solicitantes/candidatos, contratistas independientes y cualquier PII mantenida en su base de clientes. La PII incluye toda información que permita identificar a propietarios, inquilinos, clientes potenciales y empleados:

- información de contacto personal (números de teléfono, direcciones, etc.);
- número de la seguridad social (o su equivalente emitido por entidades

gubernamentales no estadounidenses);
- número de identificación fiscal (o su equivalente emitido por entidades recaudatorias gubernamentales no estadounidenses);
- número de identificación del empresario (o su equivalente emitido por entidades gubernamentales no estadounidenses);
- número de permiso de conducir estatal o extranjero o copia de tarjeta de identificación;
- número de pasaporte o sus copias;
- fecha de nacimiento;
- número de tarjeta de crédito o débito corporativa o individual (incluido el número PIN o de acceso) conservado en los registros de la organización o de proveedores acreditados; o
- información de la cuenta bancaria de PTI o de socios comerciales.

La PII se puede encontrar en copias impresas o en registros electrónicos; ambas formas se encuentran dentro del ámbito de aplicación de esta Política.

2.2 Almacenamiento y tratamiento de la información que contiene PII

PII electrónica

La PII puede almacenarse electrónicamente mediante distintos métodos y en varios dispositivos orientados al usuario final, incluidos, entre otros, los siguientes:

- Dispositivos informáticos móviles (es decir, ordenadores portátiles, teléfonos inteligentes, tabletas, ordenadores, PDA, etc.).
- Correo electrónico, Internet y programas de mensajería instantánea que almacenan, procesan o transmiten datos.
- Soportes electrónicos extraíbles, como unidades USB, unidades de CD, discos duros externos, etc., solo se deben utilizar para PII no sensible. La PII confidencial, como el número de seguridad social, la información de pasaporte, los datos bancarios u otros datos financieros, no debe almacenarse en soportes electrónicos extraíbles.
- Servidores locales y en la nube propiedad de PTI.
- Servidores basados en la nube de terceros.

Este apartado de la Política establece los requisitos, y el proceso de aprobación de los dispositivos orientados al usuario final que son propiedad de PTI, que están administrados por ella o que esta alquila. Cualquier dispositivo orientado al usuario final que no sea propiedad de PTI, ni sea alquilado o administrado por esta no podrá acceder a ningún servidor local que contenga PII ni retirarlo, a menos que lo haya autorizado, por escrito, el Director Jurídico Global.

- **Dispositivos informáticos móviles (es decir, ordenadores portátiles, teléfonos inteligentes, tabletas, PDA, etc.)**: La PII se puede almacenar en

dispositivos informáticos móviles, aunque estos deben estar protegidos con contraseña, encriptados y tener una función de borrado remoto. Este no es el método preferido para almacenar la PII. La información almacenada en dispositivos informáticos móviles debe considerarse incluida en un punto de almacenamiento temporal, y debe trasladarse la PII a un servidor de PTI tan pronto como sea posible.

- **Correo electrónico, Internet y programas de mensajería instantánea:** La Empresa no recomienda transmitir PII a través de Internet o por programas de mensajería instantánea. Cuando se vaya a transferir PII por correo electrónico, se deberán seguir estos pasos con el fin de garantizar una transmisión segura y minimizar el riesgo de una infracción después de que se confirme que dicha PII se ha guardado en el servidor local:
    1. Proteger el documento con contraseña, ya sea en pdf, word o excel. Si el documento se encuentra en un formato difícil de proteger (por ejemplo, gif o jpeg), convierta el archivo a pdf, protéjalo con contraseña y vuelva a guardarlo. El formato "original" se puede borrar en este momento y eliminarse de la papelera.
    2. Enviar el documento por correo electrónico con la mención de "**CONFIDENCIAL**" como etiqueta a continuación del nombre del asunto en el asunto.
    3. Comunicarse con el destinatario por teléfono para confirmar que recibió el correo electrónico y proporcionarle la contraseña. ***NUNCA ENVÍE LAS CONTRASEÑAS POR CORREO ELECTRÓNICO***
    4. Eliminar el archivo adjunto del correo electrónico enviado.

La PII confidencial, como el número de seguridad social, la información de los pasaportes y los datos bancarios u otros datos financieros, **no** se debe enviar por correo electrónico.

Si PTI recibe la PII a través de Internet o por programas de mensajería instantánea, o por cualquier otro medio inseguro, esta información deberá transferirse inmediatamente al servidor de PTI (primera preferencia) o a un dispositivo informático móvil y, a continuación, borrarse permanentemente del programa en el que se recibió.

- **Medios electrónicos extraíbles:** La PII se puede almacenar en soportes electrónicos extraíbles, como unidades USB, con el fin de transportar información entre soportes. Los dispositivos de soportes extraíbles deben estar protegidos con contraseña y encriptados. Este no es el método preferido para almacenar la PII. La información almacenada en soportes electrónicos extraíbles debe considerarse incluida en un punto de almacenamiento temporal, y la PII se debe trasladar a un servidor de PTI lo antes posible y eliminarse de dichos soportes. La PII confidencial, como el número de seguridad social, la información de pasaporte, los datos bancarios u otros datos financieros, **no** debe almacenarse en soportes electrónicos extraíbles.
- **Servidor local o en la nube propiedad de PTI**: El lugar preferido para el

almacenamiento de toda la PII son servidores locales o la nube propiedad de PTI, y este método debe utilizarse en primer lugar cuando esté disponible. Todas las carpetas y los datos que contengan PII deben estar claramente identificados como tales, y el acceso a dichas carpetas estará restringido únicamente a aquellos empleados que deban tener acceso en el desempeño diario de su trabajo.

