POLÍTICA DE SEGURIDAD DE

LA INFORMACIÓN DE

PHOENIX TOWER INTERNATIONAL

Revisado el 10 de mayo de 2021

PHOENIX TOWER INTERNATIONAL

Política de seguridad de la información

Contenido

Política de seguridad de la información

Propósito

Phoenix Tower US Holdings, L.P. y sus subsidiarias y afiliadas en todo el mundo (colectivamente, "PTI", "Phoenix Tower" o "Compañía"), se comprometen a proteger la seguridad de la información y el aprendizaje y la mejora continuos, como se establece en esta Política de seguridad de la información (la "Política"). El alcance de esta Política está destinado a ser integral e incluirá los requisitos de la Compañía para la seguridad y protección de los activos de PTI, incluida la Información de identificación personal ("PII"), en toda la Compañía y sus proveedores aprobados tanto dentro como fuera de las instalaciones de trabajo. Todos los Empleados deben revisar y seguir la información incluida en esta Política.

Alcance

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

Definiciones

- **Información confidencial:** Toda la información significativa, no pública, relacionada con el negocio, escrita u oral, esté o no marcada como tal, relacionada con asuntos tales como estrategia comercial, procesos, finanzas, planes de marketing, contratos o tecnología. Por ejemplo, lo siguiente:
  - contratos, tanto firmados como en borrador;
  - materiales de marketing en desarrollo; o
  - proyecciones de ventas o ingresos.
- **Seguridad de la información:** Procesos y metodologías que están diseñados e implementados para proteger información o datos confidenciales, privados o sensibles impresos, electrónicos o en cualquier otro formato contra el acceso, uso, abuso, divulgación, destrucción, modificación o interrupción no autorizados.
- **Empleado:** Persona física identificada o identificable que actúa como director, funcionario, miembro del equipo, Empleado, contratista o consultor de PTI, ya sea a tiempo completo o parcial, de forma temporal o permanente.
- **Dispositivos orientados al usuario final:** Cualquier herramienta tecnológica o dispositivo utilizado por un Empleado de PTI para almacenar información o acceder a los sistemas de PTI, incluido el correo electrónico. Algunos ejemplos de dispositivos orientados al usuario final incluyen computadoras, computadoras portátiles, teléfonos inteligentes, discos duros externos y almacenamiento USB.
- **Información de identificación personal ("PII"):** Cualquier dato que pueda identificar potencialmente a un individuo específico, como nombre, correo electrónico, información financiera, número de seguro social, número de pasaporte, etc.

Supervisión de políticas

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

Política de seguridad de la información

- La alta dirección de Phoenix Tower predicará con el ejemplo al garantizar que la seguridad de la información tenga una alta prioridad en todas las actividades e iniciativas comerciales actuales y futuras.
- El asesor general global revisará anualmente esta Política y cada uno de sus apéndices para asegurar que sean relevantes y estén actualizados y revisados, según sea necesario, con el fin de garantizar que sean adecuados a la luz de la evolución de las obligaciones legales, la tecnología y las necesidades comerciales.
- La gerencia comunicará las revisiones de las políticas a todo el personal por diversos medios, como actualizaciones electrónicas, sesiones informativas, capacitación, boletines informativos, etc.

Para cumplir o superar estos objetivos, se han implementado las siguientes prácticas:

- Los Empleados firman un aviso de recepción, revisión y reconocimiento de la Política de seguridad de la información cuando se los contrata.
- La conciencia del personal se reforzará periódicamente para que los asuntos de seguridad de la información sean lo más importante.
- La capacitación individual en seguridad de la información es obligatoria a partir de la incorporación del Empleado, junto con toda capacitación técnica que sea adecuada para las responsabilidades de la función laboral. Cuando el personal cambia de trabajo o de funciones, sus necesidades de seguridad de la información deben reevaluarse y debe brindarse la nueva capacitación como prioridad.

1. Información de identificación personal

El objetivo de esta sección es orientar la protección de la PII recopilada de Propietarios, Inquilinos, clientes potenciales de ventas y Empleados, y ayudará a los Empleados a determinar qué información se puede divulgar a quienes no son Empleados, así como la sensibilidad relativa de la información que no se divulgará fuera de Phoenix Tower sin la debida autorización.

Definiciones

Phoenix Tower reconoce su necesidad de mantener la confidencialidad de la PII y entiende que dicha información es única para cada persona y generalmente se limita a los datos que son relevantes y necesarios para sus propósitos. La PII cubierta por esta Política puede provenir de diversos tipos de personas que realizan tareas en nombre de la Compañía e incluye a Empleados, candidatos, contratistas independientes y cualquier PII que se mantenga en su base de clientes. La PII incluye toda la siguiente información de identificación sobre Propietarios, Inquilinos, clientes potenciales de ventas y Empleados:

- información de contacto personal (números de teléfono, direcciones, etc.);
- números de seguro social (o su equivalente emitido por entidades gubernamentales fuera de los Estados Unidos);
- números de identificación del contribuyente (o su equivalente emitido por entidades de ingresos gubernamentales fuera de los Estados Unidos);
- números de identificación del empleador (o su equivalente emitido por entidades gubernamentales fuera de los Estados Unidos);
- números de licencia de conducir estatales o extranjeros o copias de tarjetas de identificación;
- números de pasaporte o copias de pasaportes;
- fechas de nacimiento;
- números de tarjetas de transacciones de crédito o débito corporativas o individuales (incluidos PIN o números de acceso) mantenidos en registros de proveedores aprobados o de la organización; o
- información de la cuenta bancaria de PTI o socios comerciales.

