

Política de privacidad interna de UTREEE

Esta Política de privacidad interna de UTREEE ("Política de privacidad") establece las políticas y procedimientos de UTREEE para proteger la privacidad de los Datos personales, como se define a continuación.

La Política de privacidad es aplicable a todos los empleados de UTREEE.

1. Definiciones

Los **"controladores de datos"** son aquellas personas que determinan cómo y si se procesa la información personal. UTREEE es un controlador de datos para los fines de estos procedimientos. Cuando compartimos información con UTREEE LLC de los EE. UU., ambas organizaciones son controladores de datos.

Los **"Procesadores de datos"** son aquellas personas que procesan información personal en nombre de un controlador de datos.

Los **"Interesados"** son las personas a las que se refieren los Datos Personales.

"Datos personales" es cualquier información sobre una persona identificable. Los ejemplos de datos personales incluyen (pero no se limitan a)

- nombre, fecha de nacimiento y número de seguro social u otro documento de identidad;
- información de contacto como dirección postal, dirección de correo electrónico y números de teléfono;
- números de tarjetas de crédito y cuentas financieras;
- información médica o de salud;
- información contenida en los archivos de los empleados, incluido el historial de empleo, las evaluaciones y la información recopilada durante el proceso de solicitud y contratación; y
- información relacionada con los beneficios de los empleados, como los nombres de los dependientes, beneficiarios e información de la póliza de seguro. Los datos debidamente anonimizados y desidentificados o agregados no son datos personales.

"Proceso" se utiliza de manera muy amplia para indicar la realización de cualquier acción sobre los Datos Personales, como recopilar, registrar, organizar, almacenar, transferir, modificar, usar, retener o eliminar.

Los **"datos personales confidenciales"** son datos personales relacionados con la salud, las finanzas, la orientación sexual, las creencias religiosas o los antecedentes penales de una persona identificable.

2. Minimización de datos personales y privacidad por diseño

La protección de la privacidad es parte integral del procesamiento de datos personales de UTREEE porque ayuda a proteger a nuestros miembros y les permite sentirse cómodos compartiendo información con nosotros, y esta información nos ayuda a crecer y mejorar nuestra comunidad.

Recopilamos y procesamos datos personales de varias maneras, incluidas las siguientes:

- Miembros cuando se registran para unirse a este UTREEE, incluido el nombre, la dirección y la información de pago, o cuando utilizan varios servicios y se unen a diferentes grupos y actividades.
- Voluntarios, empleados y solicitantes como parte de su empleo o solicitud. Esta información puede incluir solicitudes de empleo, registros de capacitación de empleados, documentación de evaluaciones de desempeño, salario y otros registros de empleo.
- Invitados no miembros que visitan para ciertas actividades. Dichos procesos deben diseñarse para minimizar la recopilación o el uso innecesarios de datos personales. Por ejemplo, use un número de identificación en lugar de un número de Seguro Social cuando sea posible, y use un número de Seguro Social parcial en lugar del número completo cuando sea posible. Asimismo, el uso de datos anónimos y no identificados o agregados es generalmente preferible al uso de Datos Personales.

3. Procedimientos

Todos los empleados deben cumplir con los siguientes procedimientos:

1. Recopilación de datos y consentimiento

Antes de la recopilación y el procesamiento de los Datos Personales, UTREEE debe obtener el consentimiento del Titular de una manera adecuada al contexto. La mayoría de las veces, el consentimiento está implícito en las circunstancias. Por ejemplo, si los miembros se inscriben en una clase de natación, esperan que la información se utilice para organizar la clase y comunicarse con ellos sobre la clase. Cuando los datos personales se utilizan de formas que no están razonablemente implícitas en las circunstancias aparentes, el consentimiento puede proporcionarse oralmente, por escrito o electrónicamente, en general de forma voluntaria o excluyente, aunque los usos de los datos personales confidenciales deben tener un consentimiento más claro.