- **Almacenamiento de documentos impresos (interno):** La PII almacenada en las oficinas debe asegurarse en cajones cerrados con llave y, preferiblemente, tras puertas cerradas también con llave. El acceso a estos lugares debe estar restringido a aquellos empleados que necesiten la información en el desempeño de sus funciones diarias. Las llaves de dichos lugares protegidos deben estar en posesión exclusiva del jefe del departamento, y todo momento en que los empleados accedan a ellos debe documentarse en un formato de registro. En ningún caso, se retirarán de la oficina documentos que contengan PII, y cualquier supuesto que requiera esta retirada requerirá la aprobación del director general. Toda la información, datos y documentos que contengan PII deben estar claramente identificados para que todos los usuarios sean conscientes de la propiedad, clasificación y valor de la información. La información, datos y documentos que contengan PII se transportarán y destruirán de forma segura para protegerlos de una divulgación no intencionada. La información, datos y documentos que contengan PII se almacenarán de forma segura cuando no se utilicen.
- **Almacenamiento de documentos impresos (externo):** Por lo general, no se permite el almacenamiento externo de PII en formato impreso sin la aprobación por escrito del CEO. Los datos que contengan PII en formato impreso no deben enviarse a centros de almacenamiento externo como parte de los archivos del sitio y, en ningún caso, deben almacenarse en el domicilio de los empleados. Toda la información, datos y documentos que contengan PII deben estar claramente identificados para que todos los usuarios sean conscientes de la propiedad, clasificación y valor de la información. La información, datos y documentos que contengan PII se transportarán y destruirán de manera segura para protegerlos de una divulgación no intencionada. La información, datos y documentos que contengan PII se almacenarán de forma segura cuando no se utilicen.
- **Transporte de documentos impresos:** Cuando la PII deba transportarse fuera de las oficinas en situaciones autorizadas, solo deberán hacerlo los empleados directos de PTI. Deberán tomarse las precauciones necesarias para garantizar que los datos que contienen PII estén protegidos (maletín cerrado con llave, etc.) y que están en todo momento en posesión del empleado durante el transporte.
- **Copias impresas:** Se debe evitar en la medida de lo posible la impresión de los datos que contengan PII y que estén almacenados electrónicamente. En situaciones en las que no sea posible, el empleado que imprima los datos deberá recibir la previa autorización del jefe del departamento, indicando qué material está imprimiendo y por qué razón. El empleado también será responsable de la destrucción de las copias impresas y proporcionará al jefe del departamento una declaración de la fecha de la destrucción, de su descripción y del método utilizado.

2.3 Acceso a la PII por los empleados

Cada jefe de departamento se encarga de identificar y mantener una lista de los usuarios de su departamento que deben tener acceso a los archivos (electrónicos o en papel). La lista debe actualizarse cuando sea necesario y, como mínimo, revisarse anualmente y cuando se produzca un acontecimiento relacionado con el personal (por ejemplo, contratación, separación, terminación, promoción). La lista se proporcionará al Departamento de TI, que a su vez se encargará de garantizar que el acceso a los archivos en soporte informático que contengan PII esté restringido de acuerdo con la lista. Cada jefe de departamento se encargará de garantizar que el acceso a los archivos impresos que contengan PII esté restringido de acuerdo con la lista. Los jefes de departamento y/o los responsables que estos designen deben revisar el acceso de los usuarios ante cualquier cambio que se produzca en las funciones y responsabilidades laborales de una persona afectada, o en su estado de empleado/contratista independiente (incluido, entre otros, el despido), y comunicar cualquier cambio oportunamente a TI.

2.4 Requisitos normativos

Es política de la Empresa cumplir con los estatutos y normas internacionales, federales o estatales con respecto al acceso, al uso, al almacenamiento y la retención de PII. Los Departamentos Jurídicos y/o de Cumplimiento Normativo de Phoenix Tower supervisarán todos los aspectos de cumplimiento normativo. Si alguna disposición de esta Política entra en conflicto con algún precepto legal de la legislación internacional, federal o estatal que rige la PII, la(s) disposición(es) en conflicto será(n) reemplazada(s).

2.5 Formación

Todos los nuevos empleados que se incorporan a la Empresa reciben una formación introductoria sobre la correcta gestión y protección de la PII, además de recibir una copia de esta Política y de los procedimientos de aplicación del departamento al que están asignados (si corresponde). Los empleados que ocupan puestos con acceso habitual continuo a la PII, o los que son transferidos a dichos puestos, reciben una formación que refuerza esta Política y los procedimientos para la conservación de los datos de PII. Además, recibirán formación relativa a la seguridad y protección de los datos de PII y de los datos de la propiedad de la empresa, al menos, una vez al año. La formación correrá a cargo del Departamento de TI y formará parte de la formación para nuevos empleados cuando estos se incorporen. Si un empleado existente es añadido a la lista de acceso de PII, recibirá formación por separado en cuanto a las disposiciones de esta Política.