La PII puede encontrarse en copias impresas o en registros electrónicos. Ambas formas de PII están dentro del alcance de esta Política.

Almacenamiento y manejo de información que contiene PII

PII electrónica

La PII se puede guardar electrónicamente mediante una diversidad de métodos y en una diversidad de dispositivos orientados al usuario final, incluidos, entre otros, los siguientes:

- Dispositivos informáticos móviles (es decir, computadoras portátiles, teléfonos inteligentes, tabletas, computadoras, PDA, etc.).
- Programas de correo electrónico, Internet y mensajería instantánea que almacenan, procesan o transmiten datos.
- Los medios electrónicos extraíbles, como unidades USB, unidades de CD, discos duros externos, etc., solo deben usarse para la PII no confidencial. La PII confidencial, como los números de seguro social, la

información del pasaporte y los datos bancarios u otros datos financieros no se deben guardar en medios electrónicos extraíbles.
- Servidores locales y en la nube de propiedad de PTI.
- Servidores basados en la nube de terceros.

En esta sección de la Política, se establecen los requisitos y el proceso de aprobación para los Dispositivos orientados al usuario final que son de propiedad de PTI, o que PTI administra o alquila. No se permitirá que los dispositivos orientados al usuario final que no sean de propiedad de PTI, o que PTI alquile o administre, accedan a servidores locales que contengan PII, ni eliminen tales servidores, a menos que lo autorice, por escrito, el asesor general global.

- **Dispositivos informáticos móviles (es decir, computadoras portátiles, teléfonos inteligentes, tabletas, PDA, etc.)**: La PII se puede guardar en dispositivos informáticos móviles, pero dichos dispositivos deben estar protegidos con contraseña, encriptados y tener capacidad de borrado remoto. Este no es un método preferido para almacenar la PII, y los dispositivos informáticos móviles donde se almacena la información deben verse como una ubicación de almacenamiento temporal y la PII debe moverse a un servidor de PTI lo antes posible.
- **Programas de correo electrónico, Internet y mensajería instantánea:** La Compañía no recomienda transmitir PII a través de Internet o de programas de mensajería instantánea. Cuando la PII se va a transferir por correo electrónico, se deben seguir los siguientes pasos para 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. Proteja el documento con contraseña, ya sea pdf, Word o Excel. Si el documento está en un formato que no se puede proteger fácilmente (es decir, gif o jpeg), convierta el documento en un archivo pdf, protéjalo con contraseña en este formato y vuelva a guardarlo. El formato "original" puede eliminarse en este momento y borrarse de la papelera.
    2. Envíe por correo electrónico el documento con la leyenda "**CONFIDENCIAL**" como etiqueta después del nombre del asunto en la línea del asunto.
    3. Comuníquese con el destinatario por teléfono para confirmar que haya recibido el correo electrónico y proporciónele la contraseña. ***NUNCA ENVÍE LA CONTRASEÑA POR CORREO ELECTRÓNICO***
    4. Elimine el archivo adjunto del correo electrónico enviado.

    La PII confidencial, como los números de seguro social, la información del pasaporte y los datos bancarios u otros datos financieros, **no** debe transmitirse por correo electrónico.

    Si PTI recibe cualquier PII a través de Internet o de programas de mensajería instantánea, o por cualquier otro medio inseguro, la información debe transferirse inmediatamente al servidor de PTI (procedimiento preferido) o moverse al almacenamiento de un dispositivo informático móvil y luego borrarse permanentemente del programa en el que se recibió.
- **Medios electrónicos extraíbles:** La PII se puede guardar en medios electrónicos extraíbles, como unidades USB, con el fin de transportar información entre medios. Los dispositivos de medios extraíbles deben protegerse con contraseña y encriptarse. Este no es un método preferido para almacenar PII. Los medios electrónicos extraíbles donde se almacena la información deben verse como una ubicación de almacenamiento temporal y la PII debe moverse a un servidor de PTI lo antes posible y eliminarse de los medios extraíbles. La PII confidencial, como los números de seguro social, la información del pasaporte y

los datos bancarios u otros datos financieros, **no** se debe guardar en medios electrónicos extraíbles.