Es posible que algunas personas, como los niños o las personas con discapacidades mentales, no puedan dar su consentimiento personal para la recopilación, el uso o la divulgación de sus propios datos personales. En esos casos, podemos confiar en el consentimiento de aquellas personas que están cuidando a esa persona y que tienen derecho a dar su consentimiento en

nombre de la persona en las circunstancias dadas y de acuerdo con las leyes estatales y federales. **Los datos personales no deben recopilarse de niños sin el consentimiento claro por escrito de los padres o tutores legales, y la recopilación de datos personales confidenciales requiere un consentimiento particularmente claro para recopilarlos.**

Para notificar y recibir el consentimiento informado, divulgue lo siguiente antes de recopilar datos personales cuando no esté claro de las circunstancias:

- la identidad de la persona o entidad que recopila los Datos Personales (es decir, el Controlador de Datos);
- los fines para los que se procesarán o utilizarán los Datos Personales;
- los métodos por los cuales se recopilarán los Datos Personales;
- el alcance de los datos personales que se pueden recopilar (por ejemplo, tipos, durante qué período de tiempo, etc.); y
- la identidad de cualquier persona a la que se puedan divulgar o transferir los Datos Personales.

UTREEE no necesita obtener el consentimiento del Interesado en las siguientes circunstancias limitadas:

- en una emergencia que amenace la vida, la salud o la seguridad personal de una persona;
- cuando los Datos Personales estén disponibles y se recopilen de una fuente pública;
- cuando el tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte, o para tomar medidas a petición del interesado antes de celebrar un contrato;
- cuando el tratamiento sea necesario para el cumplimiento de las obligaciones de cumplimiento legal de la UTREEE, como investigar y proteger sus intereses legales;
- cuando el tratamiento sea necesario para proteger los intereses vitales del interesado, interpretados en sentido estricto;
- en determinadas circunstancias, cuando el tratamiento sea necesario para el desempeño de una tarea realizada en interés público;
- Cuando el tratamiento sea necesario para los intereses comerciales legítimos de la UTREEE, tal como se comunican al Titular, de conformidad con los derechos y libertades fundamentales del Titular; o
- cuando la recopilación, el uso, el procesamiento y/o la divulgación previstos estén permitidos o no excluidos por la ley aplicable.

2. Retirada del consentimiento

En algunas circunstancias, el consentimiento para la recopilación y el uso de Datos personales puede retirarse, sujeto a restricciones contractuales y legales y a un aviso razonable. En

general, nuestro UTREEE debe permitir y respetar la retirada del consentimiento en la mayor medida posible, por ejemplo, con respecto a la retirada del consentimiento para recibir materiales de marketing o llamadas telefónicas.

La retirada del consentimiento puede tener consecuencias, como no poder seguir prestando determinados servicios o comunicarse de determinadas maneras. En determinadas circunstancias, es posible que no se retire el consentimiento con respecto a ciertos usos y divulgaciones necesarios de Datos personales, como con respecto a ciertas obligaciones legales y contractuales.

Los sistemas de datos personales deben diseñarse razonablemente para permitir la retirada efectiva del consentimiento. En particular, se deben mantener listas de exclusión voluntaria y las comunicaciones deben eliminarse de estas listas para poder verificar que los destinatarios que han expresado su deseo de no recibir no están recibiendo comunicaciones, incluso si previamente dieron su consentimiento para recibir la comunicación.

El cumplimiento de dichas solicitudes es particularmente importante con respecto a cualquier campaña electrónica y de telecomunicaciones (teléfono, fax, texto, etc.), de acuerdo con los requisitos legales aplicables a la campaña. El conocimiento de las restricciones aplicables a campañas particulares es responsabilidad del gerente de esa campaña, y es su responsabilidad consultar con la gerencia de UTREEE y / o el asesor legal para lograr el pleno cumplimiento en sus circunstancias específicas.