2.6 Confirmación de confidencialidad

Todos los empleados de la Empresa deben mantener la confidencialidad de la PII, así como de la información confidencial a la que puedan tener acceso, y entender que dicha PII debe estar restringida únicamente a aquellos que tienen la necesidad comercial de conocerla.

2.7 Infracciones de seguridad/de datos de PII

Si un Empleado tiene conocimiento de cualquier uso, acceso o transferencia de PII que entre en conflicto con esta Política, o de cualquier incidente de seguridad, deberá comunicarlo de inmediato al Departamento Jurídico de Phoenix Tower. Las bases de datos o los conjuntos de datos que incluyen PII pueden infringirse de forma inadvertida o a través de una intrusión ilícita. Consulte la sección 6 de esta Política para obtener más información.

2.8 Infracciones de las políticas y procedimientos de PII

Phoenix Tower considera que la protección de los datos de PII es de máxima importancia. La infracción de esta Política o de sus procedimientos dará lugar a medidas disciplinarias, que pueden incluir la suspensión o terminación del contrato en el caso de infracciones graves o reiteradas.

2.9 Control del uso de los sistemas informáticos

La Empresa tiene el derecho y la capacidad de controlar la información electrónica generada y/o comunicada por las personas que utilizan los sistemas y redes de la Empresa, incluidos los mensajes de correo electrónico e Internet. No es política ni intención de la Empresa controlar continuamente todo el uso de los ordenadores por parte de los empleados o de otros usuarios de los sistemas informáticos y de la red de la Empresa. Sin embargo, los usuarios de los sistemas deben ser conscientes de que la Empresa puede controlar, entre otros, los patrones de uso de Internet (por ejemplo, el sitio al que se accede, la duración de la conexión o la hora del día del acceso), así como los archivos y mensajes de los empleados, en la medida en que sea necesario, para garantizar que Internet y otras comunicaciones electrónicas se utilicen conforme a la ley y a la política de la Empresa. El uso de los sistemas informáticos y de las redes de la Empresa se interpretará como el reconocimiento y el consentimiento afirmativos al control descrito anteriormente.

3. USO ACEPTABLE

El propósito de este apartado es garantizar el uso aceptable de los equipos informáticos que son propiedad de Phoenix Tower, están arrendados o son administrados por ella.

Su uso inapropiado expone a Phoenix Tower a unos riesgos que incluyen ataques de virus, el compromiso de los sistemas y de los servicios de red, daños en la reputación y problemas legales.

3.1 Uso general y propiedad

- Los usuarios tendrán presente que los datos que generen o las aplicaciones que utilicen los datos en los sistemas corporativos seguirán siendo propiedad de Phoenix Tower. Los empleados no deben esperar tener privacidad en sus actividades mientras utilicen los equipos informáticos de PTI, ni propiedad sobre ellas, incluso tras separarse de la Empresa.
- Por motivos de seguridad y de mantenimiento de la red, las personas autorizadas dentro de Phoenix Tower pueden controlar el equipo, los sistemas y el tráfico de la red en cualquier momento.
- Phoenix Tower se reserva el derecho de auditar redes y sistemas periódicamente para garantizar el cumplimiento de esta Política.

3.2 Seguridad e información confidencial

- La información de los sistemas de Phoenix Tower que contengan PII se identificará claramente como tal de acuerdo con el apartado "Información de Identificación Personal" de esta Política. Los usuarios se esforzarán por conservar esta información de forma segura.
- Proteja las contraseñas y no comparta las cuentas. Los usuarios autorizados son responsables de la seguridad e integridad de sus contraseñas y cuentas.
- Los empleados deben extremar las precauciones al abrir los archivos adjuntos de los correos electrónicos procedentes de remitentes desconocidos, que puedan contener virus o malware.
- Los sistemas que almacenen información confidencial de Phoenix Tower o que se utilicen para tratar la información no deben ser retirados de las centros de Phoenix Tower sin la aprobación oficial de la dirección.
- Los empleados no deben utilizar las funciones de autocompletado de los navegadores web ni otras funciones que guarden información del ID de usuario y contraseña en aplicaciones empresariales en línea.

3.3 Actividades prohibidas

- Participar en cualquier actividad que sea ilegal conforme a la ley local, estatal, federal o internacional mientras se emplean los recursos propiedad de Phoenix Tower.
- Es ilegal exportar software, información técnica, software o tecnología de encriptación en contra de las leyes de control de las exportaciones internacionales o regionales. Con carácter previo a la exportación de cualquier material del que se trate, se consultará a la dirección correspondiente.