- **Servidor local o en la nube de propiedad de PTI**: El lugar preferido para el almacenamiento de toda la PII es en servidores locales o basados en la nube de propiedad de PTI, y este método de almacenamiento siempre debe usarse primero cuando esté disponible. Todas las carpetas y los datos que contienen PII deben estar claramente etiquetados como tales, y el acceso a estas carpetas estará restringido solo a aquellos Empleados que deban tener acceso en la función diaria de sus trabajos.
- **Almacenamiento de copias impresas (en el lugar)**: La PII almacenada en las ubicaciones de las oficinas debe guardarse en cajones con llave y preferiblemente detrás de puertas cerradas si es posible. El acceso a estas ubicaciones debe estar restringido a aquellos Empleados que requieran la información para el desempeño de sus funciones laborales diarias. Solo el jefe del departamento debe conservar las llaves de dichos lugares seguros, y todo acceso proporcionado a los Empleados debe documentarse en un formato de registro. En ningún caso ordinario se retirarán de la oficina los documentos que contengan PII y cualquier caso de este tipo que requiera el retiro de PII de la oficina requerirá la aprobación del CEO. Toda la información, los datos y los documentos que contienen PII deben estar claramente etiquetados para que todos los usuarios conozcan la propiedad, la clasificación y el valor de la información. La información, los datos y los documentos que contienen PII se transportarán de forma segura y se destruirán de forma segura para protegerlos de la divulgación involuntaria. La información, los datos y los documentos que contienen PII se almacenarán de forma segura cuando no estén en uso.
- **Almacenamiento de copias impresas (fuera del sitio):** Por lo general, el almacenamiento de PII en formato impreso fuera del sitio no está permitido sin la aprobación por escrito del CEO. Los datos que contienen PII en formato impreso no deben enviarse a instalaciones de almacenamiento fuera del sitio como parte de los archivos del sitio, y bajo ninguna circunstancia dichos datos deben almacenarse en los hogares de los Empleados. Toda la información, los datos y los documentos que contienen PII deben estar claramente etiquetados para que todos los usuarios conozcan la propiedad, la clasificación y el valor de la información. La información, los datos y los documentos que contienen PII se transportarán de forma segura y se destruirán de forma segura para protegerlos de la divulgación involuntaria. La información, los datos y los documentos que contienen PII se almacenarán de forma segura cuando no estén en uso.
- **Transporte de copias impresas:** Cuando la PII deba transportarse fuera de las instalaciones de la oficina en situaciones aprobadas, solo deben hacerlo los Empleados directos de PTI. Se debe tener suficiente cuidado para garantizar que los datos que contienen PII estén protegidos (maletín cerrado con llave, etc.) y que dichos datos estén siempre en poder del Empleado durante el transporte.
- **Impresiones en papel**: En la medida de lo posible, se debe evitar la impresión de datos que contengan PII y el almacenamiento electrónico. En situaciones en las que esto no sea posible, el Empleado que imprima los datos deberá recibir la aprobación previa del jefe de departamento, con indicación de qué materiales se están imprimiendo y por qué motivo. El Empleado también será responsable de la destrucción de las copias impresas y proporcionará al jefe del departamento una declaración que contenga la fecha de destrucción, la descripción del material destruido y el método utilizado.

Acceso a la PII por parte de los Empleados

Cada jefe de departamento es responsable de identificar y mantener una lista de los usuarios en su departamento que deben tener acceso a los archivos (electrónicos o impresos). La lista debe actualizarse según sea necesario y, como mínimo, debe revisarse una vez al año y tras un evento relacionado con el personal (por ejemplo, contratación, separación, despido y ascenso). La lista se proporcionará al departamento de TI que, a su vez, será responsable de garantizar que el acceso a los archivos de copia electrónica que contienen PII esté restringido de acuerdo con la lista. Cada jefe de departamento será responsable de garantizar que el acceso a los archivos

impresos que contienen PII esté restringido de acuerdo con la lista. Los jefes de departamento o los gerentes que estos designen deben revisar el acceso de los usuarios ante cualquier cambio en las funciones y responsabilidades laborales de las personas afectadas, o en el estado del Empleado/contratista independiente (incluido, entre otros, el despido) y comunicar cualquier cambio oportunamente a TI.

Requisitos reglamentarios

Es política de la Compañía cumplir con los estatutos y regulaciones internacionales, federales o estatales con respecto al acceso a la PII y a su uso, almacenamiento y retención. Los Departamentos Legal o de Cumplimiento de Phoenix Tower supervisarán todas las cuestiones de cumplimiento normativo. Si alguna disposición de esta Política entra en conflicto con un requisito legal de las leyes internacionales, federales o estatales que rigen la PII, se reemplazarán las disposiciones de la Política que entren en conflicto.

Capacitación

Todos los nuevos Empleados que ingresan a la Compañía reciben capacitación introductoria sobre el manejo adecuado y la protección de la PII, y se les proporciona una copia de esta Política y los procedimientos de implementación para el departamento al que están asignados (si corresponde). Los Empleados en puestos con acceso regular continuo a la PII o aquellos transferidos a dichos puestos reciben capacitación que refuerza esta Política y los procedimientos para el mantenimiento de datos de la PII y recibirán capacitación sobre la seguridad y protección de los datos de la PII y los datos de propiedad de la Compañía al menos una vez al año. La capacitación estará a cargo del departamento de TI y formará parte de la orientación a nuevos Empleados en el caso de Empleados nuevos. Si se agrega un Empleado existente a la lista de acceso a la PII, el Empleado recibirá una capacitación separada sobre las disposiciones de esta Política.