3. Especificación de propósito y limitación de uso

Cuando se utilizan datos personales, nuestro UTREEE debe utilizar los datos personales de una manera que sea compatible con los fines para los que fueron recopilados, o para un propósito razonablemente relacionado. Si los Datos Personales deben usarse para otro propósito o manejarse de una manera que el Titular no haya dado su consentimiento, la UTREEE debe obtener el consentimiento del Sujeto de Datos para el uso nuevo o diferente.

Solo el personal de UTREEE o terceros que trabajen en nombre de este UTREEE con un propósito comercial legítimo pueden acceder o utilizar los Datos personales, e incluso esas personas pueden acceder a dichos Datos personales solo para fines legítimos requeridos por sus puestos. Cuanto más sensibles sean los Datos Personales, mayor debe ser la seguridad para protegerlos.

4. Acceso del interesado

Nuestra UTREEE debe publicar un aviso de privacidad para que los Titulares de los Datos puedan comunicarse con la persona adecuada con consultas o quejas sobre el uso de sus Datos Personales. Nuestro UTREEE debe hacer esfuerzos razonables para acceder a las solicitudes de los Titulares de los Datos para acceder a sus Datos Personales. De acuerdo con

estos procedimientos, los Titulares de los Datos pueden preguntar a la UTREEE si mantiene Datos Personales sobre ellos, y el contenido, si lo hubiera, de esos datos. Si la UTREEE niega el acceso, debe proporcionar al Titular los motivos de dicha denegación y permitir que el Titular impugne la denegación.

5. Precisión de los datos

Nuestro UTREEE debe hacer todo lo posible para procesar datos personales precisos. Con este fin, los Interesados pueden realizar solicitudes razonables para la corrección de cualquier Dato Personal incorrecto o engañoso sobre ellos. En la medida en que sea razonablemente posible, debemos, según corresponda, corregir o destruir los Datos personales que sean inexactos, engañosos o desactualizados. Si nuestro UTREEE no realiza una corrección solicitada, la solicitud debe anotarse en el archivo del Titular de los Datos en la medida de lo posible y explicarse al Interesado.

6. Retención de datos

Nuestra UTREEE no debe conservar los Datos Personales más tiempo del necesario para el propósito para el que fueron recopilados. Nuestro UTREEE debe destruir o borrar de forma segura los Datos Personales de sus sistemas cuando ya no sean necesarios para lograr el propósito para el que fueron recopilados. Nuestro UTREEE también debe esforzarse por garantizar la eliminación y destrucción seguras de los Datos Personales almacenados o mantenidos por terceros. Sin embargo, podemos retener algunos datos personales para cumplir con las leyes, regulaciones, reglas y órdenes judiciales aplicables.

7. Seguridad

Nuestro UTREEE toma medidas administrativas, técnicas y físicas razonables para protegerse contra el procesamiento o uso no autorizado de Datos Personales, y contra la pérdida accidental o el daño de los Datos Personales.

Estas medidas incluyen:

- poner a disposición planes escritos para identificar, prevenir, detectar, responder y recuperarse de amenazas e incidentes de ciberseguridad;
- desarrollar procedimientos de autenticación de seguridad para acceder a todos los sistemas que almacenan datos personales;
- mantener software antivirus parchado y actualizado, firewalls y otras medidas de seguridad informática, y designar personal apropiado para que sea responsable de mantener dichas salvaguardas actualizadas;

- exigir a los procesadores de datos de terceros, proveedores y otros proveedores de servicios que procesarán Datos personales en nombre de este UTREEE que mantengan las medidas de seguridad adecuadas;
- mantener registros adecuados de acceso y procesamiento de datos personales;
- auditar la seguridad de los datos personales a intervalos regulares (pero no menos de una vez al año) y registrar los resultados de dichas auditorías;
- usar las protecciones adecuadas, como el cifrado, para proteger los Datos Personales Confidenciales en tránsito y cuando se almacenan en medios informáticos portátiles según sea necesario o apropiado;
- utilizar métodos de destrucción apropiados y seguros de Datos Personales según lo exija la ley; y
- tomar todas las demás medidas razonables que exijan de vez en cuando las leyes y regulaciones locales.