- Utilizar un activo informático de Phoenix Tower para participar activamente en la adquisición o transmisión de material que infrinja las leyes de acoso sexual o sobre lugares de trabajo hostiles.
- Eludir la autenticación de usuario o la seguridad de cualquier host, red o cuenta. Queda terminantemente prohibido el uso no autorizado de un ID de red que no sea el suyo.
- El intento no autorizado de eludir la seguridad de la red, la protección de datos, la seguridad de contraseñas o la instalación/uso de un software para eludir cualquier seguridad o política creada e implementada por Phoenix Tower.
- Intentar alterar o manipular la comunicación o los archivos de la red de otro empleado.
- Infringir las leyes de derechos de autor y sus disposiciones de uso justo. Esto incluye copiar o "piratear" un software o vulnerar las licencias/acuerdos de software.
- La instalación de aplicaciones no oficiales en cualquier activo de Phoenix Tower sin el consentimiento previo de TI.
- Revelar información confidencial y/o secretos comerciales.
- Los usuarios no accederán intencionadamente a los sistemas de la Empresa para los que no tengan autorización o una necesidad comercial.

4. USO DE CORREO ELECTRÓNICO

Este apartado tiene como objetivo proporcionar directrices para el uso adecuado del correo electrónico y describir los procedimientos de conservación del mismo.

4.1 Uso permitido

- El correo electrónico y los sistemas de correo electrónico de la Empresa deben emplearse únicamente con fines comerciales y ser conformes con las políticas y procedimientos de PTI para la conducta ética, la seguridad y el cumplimiento de las leyes y prácticas comerciales aplicables. Debe limitarse cualquier comunicación personal en el correo electrónico de la Empresa.
- Los empleados no deben esperar privacidad en lo que almacenen, envíen o reciban en el sistema de correo electrónico de la Empresa. PTI podrá controlar los mensajes sin previo aviso.
- Los empleados deben cumplir con el sistema de Autenticación Multifactor.

4.2 Correo electrónico que contenga PII

- Si se va a transferir PII por correo electrónico, se deberán tomar las siguientes medidas para garantizar una transmisión segura y minimizar el riesgo de infracción después de que se confirme que dicha PII se guardó en el servidor local:
    1. Proteger el documento con contraseña, ya sea en pdf, word o excel. Si el documento se encuentra en un formato difícil de proteger (por ejemplo,

gif o jpeg), convierta el archivo a pdf, protéjalo con contraseña y vuelva a guardarlo. El formato "original" se puede borrar en este momento y eliminarse de la papelera.

2. Enviar el documento por correo electrónico con la mención de "**CONFIDENCIAL**" como etiqueta a continuación del nombre del asunto en el asunto.
3. Comunicarse con el destinatario por teléfono para confirmar que recibió el correo electrónico y proporcionarle la contraseña. ***NUNCA ENVÍE LA CONTRASEÑA EN EL MISMO CORREO ELECTRÓNICO QUE LA PII***
4. Eliminar el archivo adjunto del correo electrónico enviado.

- La PII confidencial, como el número de seguridad social, la información de los pasaportes y los datos bancarios u otros datos financieros, **no** se debe enviar por correo electrónico.
- Si PTI recibe PII por correo electrónico, Internet o programas de mensajería instantánea, esta información deberá transferirse inmediatamente al servidor local (primera preferencia) o a un dispositivo informático móvil y, a continuación, borrarse permanentemente del programa en el que se recibió.

4.3 Actividades de correo electrónico y comunicaciones prohibidas

- Usar el correo electrónico de PTI para usos comerciales no relacionados con PTI o para uso personal frecuente.
- Reenviar automáticamente el correo electrónico de PTI a plataformas o sistemas de correo electrónico de terceros.
- Suprimir o alterar el mensaje de aviso legal generado por el sistema que se adjunta a cada correo electrónico de PTI.
- Enviar mensajes de correo electrónico no solicitados, incluido el envío de "correo basura" u otro material publicitario o de solicitud a personas que no lo hayan solicitado específicamente (correo electrónico no deseado).
- Crear o distribuir cualquier mensaje perturbador u ofensivo. Los empleados que reciban correos electrónicos con este contenido por parte de cualquier empleado de Phoenix Tower informarán de ello a su supervisor de inmediato.
- Usar cuentas de correo electrónico que no sean de Phoenix Tower (Hotmail, Gmail, etc.) para asuntos oficiales o reenviar correos electrónicos recibidos en cuentas de correo electrónico de Phoenix Tower a otras cuentas personales o que no sean de la empresa (Hotmail, Gmail, etc.).
- La suscripción a servicios electrónicos u otros contratos utilizando direcciones de correo electrónico de PTI sin una razón comercial válida.

4.4 Dispositivos móviles

- Los empleados deben obtener la aprobación previa de su responsable o supervisor antes de acceder al correo electrónico de PTI con sus dispositivos

móviles personales.

- Phoenix Tower proporciona acceso al correo electrónico con dispositivos móviles personales de conformidad con esta Política. Phoenix Tower no se hace responsable de la pérdida de información en caso de que un dispositivo se elimine (ya sea debido a un error del usuario o por medidas de seguridad aplicadas). Esta Política se aplica a todos los dispositivos portátiles del usuario final y a cualquier otro dispositivo que pueda acceder a los servicios de correo electrónico de Phoenix Tower y/o a sus datos protegidos. El cumplimiento de esta Política es obligatorio para todos los dispositivos informáticos portátiles que almacenen datos protegidos de Phoenix Tower o accedan a ellos.
- Los usuarios que utilicen un dispositivo informático portátil para acceder al correo electrónico, a los datos, a los registros o a los documentos de Phoenix Tower deben implementar las siguientes medidas de seguridad en la medida en que estén disponibles:
    - Estar configurado para desconectarse o apagarse no más de diez (10) minutos después de la última actividad del usuario.
    - Requerir contraseña o código de acceso.
    - Requerir que la contraseña tenga una longitud mínima de cuatro (4) caracteres o teclas.
    - Activar el restablecimiento del dispositivo (borrado de datos) si se introduce una contraseña incorrecta más de ocho (8) veces consecutivas, cuando sea técnicamente factible.
    - El dispositivo debe estar encriptado.

