AVISO DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES — SAVA ULEAM

Versión: 1.0
Fecha de actualización: [DÍA/MES/AÑO]

Este Aviso de Privacidad informa a los usuarios sobre el tratamiento de datos personales que puede realizarse mediante SAVA ULEAM, aplicación destinada a apoyar la gestión de solicitudes de justificación de ausencias y los procedimientos administrativos relacionados.

1. Identificación del responsable del tratamiento

Responsable del tratamiento: (Nombre de la empresa pública de la facultad).

Domicilio:

Correo electrónico:

Teléfono:

Delegado de Protección de Datos Personales, cuando corresponda: [NOMBRE Y DATOS DE CONTACTO].

2. Datos personales que pueden tratarse

Según la modalidad de acceso, las funcionalidades habilitadas y el trámite realizado, podrán tratarse las siguientes categorías:

a. **Datos de identificación:** nombres, apellidos y número de identificación personal.
b. **Datos de contacto:** correo electrónico y número de teléfono celular.
c. **Datos institucionales:** rol, cargo, facultad, carrera, unidad administrativa u otra información necesaria para determinar la pertenencia institucional y los permisos de acceso.
d. **Datos de autenticación:** información técnica necesaria para gestionar la sesión, verificar el acceso y mantener la seguridad de la cuenta.
e. **Datos del trámite:** información proporcionada en las solicitudes de justificación, fechas, motivos, documentos adjuntos, observaciones, estado del trámite y decisiones administrativas relacionadas.

f. **Datos técnicos y de auditoría:** registros de acceso, eventos de seguridad y operaciones relevantes realizadas dentro de la aplicación, cuando sean necesarios y proporcionales para su funcionamiento, seguridad y trazabilidad.

Los documentos adjuntos podrían contener datos personales de categorías especiales, incluidos datos relativos a la salud. Su tratamiento estará sujeto a las condiciones y garantías adicionales que establezca la legislación aplicable.

No todos los datos enumerados se tratarán necesariamente en todos los casos. Su recopilación dependerá de las funcionalidades efectivamente habilitadas y de la necesidad del tratamiento.

3. Finalidades del tratamiento

Los datos podrán tratarse para las siguientes finalidades:

a. Crear, verificar, administrar y mantener las cuentas de usuario.
b. Autenticar a los usuarios mediante el formulario de registro o, si se encuentra habilitado, mediante Microsoft 365 institucional.
c. Determinar los roles y permisos de acceso a las funcionalidades correspondientes.
d. Recibir, tramitar, revisar y gestionar solicitudes de justificación de ausencias.
e. Generar los documentos administrativos asociados al procedimiento.
f. Facilitar la revisión, aprobación o rechazo de solicitudes por las personas autorizadas.
g. Enviar notificaciones relacionadas con el estado y la resolución de los trámites.
h. Mantener registros de auditoría y trazabilidad cuando sean necesarios para la seguridad y el control administrativo.
i. Detectar, investigar y atender incidentes de seguridad, errores técnicos y accesos no autorizados.
j. Cumplir las obligaciones legales y administrativas aplicables al procedimiento institucional.

Los datos no deberán utilizarse para finalidades incompatibles con las informadas, salvo que exista una base jurídica válida y se cumplan las obligaciones de información que correspondan.

4. Base jurídica del tratamiento

Cada finalidad deberá sustentarse en una base jurídica válida conforme a la Ley Orgánica de Protección de Datos Personales.

Dependiendo de la naturaleza del procedimiento y de las competencias de la institución, podrán resultar aplicables el cumplimiento de obligaciones legales, el cumplimiento de una misión realizada en interés público, la ejecución de una relación contractual u otra base legitimadora prevista en la ley.

La base jurídica concreta deberá identificarse y documentarse por el responsable antes de implementar el tratamiento. No se presume que el consentimiento sea la base aplicable a todas las operaciones.

Cuando un tratamiento requiera consentimiento, este deberá cumplir los requisitos legales correspondientes. Los tratamientos de categorías especiales de datos deberán satisfacer, además, las condiciones específicas previstas en la normativa.

5. Inicio de sesión mediante Microsoft 365

Cuando esta modalidad se encuentre habilitada, el usuario podrá autenticarse utilizando su cuenta institucional Microsoft 365, conforme a la configuración técnica implementada.

En tal caso, la aplicación podrá recibir los atributos estrictamente necesarios para identificar y autenticar al usuario, como un identificador de cuenta y, cuando corresponda, el correo institucional y el nombre asociado a la cuenta.

La información concreta que se reciba dependerá de los permisos y atributos configurados en la integración.

La autenticación mediante Microsoft 365 no implica que la aplicación tenga acceso irrestricto al contenido del correo electrónico, los archivos, los contactos u otros servicios de Microsoft 365. Cualquier acceso adicional requerirá una configuración y autorización específica, una finalidad definida y una base jurídica válida.

El proveedor de identidad podrá tratar datos de acuerdo con sus propias condiciones y políticas. La información correspondiente deberá revisarse al configurar la integración.

6. Destinatarios y acceso a la información

Los datos podrán ser accesibles para las personas y entidades que necesiten tratarlos legítimamente para las finalidades descritas, conforme a sus funciones y permisos.