8. Compartir Datos personal con terceros

UTREEE puede compartir los Datos Personales con sus filiales corporativas, como UTREEE de EE. UU., y terceros que prestan servicios a nuestra UTREEE en la medida en que dichos terceros estén obligados contractualmente a seguir los procedimientos establecidos en este documento, o normas sustancialmente equivalentes, y a proteger los Datos Personales de acuerdo con todas las leyes pertinentes. regulaciones y reglas, y sujeto a las medidas e instrucciones de seguridad apropiadas de nuestro UTREEE. Estos requisitos también deben aplicarse a cualquier subcontratista contratado por terceros.

Los datos personales no pueden venderse, transferirse ni divulgarse a terceros, excepto según lo autorice por escrito la gerencia de UTREEE.

Antes de divulgar los Datos Personales a un tercero, la UTREEE puede brindar al Titular la oportunidad de elegir si su información puede ser divulgada a ese tercero o utilizada para un propósito incompatible con el propósito para el cual fue recopilada originalmente o posteriormente autorizada por el Titular. En todos los casos, los Datos Personales Sensibles no deben ser revelados a terceros no afiliados ni utilizados para nuevos fines sin el consentimiento explícito o la presencia de otras circunstancias que requieran o justifiquen dicho uso.

9. Confidencialidad

Los empleados y contratistas externos no pueden divulgar la información disponible en los sistemas y redes de UTREEE, incluso a otro personal de UTREEE, excepto según lo autorice

expresamente el gerente correspondiente. El deber de no divulgación y confidencialidad se extiende a las interacciones con terceros, incluidos otros empleados, clientes, socios comerciales y proveedores.

10. Informes y respuesta a incidentes

La sospecha de robo, pérdida o procesamiento no autorizado de datos, incluidos los datos personales, debe abordarse de inmediato. Nuestro UTREEE debe tomar medidas para investigar de inmediato la causa de la violación de seguridad y hacer todo lo posible para contener la violación. Nuestro UTREEE debe seguir los pasos establecidos en el Plan de Respuesta a Incidentes de Seguridad de Datos al responder a incidentes de seguridad.

11. Información para niños

Si nuestro UTREEE tiene la intención de recopilar o utilizar información personal de niños menores de 13 años, primero debe obtener el consentimiento verificable de sus padres o tutores, como a través de formularios de consentimiento que el padre o tutor firma en persona. No es necesario obtener el consentimiento cuando la información sobre los niños es proporcionada por sus padres o tutores.

4. Consultas y disputas de privacidad

Nuestra UTREEE debe designar a una persona para manejar las quejas y disputas relacionadas con el uso de Datos Personales. Nuestro UTREEE debe informar a las personas de las que recopila Datos Personales de un número de teléfono o dirección de correo electrónico con la que pueden comunicarse para quejas o disputas sobre cómo se manejan sus Datos Personales. Estas quejas y disputas serán atendidas por la gerencia de UTREEE, quien puede decidir cuándo es apropiado consultar con un asesor legal en previsión de un posible litigio con el Sujeto de Datos. El procesamiento interno de las solicitudes de asesoría legal estaría sujeto al privilegio abogado-cliente y a las protecciones de la doctrina del producto del trabajo del abogado en la medida aplicable según la ley estatal o federal. La(s) persona(s) autorizada(s) para manejar quejas y disputas es la Directora General Bermina Amparo.

5. Cumplimiento y modificación de procedimientos

Los empleados de YMCA que violen esta Política de privacidad pueden estar sujetos a medidas disciplinarias, que pueden incluir el despido.

Según corresponda, nuestra YMCA puede modificar sus procedimientos para el manejo de Datos Personales, pero los cambios materiales en el manejo de Datos Personales no se pueden aplicar retroactivamente sin el consentimiento expreso del Sujeto de Datos, a menos que el consentimiento no sea necesario para recopilar y utilizar los Datos Personales.