- Los usuarios que utilicen un dispositivo informático portátil para acceder al correo electrónico, a los datos, a los registros o a los documentos de Phoenix Tower deben llevar su dispositivo a TI para asegurarse de que se apliquen estas medidas de seguridad.

4.5 Eliminación de equipos

Antes de desecharlos o transferirlos, todos los dispositivos informáticos portátiles y las tarjetas de memoria asociadas deben formatearse por completo y eliminar todos los datos de Phoenix Tower. Una vez finalizado el acceso de un empleado a los sistemas de Phoenix Tower, la persona llevará su dispositivo informático portátil a TI para que pueda eliminar de él cualquier información de Phoenix Tower.

4.6 Remisión de informes

- La pérdida, el robo o cualquier uso no autorizado de un dispositivo de usuario final portátil que haya sido utilizado para almacenar información protegida de Phoenix Tower o para acceder a ella constituye una divulgación y debe ser denunciada ante el Departamento de TI de Phoenix Tower.
- Dicho departamento se coordinará con el Departamento Jurídico y con el

supervisor del usuario para determinar hasta qué punto debe formatearse o eliminarse un dispositivo de usuario final, personal o propiedad de PTI en caso de pérdida o robo y al finalizar la relación laboral del usuario con PTI. Si se determina que es necesario y posible ejecutar un borrado remoto, el Departamento de TI intentará limitar la información borrada, únicamente, a la de Phoenix Tower, en la medida en que sea técnicamente posible en los dispositivos propiedad de PTI y/o dispositivos en los que se apliquen reembolsos.

5. USO DE INTERNET

La Empresa proporcionará acceso a Internet a los empleados y contratistas que estén conectados a la red interna y que tengan una necesidad empresarial para este acceso.

Internet es una herramienta comercial para la Empresa. Se utilizará para fines comerciales, como comunicarse por correo electrónico con proveedores y socios comerciales, obtener información comercial de utilidad e investigar temas técnicos y empresariales relevantes.

El servicio de Internet no se puede utilizar para transmitir, recuperar o almacenar comunicaciones de naturaleza discriminatoria o vejatoria, que sean denigrantes para un particular o un grupo, obscenas o pornográficas, de naturaleza difamatoria o amenazante, para "cartas en cadena" o para cualquier otro propósito ilegal o beneficio personal.

6. PERSONAL

El propósito de este apartado es reducir el riesgo de error humano, robo, fraude o uso indebido de las instalaciones. Dado que la seguridad de nuestros activos de información es un componente crítico de nuestro modelo de negocio, es vital que todos los empleados de Phoenix Tower se sometan a ciertos estándares para garantizar la credibilidad y la seguridad.

6.1 Almacenamiento de PII en los sistemas de la empresa

- A pesar del respeto de Phoenix Tower por la privacidad de los empleados en el lugar de trabajo, se reserva el derecho de acceso a toda la información creada y almacenada en los sistemas de la empresa.
- Phoenix Tower tiene el derecho de controlar toda la información recibida, almacenada, transmitida y/o creada en los sistemas de Phoenix Tower.

6.2 Intercambio de información confidencial

- La información confidencial solo se compartirá con otras personas autorizadas.
- La información de la organización tiene sus propios niveles de sensibilidad y no se debe divulgar al personal que no tiene autorización para acceder a ella.
- Todos los datos y la información que no sean de dominio público, relacionados con la actividad de Phoenix Tower y sus empleados, deben

ser confidenciales en todo momento.
- La información confidencial no se debe divulgar a miembros de la familia que no tengan autorización para recibirla.

7. SEGURIDAD FÍSICA

Este apartado prohíbe el acceso físico no autorizado a las instalaciones y a la información de Phoenix Tower y evita cualquier daño o interferencia en las operaciones comerciales ordinarias. Esta Política también abarca toda la seguridad física de las entradas, de las instalaciones de la oficina y de otras áreas fundamentales que deben ser seguras para proteger los activos.

7.1 Seguridad física

- Se utilizan puertas de seguridad, lectores de tarjetas y teclados con PIN para proteger las áreas con información crítica. Solo los empleados autorizados pueden acceder a estas áreas seguras.
- El personal será supervisado electrónicamente en función de las áreas a las que se le haya dado acceso. Esto es para mitigar el peligro de robo, el vandalismo y el uso no autorizado de los sistemas.
- Las áreas en las que se gestione información segura (incluido el tratamiento de la información y las instalaciones informáticas) estarán sometidas a estrictos controles para garantizar que no se permita el acceso a empleados no autorizados ni a personas ajenas a la organización.