Confirmación de confidencialidad

Todos los Empleados de la Compañía deben mantener la confidencialidad de la PII, así como la información Confidencial de la Compañía a la que puedan tener acceso, y comprender que dicha PII debe restringirse solo a aquellos con una necesidad comercial de conocerla.

Violaciones de datos de PII/incidentes de seguridad

Si un Empleado toma conocimiento sobre cualquier acceso a la PII, o su uso o transferencia, que estén en conflicto con esta Política o sobre cualquier incidente de seguridad, deberá informarlo de inmediato al Departamento Legal de Phoenix Tower. Las bases de datos o los conjuntos de datos que incluyen PII pueden violarse inadvertidamente o mediante una intrusión indebida. Consulte la sección 6 de esta Política para obtener más información.

Violaciones de las políticas y procedimientos de PII

Phoenix Tower considera que la protección de los datos de PII es de suma importancia. Las infracciones de esta Política o sus procedimientos darán lugar a acciones disciplinarias, que podrán incluir la suspensión o el despido en el caso de infracciones graves o reiteradas.

Supervisión del uso de sistemas informáticos

La Compañía tiene el derecho y la capacidad de supervisar la información electrónica creada o comunicada por personas que utilizan las redes y sistemas informáticos de la Compañía, incluidos los mensajes de correo

electrónico y el uso de Internet. No es la política ni la intención de la Compañía supervisar continuamente todo el uso de las computadoras por parte de los Empleados u otros usuarios de los sistemas informáticos y la red de la Compañía. Sin embargo, los usuarios de los sistemas deben ser conscientes de que la Compañía puede supervisar el uso, incluidos, entre otros, los patrones de uso de Internet (por ejemplo, sitios accedidos, duración de la conexión, hora del acceso) y los archivos electrónicos y mensajes de los Empleados en la medida necesaria para garantizar que Internet y otras comunicaciones electrónicas se utilicen de conformidad con la ley y la política de la Compañía. El uso de las redes y los sistemas informáticos de la Compañía se considerará un consentimiento y reconocimiento afirmativo de la supervisión descrita anteriormente.

2. Uso aceptable

El propósito de esta sección es garantizar el uso aceptable de los equipos informáticos que son propiedad de Phoenix Tower, o que Phoenix Tower alquila o administra. El uso inadecuado expone a Phoenix Tower a riesgos que incluyen ataques de virus, riesgo de los sistemas y servicios de red, daños a la reputación y problemas legales.

Uso general y propiedad

- Los usuarios sabrán que los datos que crean o las aplicaciones que utilizan los datos en los sistemas corporativos siguen siendo propiedad de Phoenix Tower. Los Empleados no deben tener ninguna expectativa de privacidad para sus actividades mientras usan equipos informáticos de PTI y no deben tener expectativas de propiedad, incluso después de la separación de la Compañía.
- Por motivos de seguridad y mantenimiento de la red, las personas autorizadas dentro de Phoenix Tower podrán supervisar los equipos, los sistemas y el tráfico de la red en cualquier momento.
- Phoenix Tower se reserva el derecho de auditar las redes y los sistemas en forma periódica para garantizar el cumplimiento de esta Política.

Seguridad e información privada

- La información guardada en los sistemas de Phoenix Tower que contienen PII estará claramente etiquetada como tal de acuerdo con la sección Información de identificación personal de esta Política. Los usuarios se esforzarán por mantener segura esta información.
- Mantenga las contraseñas seguras y no comparta las cuentas. Los usuarios autorizados son responsables de la seguridad e integridad de sus contraseñas y cuentas.
- Los Empleados deben tener extrema precaución al abrir archivos adjuntos de correos electrónicos recibidos de remitentes desconocidos, ya que pueden contener virus o malware.
- Los sistemas que almacenan información confidencial de Phoenix Tower, o que se utilizan para el procesamiento de información, no deben retirarse de las instalaciones de Phoenix Tower sin la aprobación oficial de la gerencia.
- Los Empleados no deben utilizar las funciones de autocompletar del explorador web u otras funciones que guarden la información de identificación de usuario y contraseña en aplicaciones comerciales en línea.

Actividades prohibidas

- Participar en cualquier actividad que sea ilegal según las leyes locales, estatales, federales o internacionales mientras se utilizan los recursos de propiedad de Phoenix Tower.
- La exportación de software, información técnica, software o tecnología de cifrado, en infracción de las leyes de control de exportaciones internacionales o regionales, es ilegal. Se consultará a la dirección correspondiente antes de exportar cualquier material que se cuestione.
- Utilizar un activo informático de Phoenix Tower para participar activamente en la obtención o transmisión de material que infrinja las leyes de acoso sexual o de lugar de trabajo hostil.
- Eludir la autenticación de usuario o la seguridad de cualquier host, red o cuenta. El uso no autorizado de una identificación de red que no sea la suya está estrictamente prohibido.
- Los intentos no autorizados de eludir la seguridad de la red, la protección de datos, la seguridad por contraseña o la instalación/uso de software diseñado 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.
- Violar las leyes de derechos de autor y sus disposiciones de uso justo. Esto incluye copiar o "piratear" software o violar licencias/acuerdos de software.
- Instalar aplicaciones no oficiales en cualquier activo de Phoenix Tower sin el consentimiento previo de TI.
- Revelar información confidencial o secretos comerciales.
- Los usuarios no deben participar intencionalmente en la obtención de acceso a los sistemas de la Compañía para los cuales no tienen autorización o una necesidad comercial de conocerlos.