Esto puede incluir, según el procedimiento institucional:

a. El personal autorizado para revisar y gestionar las solicitudes.
b. Las autoridades o unidades administrativas competentes, incluida Talento Humano, cuando corresponda.
c. El proveedor tecnológico, en la medida necesaria para prestar los servicios que le hayan sido legítimamente encomendados.
d. Los proveedores de infraestructura, autenticación, alojamiento u otros servicios tecnológicos que intervengan legítimamente, cuando corresponda.
e. Las autoridades competentes cuando exista una obligación legal que justifique la entrega de información.

Los accesos deberán limitarse a lo necesario para cada función. La existencia de una relación institucional o técnica no autoriza por sí sola la consulta indiscriminada de los expedientes.

La identidad de los proveedores, las comunicaciones de datos y las transferencias nacionales o internacionales que correspondan deberán precisarse conforme a la arquitectura y los contratos efectivamente implementados.

7. Conservación de los datos

Los datos se conservarán durante el tiempo necesario para cumplir las finalidades informadas y las obligaciones legales, administrativas o de archivo aplicables.

Los plazos concretos deberán definirse considerando la naturaleza de cada registro, el procedimiento institucional, las obligaciones de conservación y la necesidad de atender reclamaciones o responsabilidades legales.

Al finalizar el período aplicable, los datos deberán eliminarse, bloquearse o anonimizarse según corresponda, salvo que exista una obligación jurídica que justifique su conservación.

Plazos específicos de conservación: 1.6 años (un año con seis meses).

8. Seguridad de los datos

Se aplicarán medidas técnicas y organizativas proporcionales a la naturaleza de los datos y a los riesgos del tratamiento, orientadas a preservar su confidencialidad, integridad y disponibilidad.

Estas medidas podrán incluir controles de acceso, autenticación, registros de auditoría, mantenimiento de software, respaldos, protección de comunicaciones y procedimientos de gestión de incidentes, según las funciones y responsabilidades de cada participante.

La administración de la infraestructura y la distribución concreta de las obligaciones de seguridad se determinarán conforme a los acuerdos aplicables. Esta descripción no constituye una garantía de seguridad absoluta ni sustituye las medidas que deban implementarse efectivamente.

Cuando se produzca una vulneración de seguridad, se aplicarán los procedimientos correspondientes para evaluar el incidente y efectuar las notificaciones exigidas por la legislación vigente.

9. Cookies de sesión y autenticación

SAVA ULEAM podrá utilizar cookies de sesión u otros mecanismos técnicos necesarios para mantener la sesión autenticada, gestionar el acceso a las funcionalidades y contribuir a la seguridad de la cuenta. Estas tecnologías se utilizarán de acuerdo con su finalidad y configuración.

El usuario puede cerrar su sesión al terminar de utilizar la aplicación y **deberá tomar** precauciones adicionales al acceder desde dispositivos compartidos. La gestión técnica, configuración, protección y eliminación de las cookies utilizadas por la aplicación corresponderá a los mecanismos implementados en la plataforma y al funcionamiento del navegador, según corresponda.

Las cookies estrictamente necesarias para la autenticación y seguridad deberán distinguirse de aquellas que requieran información adicional o una base jurídica específica. El uso de estas tecnologías no sustituye las obligaciones legales de seguridad y protección de datos de los responsables y encargados del tratamiento, según corresponda.

10. Derechos de los titulares

Los titulares podrán ejercer los derechos reconocidos en la legislación ecuatoriana, de acuerdo con los requisitos, procedimientos y excepciones aplicables.

Entre ellos se encuentran los derechos de acceso, rectificación y actualización, eliminación, oposición, portabilidad y los demás previstos en la LOPDP.

Las solicitudes podrán presentarse a través de:

Correo para solicitudes de protección de datos: Datos del responsable de la facivitec

Canal alternativo:

El responsable deberá verificar la identidad del solicitante cuando resulte necesario, tramitar la solicitud dentro de los plazos legales y explicar los motivos de cualquier limitación que corresponda conforme a la ley.

El ejercicio de estos derechos no supone necesariamente la eliminación de documentos que deban conservarse por una obligación legal o administrativa. Cada solicitud se evaluará de acuerdo con las circunstancias y la normativa aplicable.

11. Datos obligatorios y consecuencias de no proporcionarlos

Los datos estrictamente necesarios para crear la cuenta, verificar la identidad, asignar permisos o tramitar una solicitud deberán identificarse como tales en el formulario correspondiente.

La falta de información indispensable podrá impedir la creación de la cuenta o la gestión del trámite concreto, cuando esa consecuencia sea necesaria y esté debidamente justificada.

No se solicitarán datos adicionales sin una finalidad definida y una base jurídica aplicable.

12. Actualizaciones de este aviso

Este aviso podrá actualizarse cuando cambien las funcionalidades, las finalidades, los proveedores, las modalidades de autenticación o las condiciones jurídicas del tratamiento.

Las modificaciones relevantes deberán comunicarse por medios apropiados y, cuando corresponda, antes de iniciar el nuevo tratamiento.

13. Reclamaciones

Si el titular considera que sus derechos no han sido atendidos adecuadamente, podrá acudir a la Superintendencia de Protección de Datos Personales, sin perjuicio de los mecanismos previstos en la legislación ecuatoriana.