7.2 Protección de puestos de trabajo e instalaciones de trabajo desatendidas

- El equipo siempre debe protegerse de forma adecuada, especialmente cuando se deja desatendido.
- Antes de abandonar su mesa, si no va a estar a la vista, debe cerrar sesión o bloquear su ordenador para evitar accesos no autorizados.
- Las impresoras y faxes se formatearán diariamente de datos sensibles. Los documentos sensibles enviados a impresoras o faxes deben protegerse tan pronto como se impriman.

7.3 Préstamo de llaves, códigos de seguridad o tarjetas de acceso de seguridad a otras personas

- El uso de llaves, ya sean físicas o electrónicas, para acceder a áreas seguras se limitará estrictamente al empleado al que se le asignaron. Está prohibido prestar llaves, códigos de seguridad o tarjetas de acceso de seguridad a empleados que no pertenezcan a PTI ni a personas ajenas.
- El incumplimiento de esta Política podría considerarse una infracción de la seguridad y será objeto de medidas disciplinarias.

7.4 Gestión de personas ajenas en las instalaciones

- Si una persona ajena no está acompañada por un empleado de Phoenix Tower, los trabajadores informarán de su presencia en las instalaciones de la organización.

8. CONTROL DE ACCESO

Un componente fundamental de nuestra Política de seguridad de la información es el control del acceso a los recursos de información cruciales que requieren protección frente a la divulgación o modificación no autorizadas. El significado principal del control de acceso es que los permisos se asignan a personas o sistemas que están autorizados para acceder a recursos específicos. Los controles de acceso existen en varias capas del sistema, incluida la red. El control de acceso se implementa mediante ID de inicio de sesión y contraseña. A nivel de aplicación y de base de datos, pueden aplicarse otros métodos de control de acceso para restringir aún más el acceso. Los sistemas de aplicaciones y bases de datos pueden limitar el número de aplicaciones y de bases de datos disponibles para los usuarios en función de los requisitos de su trabajo.

8.1 Sistema de usuario y acceso a la red: identificación ordinaria del usuario

Todos los usuarios deberán disponer de una ID de inicio de sesión y de una contraseña únicos para acceder a los sistemas. La contraseña del usuario debe mantenerse confidencial y NO DEBE compartirse con el personal de administración y de supervisión ni con cualquier otro empleado. Todos los usuarios deben cumplir con las siguientes reglas relativas a la creación y al mantenimiento de contraseñas:

- La contraseña debe ser compleja. :
  - La longitud mínima de una contraseña debe ser de 8 caracteres.
  - Debe consistir en una combinación de caracteres alfanuméricos (letras mayúsculas y minúsculas, dígitos numéricos y signos especiales).
  - Letra minúscula.
  - Letra mayúscula.
  - Símbolos: . : { } ! @ # $ % ^ & * ? _~-
  - Números del 0 al 9.
  - No debe contener caracteres consecutivos idénticos.
  - Como recomendación, la contraseña no debe ser igual a ninguna de las últimas 5 contraseñas utilizadas.
- No use ningún nombre común, sustantivo, verbo, adverbio o adjetivo. Estas sencillas contraseñas se pueden descifrar fácilmente con las "herramientas de hackers" estándar.
- Las contraseñas no deben colocarse en los terminales o cerca de ellos, ni ser

fácilmente accesibles.
- La contraseña debe cambiarse cada 60 días.
- Las cuentas de usuario se bloquean después de 5 intentos fallidos de inicio de sesión.
- Los ID de inicio de sesión y las contraseñas se suspenderán después de 20 días sin uso.

Los usuarios no pueden acceder a los archivos de contraseñas de ningún componente de la infraestructura de red. Los archivos de contraseñas de los servidores se controlarán para evitar el acceso de usuarios no autorizados. Está estrictamente prohibido copiar, leer, eliminar o modificar un archivo de contraseñas en cualquier sistema informático.

Los usuarios no podrán iniciar sesión como administradores del sistema. Los usuarios que necesiten este nivel de acceso a los sistemas de producción deben solicitar una cuenta de acceso especial, tal y como se indica en otras secciones de este documento.

Los identificadores de inicio de sesión y las contraseñas de los empleados se desactivarán lo antes posible si el empleado es separado, despedido, suspendido, puesto en excedencia o deja de trabajar para la Empresa.

Los supervisores/responsables se comunicarán de inmediato y directamente con el Departamento de TI de la Empresa para informar sobre cualquier cambio en la situación del empleado que requiera el cese o la modificación de sus privilegios de acceso al sistema.

Los empleados que olviden su contraseña deben avisar al Departamento de TI o recurrir a las herramientas provistas para que se le asigne una nueva contraseña. El empleado debe identificarse (p. ej., número de empleado) ante el Departamento de TI.

Los empleados serán responsables de todas las transacciones que se produzcan durante las sesiones de inicio de sesión iniciadas, mediante el uso de la contraseña y del identificador del empleado. Los empleados no podrán conectarse a un ordenador y luego permitir que otra persona lo utilice o compartir de otro modo el acceso a los sistemas informáticos.