3. **Uso del correo electrónico**

El propósito de esta sección es proporcionar pautas para el uso aceptable del correo electrónico y describir los procedimientos de retención de correos electrónicos.

Uso permitido

- El correo electrónico y los sistemas de correo electrónico de la Compañía deben usarse solo con fines comerciales y deben ser coherentes con las políticas y procedimientos de PTI para el comportamiento ético, la seguridad y el cumplimiento de las leyes y prácticas comerciales aplicables. Toda comunicación personal a través del correo electrónico de la Compañía debe ser limitada.
- Los Empleados no deben tener ninguna expectativa de privacidad en todo lo que almacenan, envían o reciben a través del sistema de correo electrónico de la Compañía. PTI puede supervisar los mensajes sin previo aviso.
- Los Empleados deben cumplir con la autenticación multifactor.

Correos electrónicos que contienen PII

- Si la PII se transferirá por correo electrónico, se deben seguir los siguientes pasos para garantizar una transmisión segura y minimizar el riesgo de una infracción <u>después</u> de que se confirme que dicha PII se ha guardado en el servidor local:
    1. Proteja el documento con contraseña, ya sea pdf, Word o Excel. Si el documento está en un formato que no se puede proteger fácilmente (es decir, gif o jpeg), convierta el documento en un archivo pdf, protéjalo con contraseña en este formato y vuelva a guardarlo. El formato "original" puede eliminarse en este momento y borrarse de la papelera.
    2. Envíe por correo electrónico el documento con la leyenda "**CONFIDENCIAL**" como etiqueta después del nombre del asunto en la línea del asunto.
    3. Comuníquese con el destinatario por teléfono para confirmar que haya recibido el correo electrónico y proporciónele la contraseña. ***NUNCA ENVÍE LA CONTRASEÑA EN EL MISMO CORREO ELECTRÓNICO QUE LA PII***
    4. Elimine el archivo adjunto del correo electrónico enviado.

  La PII confidencial, como los números de seguro social, la información del pasaporte y los datos bancarios u otros datos financieros, **no** debe enviarse por correo electrónico.

- Si PTI recibe cualquier PII a través de correo electrónico, Internet o programas de mensajería instantánea, la información deberá transferirse inmediatamente al servidor local (procedimiento preferido) o moverse al almacenamiento de un dispositivo informático móvil y luego borrarse permanentemente del programa

en el que se recibió.

Actividades prohibidas de correo electrónico y comunicaciones

- La utilización del correo electrónico de PTI para usos comerciales no relacionados con PTI o el uso personal frecuente.
- El reenvío automático del correo electrónico de PTI a sistemas o plataformas de correo electrónico de terceros.
- La eliminación o alteración del mensaje de descargo de responsabilidad legal generado por el sistema que se adjunta a cada correo electrónico de PTI.
- El envío de mensajes de correo electrónico no solicitados, incluido el envío de "correo basura" u otro material publicitario o de solicitud a personas que no pidieron específicamente dicho material (correo electrónico no deseado).
- La creación o distribución de cualquier mensaje perturbador u ofensivo. Los Empleados que reciban correos electrónicos con este contenido de cualquier Empleado de Phoenix Tower informarán el asunto a su supervisor de inmediato.
- La utilización de cuentas de correo electrónico que no sean de Phoenix Tower (Hotmail, Gmail y otros) para negocios oficiales de Phoenix Tower, o el reenvío de correos electrónicos recibidos en cuentas de correo de Phoenix Tower a cuentas de correo electrónico personales o que no sean de Phoenix Tower (Hotmail, Gmail y otros).
- La suscripción a servicios electrónicos u otros contratos mediante direcciones de correo electrónico de PTI sin un motivo comercial válido.

Dispositivos móviles

- Los Empleados deben obtener la aprobación previa de su gerente o supervisor antes de intentar acceder al correo electrónico de PTI a través de dispositivos móviles personales.
- Phoenix Tower proporciona acceso al correo electrónico a través de dispositivos personales móviles de conformidad con esta Política. Phoenix Tower no se hace responsable de la pérdida de datos en caso de que se borre un dispositivo (ya sea debido a un error del usuario o por las características de seguridad implementadas). Esta política se aplica a todos los dispositivos portátiles de usuario final y a cualquier otro dispositivo que pueda acceder a los servicios de correo electrónico de Phoenix Tower o a datos protegidos de Phoenix Tower. El cumplimiento de esta Política es un requisito para todos los dispositivos informáticos portátiles que almacenan datos protegidos de Phoenix Tower, o que acceden a estos.
- Los usuarios que utilizan un dispositivo informático portátil para acceder al correo electrónico, los datos, los registros o los documentos de Phoenix Tower deben implementar las siguientes funciones de seguridad en la medida en que estén disponibles en el dispositivo:

    - Estar configurado para cerrar sesión o apagarse no más de diez (10) minutos después de la última actividad del usuario.
    - Requerir una contraseña de encendido o un código de acceso.
    - Requerir una longitud mínima de contraseña de cuatro (4) caracteres o claves.
    - Proporcionar un restablecimiento del dispositivo (borrado de datos) si se ingresa una contraseña incorrecta más de ocho (8) veces consecutivas, cuando sea técnicamente posible.