Para facilitar el cumplimiento de esta Política de privacidad y proteger a sus trabajadores, sistemas, información y activos; nuestra YMCA puede revisar, auditar, monitorear, interceptar, acceder y divulgar información procesada o almacenada en equipos y tecnología de la YMCA, o en dispositivos de propiedad personal a los que se permite el acceso a la red de la YMCA. Si tiene conocimiento de cualquier incumplimiento real o sospechado de esta Política, notifique a Nathan Prenzlou al 712-262-3782. Si tiene alguna pregunta sobre esta guía, o para obtener información o capacitación adicional, comuníquese con nosotros al 712-262-3782. La gerencia de nuestra YMCA puede monitorear, evaluar y promover el cumplimiento de esta Política al • proporcionar orientación sobre la implementación y el cumplimiento de la Política; • ayudar con el diseño de iniciativas para minimizar la recopilación y otro procesamiento de datos personales; • diseñar y llevar a cabo una capacitación adecuada en privacidad; • servir como punto de contacto inicial para cuestiones de privacidad y protección de datos personales; • manejar investigaciones y resoluciones de quejas de privacidad; • proporcionar orientación sobre contratos para el procesamiento de datos personales; • monitorear los desarrollos legales relacionados con la privacidad y la protección de datos; y • proporcionar a nuestra YMCA una evaluación continua del cumplimiento de las leyes aplicables y las mejores prácticas de la industria.

6. Declaración de política

- Todos los cambios en los recursos de TI deben documentarse según el proceso de control de cambios.
- Todos los cambios en los recursos de TI deben seguir el proceso de control de cambios para garantizar la aprobación, la planificación y la ejecución adecuadas.
- Es posible que no se requieran solicitudes de cambio para entornos que no sean de producción (por ejemplo, DEV, Test, QA) a menos que haya una actualización significativa o un impacto.
- Las solicitudes de cambio de producción deben tener en cuenta que el cambio se ha aplicado, probado y verificado correctamente en un entorno que no es de producción cuando existen entornos aplicables.

- Los cambios en los entornos de producción se someten a un examen de impacto antes de la presentación de la solicitud de cambio según el proceso de control de cambios. Esta información se utilizará para determinar el impacto del cambio teniendo en cuenta:
 - El impacto que tendrá el cambio propuesto en los servicios empresariales, si se espera que cause una interrupción generalizada, una pérdida de conectividad o funcionalidad para un grupo o grupos específicos;
 - El riesgo que implica no hacer el cambio;
 - El riesgo si el cambio no sale según lo planeado; y
 - Previsibilidad del éxito del cambio.
- Los cambios significativos en la experiencia del usuario deben transmitirse al panel de control de cambios (CCB) y comunicarse a la audiencia afectada y al servicio de atención al cliente de TI (ITCC).
- Los cambios deben ser examinados por las implicaciones de seguridad a través de la participación de la Oficina de Seguridad de la Información (ISO).
- Debe ocurrir una sesión de lecciones aprendidas en caso de un incidente durante una solicitud de cambio.

7. Definiciones

El control de cambios es un enfoque sistemático para administrar todos los cambios realizados en los recursos de TI. El propósito es garantizar que no se realicen cambios innecesarios, que todos los cambios estén documentados, que los servicios no se interrumpan innecesariamente y que los recursos se utilicen de manera eficiente.

Los recursos de TI incluyen sistemas informáticos, de redes, de comunicaciones, de aplicaciones y de telecomunicaciones, infraestructura, hardware, software, datos, bases de datos, personal, procedimientos, instalaciones físicas, proveedores basados en la nube, proveedores de software como servicio (SaaS) y cualquier material y servicio relacionado.

8. Historial de versiones de directivas

Versión	Fecha	Descripción	Aprobado por
1.0	4/6/2019	Comenzó la política inicial	
1.1	5/12/2020	Revisión	
1.2	1/2/2022	Revisión	