8.2 Acceso del administrador del sistema

Los administradores de sistemas, de redes y de seguridad tendrán un acceso con privilegios elevados a los sistemas host, rúteres, hubs y cortafuegos, según sea necesario para desempeñar las funciones de su puesto.

Todas las contraseñas del administrador del sistema se **ELIMINARÁN** inmediatamente después de que cualquier empleado que tenga acceso a ellas sea separado, cesado, despedido o deje el empleo por cualquier otro motivo. Se suspenderán las contraseñas de los empleados que se encuentren en excedencia administrativa o disciplinaria hasta que se restablezca la situación de empleo activo.

8.3 Acceso especial

Se proporcionan cuentas de acceso especial a las personas que requieren privilegios temporales de administrador del sistema para su trabajo. Estas cuentas son controladas por la Empresa y requieren el permiso del Departamento de TI de la Empresa del usuario. El control de las cuentas de acceso especial se realiza introduciendo a los usuarios a un área específica y generando periódicamente informes para la dirección. Los informes mostrarán quién tiene actualmente una cuenta de acceso especial, por qué motivo y cuándo expirará. Las cuentas especiales expirarán en 2 días y no se renovarán automáticamente sin un permiso por escrito.

8.4 Conexión a redes de terceros

Esta política se establece para garantizar un método seguro de conectividad proporcionado entre la Empresa y todas las empresas terceras y otras entidades obligadas a intercambiar electrónicamente información con la Empresa.

"Terceros" se refiere a los proveedores, a los consultores y a los socios comerciales que hacen negocios con la Empresa, y a otros socios que intercambian información con ella. Las conexiones de red de terceros deben ser utilizadas únicamente por los empleados del tercero, y para los fines comerciales de la Empresa. La Empresa tercera se asegurará de que solo los usuarios autorizados puedan acceder a la información de la red de la Empresa. El tercero no permitirá que el tráfico de Internet o de una red privada se introduzca en la red de la Empresa. Una conexión de red de terceros se define como una de las siguientes opciones de conectividad:

- Una conexión de red terminará en un cortafuegos y el tercero estará sujeto a las normas de autenticación estándar de la empresa.

Esta política se aplica a todas las solicitudes de conexión de terceros y a cualquier conexión de terceros existente. En los casos en que las conexiones de red de terceros existentes no cumplan con los requisitos descritos en este documento, se rediseñarán cuando sea necesario.

Todas las solicitudes de conexiones de terceros deben realizarse por escrito y ser aprobadas por el Departamento de TI.

8.5 Conexión de dispositivos a la red

Solo los dispositivos autorizados pueden conectarse a la(s) red(es) de la Empresa. Los dispositivos autorizados incluyen PC y estaciones de trabajo propiedad de la Empresa que cumplan con sus directrices de configuración. Otros dispositivos autorizados son los dispositivos de infraestructura de red utilizados para la gestión y supervisión de la red.

Los usuarios no conectarán a la red ordenadores ajenos a la empresa que no estén autorizados por la Empresa, no sean de su propiedad o no estén controladas por ella. Los usuarios tienen específicamente prohibido conectar a la red cualquier dispositivo que no

sea de la Empresa, como portátiles, ordenadores, discos duros externos, teléfonos o tabletas.

NOTA: Los usuarios no están autorizados a conectar ningún dispositivo que altere las características topológicas de la red ni ningún dispositivo de almacenamiento no autorizado (p. ej., memorias USB y CD grabables).

8.6 Acceso remoto

Solo las personas autorizadas pueden acceder de forma remota a la red de la Empresa. El acceso remoto se proporciona a aquellos empleados, contratistas y socios comerciales de la Empresa que tienen una necesidad comercial legítima de intercambiar información, copiar archivos o programas, o acceder a aplicaciones informáticas. Una conexión autorizada puede ser un PC remoto a la red o de una red remota a la red de la empresa. El único método aceptable de conexión remota a la red interna es el uso de una identificación segura.

8.7 Acceso remoto no autorizado

Está prohibida la conexión de hubs al PC o estación de trabajo de un usuario que esté conectado a la red de área local (LAN) de la Empresa sin su permiso por escrito. Además, los usuarios no pueden instalar ningún software personal para controlar de manera remota el PC o la estación de trabajo. Este tipo de acceso remoto elude los métodos autorizados de acceso remoto de alta seguridad y representa una amenaza para la seguridad de toda la red.

9. RESPUESTA A INCIDENTES Y NOTIFICACIÓN DE VIOLACIONES DE DATOS

En caso de un incidente de seguridad, es importante que los empleados de Phoenix Tower puedan identificarlo y responder adecuadamente. Cada posible incidente se investigará hasta el nivel que consideren adecuado los Departamentos Jurídico y de TI. Una respuesta adecuada y oportuna a los incidentes de seguridad de la información contribuirá a proteger los activos de Phoenix Tower.