- El dispositivo debe estar encriptado.

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

Desecho de equipos

Antes de su desecho o transferencia, se deben eliminar por completo todos los datos de Phoenix Tower almacenados en los dispositivos informáticos portátiles y las tarjetas de memoria asociadas. Una vez finalizado el acceso de un Empleado a los sistemas de Phoenix Tower, este llevará su dispositivo informático portátil a TI para que pueda eliminar del dispositivo todos los datos de Phoenix Tower.

Denuncia

- La pérdida, el robo o cualquier uso no autorizado de un Dispositivo portátil de usuario final que se haya utilizado para almacenar información protegida de Phoenix Tower, o para acceder a esta, constituye una divulgación y debe informarse a TI de Phoenix Tower.

- TI coordinará con el Departamento Legal y el supervisor del usuario para determinar hasta qué punto un Dispositivo de usuario final personal o de propiedad de PTI debe borrarse o limpiarse en caso de pérdida o robo y al final del empleo del usuario en PTI. Si se determina que es necesaria y posible la realización de un borrado remoto, TI intentará limitar los datos borrados solo a la información de Phoenix Tower, en la medida en que sea técnicamente posible, en los dispositivos de propiedad de PTI o en los dispositivos en los que se aplican reembolsos.

4. Uso de Internet

La Compañía proporcionará acceso a Internet a los Empleados y contratistas que estén conectados a la red interna y que tengan una necesidad comercial de este acceso.

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

El servicio de Internet no se podrá utilizar para transmitir, recuperar o almacenar comunicaciones de naturaleza discriminatoria o acosadora, o que sean despectivas para cualquier persona o grupo, obscenas o pornográficas, o de naturaleza difamatoria o amenazante, para "cartas en cadena" o con cualquier otro propósito que sea ilegal o para beneficio personal.

5. **Personal**

El propósito de esta sección es reducir el riesgo de error humano, robo, fraude o mal uso de las instalaciones. Debido a que la seguridad de nuestros activos de información es un componente crítico de nuestro modelo comercial, es vital que todos los Empleados de Phoenix Tower estén sujetos a determinadas normas para garantizar la credibilidad y la seguridad.

Almacenamiento de la PII en los sistemas de la Compañía

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

Uso compartido de la información confidencial

- La información confidencial solo se compartirá con otras personas autorizadas.
- La información de la organización tiene sus propios niveles individuales de confidencialidad y no debe divulgarse al personal que no tiene autorización para acceder a esa información.
- Todos los datos e información que no sean de dominio público, relacionados con el negocio de Phoenix Tower y sus Empleados, deben permanecer confidenciales en todo momento.
- No se debe divulgar la información confidencial a familiares que no tengan autorización para recibir dicha información.

6. Seguridad física

En esta sección, se prohíbe el acceso físico no autorizado a las instalaciones y a la información de Phoenix Tower y se busca evitar daños a las operaciones comerciales habituales, o interferencias con estas. Esta Política también cubre toda la seguridad física de las entradas, las instalaciones de trabajo de la oficina y otras áreas críticas que deben ser seguras para proteger los activos.

Seguridad física

- Se utilizan puertas de seguridad, lectores de credenciales y teclados con PIN para proteger las áreas con información crítica. Solo los Empleados autorizados podrán ingresar a estas áreas seguras.
- Se supervisará electrónicamente al personal de acuerdo con las áreas a las que se le ha otorgado acceso. Esto es para mitigar los peligros de robo, vandalismo y uso no autorizado de los sistemas.
- Las áreas donde se maneja información segura (incluido el procesamiento de información y las instalaciones de computación) estarán sujetas a estrictos controles para garantizar que no se otorgue acceso a Empleados no autorizados o a personas fuera de la organización.

Protección de instalaciones y estaciones de trabajo desatendidas

- El equipo siempre debe protegerse adecuadamente, en especial cuando se deja desatendido.
- Antes de abandonar su escritorio, si este no estará a la vista, debe cerrar sesión en su computadora, o dejarla bloqueada, para evitar el acceso no autorizado.
- Diariamente, se eliminarán los datos confidenciales de las impresoras y las máquinas de fax. Los documentos confidenciales que se envíen a impresoras o máquinas de fax deben protegerse tan pronto como se impriman.

Préstamo de llaves, códigos de seguridad o credenciales de acceso de seguridad a terceros

- El uso de llaves, ya sean estas físicas o electrónicas, para acceder a áreas seguras se limitará estrictamente al Empleado al que se asignaron las llaves. Se prohíbe el préstamo de llaves, códigos de seguridad o credenciales de acceso de seguridad a Empleados que no pertenecen a PTI o a personas externas.
- El incumplimiento de esta Política podría considerarse una violación de la seguridad y está sujeto a medidas disciplinarias.

Manejo de extraños en las instalaciones

- Si un extraño no está acompañado por un Empleado de Phoenix Tower, los Empleados cuestionarán la presencia del extraño en las instalaciones de la organización.

7. Control de acceso

Un componente fundamental de nuestra Política de seguridad de la información es controlar el acceso a los recursos de información críticos que requieren protección contra divulgaciones o modificaciones no autorizadas. El significado fundamental del control de acceso es que los permisos se asignen a personas o sistemas que estén autorizados a acceder a recursos específicos. Los controles de acceso existen en varias capas del sistema, incluida la red. El control de acceso se implementa mediante la identificación de inicio de sesión y contraseña. A nivel de aplicación y base de datos, se pueden implementar otros métodos de control de acceso para restringir aún más el acceso. Los sistemas

de aplicaciones y bases de datos pueden limitar la cantidad de aplicaciones y bases de datos disponibles para los usuarios en función de los requisitos de su trabajo.

Sistema de usuario y acceso a la red: identificación de usuario normal

Todos los usuarios deberán tener una identificación de inicio de sesión y una contraseña únicas para acceder a los sistemas. La contraseña del usuario debe mantenerse confidencial y NO DEBE compartirse con el personal de administración y supervisión ni con ningún otro Empleado. Todos los usuarios deben cumplir con las siguientes reglas con respecto a la creación y mantenimiento de contraseñas:

- La contraseña debe ser compleja. Es decir, no use ningún nombre, sustantivo, verbo, adverbio o adjetivo común. Estas contraseñas sencillas se pueden descifrar fácilmente con "herramientas de piratas informáticos" estándar.
- Las contraseñas no deben estar escritas en terminales de computadora, o cerca de estos, ni deben ser fácilmente accesibles en el terminal.
- La contraseña debe cambiarse cada 60 días.
- Las cuentas de usuario se bloquearán después de 5 intentos fallidos de inicio de sesión.
- Las identificaciones de inicio de sesión y las contraseñas se suspenderán después de transcurridos 20 días sin uso.

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

Los usuarios no podrán iniciar sesión como administrador del sistema. Los usuarios que necesitan este nivel de acceso a los sistemas de producción deben solicitar una cuenta de acceso especial como se describe en otra parte de este documento.

Las identificaciones de inicio de sesión y las contraseñas de los Empleados se desactivarán lo antes posible si al Empleado se lo separa del cargo, despide, desvincula, suspende, se le concede una licencia o si este deja de trabajar en la oficina de la Compañía.

Los supervisores/gerentes se comunicarán de inmediato y en forma directa con el departamento de TI de la Compañía para informar todo cambio en el estado del Empleado que requiera la terminación o modificación de los privilegios de acceso de inicio de sesión del Empleado.

Los Empleados que olvidan su contraseña deben llamar al departamento de TI o seguir las herramientas que TI proporciona para que se asigne una nueva contraseña a su cuenta. El Empleado debe identificarse (por ejemplo, con el número de empleado) ante el departamento de TI.

Los Empleados serán responsables de todas las transacciones que ocurran durante las sesiones iniciadas mediante el uso de la contraseña y la identificación del Empleado. Los Empleados no deben iniciar sesión en una computadora y luego permitir que otra persona use la computadora o comparta el acceso a los sistemas informáticos.

Acceso de administrador del sistema

Los administradores de sistemas, administradores de red y administradores de seguridad tendrán acceso de alto privilegio a sistemas de host, enrutadores, concentradores y firewalls, según sea necesario, para cumplir con las obligaciones de su trabajo.

Todas las contraseñas del administrador del sistema se **BORRARÁN** inmediatamente después de que a cualquier Empleado que tenga acceso a dichas contraseñas se lo separe del cargo, despida o desvincule, o si deja de trabajar en la Compañía. Se suspenderán las contraseñas de los Empleados con licencia administrativa o disciplinaria hasta que se restablezca el estado de empleo activo.

Acceso especial

Se proporcionan cuentas de acceso especial a las personas que requieren privilegios temporales de administrador del sistema para realizar su trabajo. La Compañía supervisa estas cuentas, y estas requieren el permiso de TI de la Compañía del usuario. La supervisión de las cuentas de acceso especial se realiza mediante el ingreso de los usuarios en un área específica y mediante la generación periódica de informes a la gerencia. En los informes, se observará quién tiene actualmente una cuenta de acceso especial, por qué motivo y cuándo caducará. Las cuentas especiales vencerán en el plazo de 2 días y no se renovarán automáticamente sin un permiso por escrito.

Conexión a redes de terceros

Esta política se establece para garantizar un método seguro de conectividad proporcionada entre la Compañía y todas las compañías de terceros y otras entidades con las que es necesario que la Compañía intercambie información electrónicamente.