9.1 Remisión de informes

- Cada empleado es responsable de informar de todas las vulnerabilidades de seguridad de la información identificadas o sospechosas, incluidas, entre otras, las violaciones de datos de PII potenciales o reales, de inmediato a los Departamentos de TI, o Jurídico o de Cumplimiento Normativo:
    - Línea de atención al cliente: 1-844-348-5247 o https://secure.ethicspoint.com
    - Correo electrónico: privacy@phoenixintnl.com

- Una violación en la confidencialidad, o una divulgación no autorizada de la información confidencial de Phoenix Tower, también se considera un incidente de seguridad de la información y debe notificarse como se ha indicado anteriormente.
- TI registrará los incidentes de seguridad notificados para controlar tanto los tipos como el volumen de incidentes que se producen en Phoenix Tower.
- Las pruebas relativas a una violación en la seguridad de la información deben recopilarse adecuadamente según las indicaciones del responsable del departamento de TI y enviarse a su departamento. Deben recopilarse para cumplir las obligaciones legales, reglamentarias o contractuales y evitar infracciones penales o civiles.
- Tras realizar una investigación inicial, el responsable del Departamento de TI determinará si el evento es o no un incidente de seguridad de la información. Si se ha producido un incidente de seguridad, el Departamento Jurídico determinará si el incidente constituye una violación en los datos sobre la que le sea obligatorio informar, y de las violaciones de datos que incluyan PII.
- El Departamento Jurídico mantendrá un registro de los incidentes de seguridad informados que constituyan una violación de datos.
- La información relacionada con los incidentes de seguridad de la información solo puede ser divulgada por las personas autorizadas. Los empleados no pueden divulgar ninguna información sobre un incidente de seguridad fuera de PTI sin el permiso expreso del equipo del Departamento Jurídico.
- Tras el incidente o la violación de datos, el Departamento de TI será responsable de realizar una reunión con todos los empleados y partes afectadas/correspondientes para revisar los resultados de la investigación y analizar la causa principal del incidente. Todos los empleados que participen en el descubrimiento o la investigación de un
- incidente de seguridad están obligados a asistir a esta reunión.
- Los empleados de Phoenix Tower o los contratistas externos involucrados en un incidente de seguridad o que hayan violado la política de seguridad de la información de Phoenix Tower, independientemente de la intencionalidad, se someterán a un tribunal disciplinario, que determinará la falta, las medidas correctivas y otras medidas oportunas.

9.2 Notificación de la violación de datos

- **Notificación a la autoridad de control:** PTI, como responsable del tratamiento, notificará a la Autoridad Nacional de Control inmediatamente (en cuanto tenga conocimiento del incidente) y, como máximo, en un plazo de 72 horas desde que se le informó del incidente, incluidas las horas transcurridas en fines de semana y días festivos. Para la comunicación, PTI deberá utilizar el formulario de notificación, por país, previsto en el **Procedimiento de gestión de incidencias.**

- **Notificación a los interesados:** PTI, como responsable del tratamiento, debe notificar a los afectados las violaciones de seguridad cuando esta pueda afectar negativamente a sus datos personales o privacidad.

10. PRIVACIDAD POR DISEÑO

PTI se compromete a adoptar las medidas técnicas y organizativas necesarias para dar cumplimiento concreto a las disposiciones y principios de protección de datos y garantizar así los derechos de los interesados. Para ello, PTI deberá considerar la adopción de las medidas legales, técnicas y organizativas necesarias desde la fase de desarrollo y diseño de los productos y servicios, o desde el momento inicial en que se presente cualquier proyecto, iniciativa o idea que implique el tratamiento de datos personales propuesto por PTI.

Para la aplicación de medidas legales se deberá consultar al responsable en materia de protección de datos, y para las medidas técnicas y organizativas al responsable del Departamento de TI.

Para ello, cada responsable de área, proyecto o nuevo proceso debe asegurarse de que la privacidad se aplique desde el diseño y por defecto, además de cumplir con los principios básicos de la normativa.

11. MEDIDAS DE SEGURIDAD ADICIONALES

Para proteger la integridad, confidencialidad y disponibilidad de la información, PTI ha aplicado las siguientes medidas de seguridad:

11.1 Detección y gestión de vulnerabilidades y software malicioso.

En relación con el proceso continuo de detección y gestión de vulnerabilidades, esta medida de seguridad se implementa para identificar, evaluar, abordar y reportar vulnerabilidades de seguridad en los sistemas. Para ello, PTI ha instalado las herramientas Microsoft Defender y Zscaler para la detección y gestión de vulnerabilidades y malware.

11.2 Política de gestión de parches

En relación con la gestión de parches, PTI ha desarrollado una política que establece que los parches publicados por Microsoft se instalarán como Intune, Zero day. Control de acceso a la red.

11.3 Mecanismos de encriptación

En relación a los mecanismos de encriptación, PTI los ha implementado tanto en la base de datos como en el disco duro de los ordenadores portátiles. De esta forma, la información almacenada en los dispositivos no es accesible en el caso de un acceso no autorizado. Se utilizan mecanismos de encriptación, tanto en las bases de datos como en el disco duro de los portátiles. En este caso, se ha implementado un mecanismo de borrado en caso de

pérdida o robo del equipo que, además de las medidas de seguridad de cifrado de datos, permite borrar información de forma remoto.

11.4 Administración de cuentas.

En relación con la gestión de cuentas. PTI ha implementado mecanismos denominados Gestión de Identidad Privilegiada (PIM) y Gestión de Acceso Privilegiado (PAM).