“Terceros” se refiere a proveedores, consultores y socios comerciales que hacen negocios con la Compañía y otros socios que tienen la necesidad de intercambiar información con la Compañía. Solo los empleados de terceros deben utilizar las conexiones de red de terceros y exclusivamente para los fines comerciales de la Compañía. La Compañía de terceros se asegurará de que solo los usuarios autorizados puedan acceder a la información en la red de la Compañía. El tercero no permitirá que el tráfico de Internet u otro tráfico de red privada fluyan hacia la red de la Compañía. Una conexión de red de terceros se define como una de las siguientes opciones de conectividad:

- Una conexión de red terminará en un firewall y el tercero estará sujeto a las reglas de autenticación estándar de la Compañía.

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

Todas las solicitudes de conexiones de terceros deben realizarse mediante la presentación de una solicitud por escrito y ser aprobadas por el departamento de TI.

Conexión de dispositivos a la red

Solo los dispositivos autorizados pueden conectarse a las redes de la Compañía. Los dispositivos autorizados incluyen

PC y estaciones de trabajo de propiedad de la Compañía que cumplen con las pautas de configuración de la Compañía. Otros dispositivos autorizados incluyen dispositivos de infraestructura de red que se utilizan para la administración y supervisión de la red.

Los usuarios no deben conectar a la red computadoras que no pertenezcan a la Compañía, que no estén autorizadas por esta, que no sean de su propiedad o que no estén bajo su control. Los usuarios tienen específicamente prohibido conectar a la red de la Compañía cualquier dispositivo que no sea de la Compañía, como computadoras portátiles, computadoras, discos duros externos, teléfonos o tabletas.

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

Acceso remoto

Solo las personas autorizadas pueden acceder de forma remota a la red de la Compañía. Se proporciona acceso remoto a aquellos Empleados, contratistas y socios comerciales de la Compañía que tienen una necesidad comercial legítima de intercambiar información, copiar archivos o programas o acceder a aplicaciones informáticas. Las conexiones autorizadas pueden ser de una PC remota a la red o de una red remota a una conexión de red de la Compañía. El único método aceptable para conectarse de forma remota a la red interna es mediante una identificación segura.

Acceso remoto no autorizado

Está prohibida la conexión de concentradores a la PC o estación de trabajo de un usuario que esté conectada a la red de área local (LAN) de la Compañía sin el permiso por escrito de la Compañía. Además, los usuarios no podrán instalar software personal diseñado para proporcionar el control remoto de la PC o estación de trabajo. Este tipo de acceso remoto evita los métodos autorizados de acceso remoto altamente seguros y representa una amenaza para la seguridad de toda la red.

8. **Respuesta a incidentes y notificación de filtraciones de datos**

En caso de un incidente de seguridad, es importante que los Empleados de Phoenix Tower puedan identificarlo y responder adecuadamente. Cada incidente potencial será investigado al nivel que el departamento Legal y el departamento de TI consideren apropiado. La respuesta adecuada y oportuna a los incidentes de seguridad de la información ayudará a proteger los activos de Phoenix Tower.

Denuncia

- Cada Empleado es responsable de informar todas las debilidades de seguridad de la información identificadas o sospechadas, incluidas, entre otras, las violaciones de datos de PII potenciales o reales, de inmediato a TI o al departamento Legal o de Cumplimiento:
  - Línea directa: 1-844-348-5247 o https://secure.ethicspoint.com
  - Correo electrónico: security@phoenixintnl.com
- Una violación de la confidencialidad o la divulgación no autorizada de la información confidencial de Phoenix Tower también se considera un incidente de seguridad de la información y debe informarse como se describe anteriormente.
- El departamento de TI registrará los incidentes de seguridad informados para supervisar tanto los tipos

de incidentes de seguridad como el volumen de incidentes que ocurren en Phoenix Tower.

- Las pruebas relacionadas con una violación de la seguridad de la información deben recopilarse adecuadamente según las instrucciones del gerente del departamento de TI y enviarse a dicho departamento. Debe recopilarse para cumplir con las obligaciones legales, reglamentarias o contractuales y evitar violaciones de derecho penal o civil.
- Después de realizar una investigación inicial, el gerente del departamento de TI determinará si el evento es realmente un incidente de seguridad de la información. Si ha ocurrido un incidente de seguridad, el departamento Legal determinará si el incidente constituye una violación de datos que se debe informar y si son violaciones de datos que involucran PII.
- El departamento legal mantendrá un registro de los incidentes de seguridad notificados que constituyan una violación de datos.
- Solo las personas autorizadas pueden divulgar información relacionada con incidentes de seguridad de la información. Los Empleados no pueden divulgar ninguna información relacionada con un incidente de seguridad fuera de PTI sin el permiso expreso del equipo Legal.
- Después del incidente o la violación de datos, el departamento de TI será responsable de llevar a cabo una reunión con todos los Empleados y partes afectados/pertinentes para revisar los resultados de la investigación y analizar la causa raíz del incidente. Todos los Empleados involucrados en el descubrimiento o la investigación de un incidente de seguridad deben asistir a esta reunión.
- Los Empleados de Phoenix Tower o los contratistas externos involucrados en un incidente de seguridad o que se descubra que han violado la Política de seguridad de la información de Phoenix Tower, independientemente de su intención, se enfrentarán a un panel disciplinario, que determinará la falla, la acción correctiva y otras acciones adecuadas.