UFLO
UNIVERSIDAD

Política de Seguridad de la Información

Autoridades del Rectorado

Arq. Ruth Fische
Rectora

Lic. Christian Kreber
Vicerrector General

Dra. Analía Verónica Losada
Vicerrectora General en Docencia e Investigación

Mg. Julieta Gomez Zeliz
Secretaria Académica Regional Buenos Aires

Esp. Micaela Alejandra de Vega
Secretaria Académica Regional Comahue

Lic. María Victoria Jimenez
Secretaria General de Investigación y Desarrollo

Cdra. Susana Perinat
Secretaria General de Administración y Finanzas

Esp. Natalia Arias
Secretaria de Vinculación Regional Buenos Aires

Lic. Emiliano Sapag
Secretario de Vinculación Regional Comahue

Lic. Florencia Peralta
Directora de evaluación

Ing. Francisco Tassara
Director de procesos y datos

Ing. Ariel Veneziano
Director de Sistemas

Mg. Beatriz Baroni
Directora de Internacionalización y posgrado

Créditos

RESOLUCIÓN Nº 82/2022 DEL CONSEJO SUPERIOR DE LA UNIVERSIDAD DE FLORES

Para la realización de este documento de carácter institucional y a pedido del rectorado UFLO, se conformó un grupo de trabajo conformado por miembros que participan de diferentes áreas institucionales, cumpliendo a su vez distintos roles y funciones. El grupo de trabajo organizó diferentes tareas:

1. relevar información,
2. realizar un análisis comparativo de documentos similares de diferentes instituciones,
3. relevar nuestros propios sistemas de datos y plataformas comunicativas digitales,
4. decidir los tópicos y aspectos más relevantes sobre los cuales destacar buenas prácticas de uso,
5. producir el material, someter a aprobación del Consejo Superior UFLO.

Autores:

Ariel Veneziano
Juan Carretero
Ignacio Bengochea
Francisco Tassara
Ana Clara Genta
Sandra Sarda
Fabiana Grinsztajn

Acerca de este documento

La información es un activo que, como otros bienes y servicios requeridos para el cumplimiento de los objetivos de la Universidad, resulta esencial para el desarrollo de sus actividades. En consecuencia, necesita ser protegida adecuadamente.

Dicha información puede presentarse en diversos formatos (impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos o como contenido multimedial, entre otros). Por lo tanto, debe estar apropiadamente protegida desde su creación, durante todo su ciclo de vida y hasta su eventual destrucción, desuso o archivo definitivo.

La seguridad de la información es la protección de la información de un rango amplio de amenazas, con el objeto de minimizar los riesgos a los que se encuentra expuesta y asegurar la continuidad de la operación normal de la Universidad. **Tiene por objetivos la preservación de la confidencialidad, integridad y disponibilidad de la información, así como del equipamiento necesario para trabajar con ella.** Consideramos la seguridad de la información no solo desde el dato en sí mismo, sino del medio en el cual se genera y se manipula, por eso estas políticas abarcan tanto la información como el medio tecnológico que hace posible el trabajo y acceso a ella (equipamiento físico y plataformas institucionales).

Dicho estado de protección adecuada se logra implementando un conjunto de mecanismos de seguridad o controles que incluyen entre otros, procesos, políticas, procedimientos, estructuras organizacionales, software y hardware. Se necesita establecer, implementar, monitorear, revisar y mejorar estos mecanismos para fortalecer el cumplimiento de los objetivos de seguridad específicos.

Del mismo modo, los procesos, sistemas y redes de apoyo son también activos importantes. Definir, lograr, mantener y mejorar la seguridad de la información es esencial para preservarlos, mantener la eficacia en la operación, cumplir con el marco legal y las normas internas, y preservar la imagen de la Institución.

Las Universidades, como cualquier organización, enfrentan amenazas de seguridad en sus sistemas y redes de información, cada vez más frecuentes y sofisticadas. La seguridad de la información es importante para el desarrollo de sus actividades y para proteger las infraestructuras críticas de información que permiten la ejecución de sus tareas.

Esta política se divide en tres partes, y guarda la siguiente estructura:

- Un capítulo introductorio, que presenta la política, su relevancia y alcance.
- El desarrollo de los términos de referencia que dan marco a la política.
- Cuatro puntos o cláusulas que abarcan los diferentes aspectos o dominios de la seguridad de la información. Se presentan de manera sistemática y consistente. Cada punto contiene un número de categorías o grupo de control de seguridad principales.

Contenido

Capítulo 1: Aspectos generales

Objeto

La presente **Política de Seguridad de la Información** (en adelante, PSI) establece las directrices y líneas de actuación en materia de seguridad de la información que establecen el modo en que **UFLO Universidad** debe gestionar y proteger los datos a los que da tratamiento, los recursos tecnológicos que utiliza y los servicios que brinda.

Detalla también lineamientos respecto a la Política a los empleados bajo cualquier modalidad de contratación y demás involucrados internos y externos, así como respecto a su implementación en todas las dependencias de la Universidad.

El objetivo principal de esta PSI es definir el propósito, la dirección, los principios, las reglas básicas y los mecanismos de comunicación para la protección de la información de la institución, así como de los recursos utilizados en su tratamiento.

El presente documento se dicta en cumplimiento de las disposiciones legales vigentes, tanto externas a la institución así como internas de la propia entidad, como políticas, procedimientos, cláusulas contractuales, acuerdos con empleados y terceros, etc.

Una adecuada gestión de la seguridad de la información permite proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad de la información, así como el cumplimiento de las normas aplicables.

Alcance

Esta PSI se aplica en todo el ámbito de **UFLO Universidad**, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Debe ser comunicada fehacientemente y cumplida por todos los agentes que la integran, cualquiera sea su modalidad de vinculación y contractual y las fuentes de financiamiento correspondientes. En su alcance se encuentran tanto el personal que desempeñe funciones directivas como administrativas o técnicas, cualquiera sea su vínculo/relación contractual, su nivel jerárquico y las tareas que desempeñe.

Asimismo, debe ser conocida y cumplida por todas aquellas personas, ya sean internos o externos, vinculadas a la institución a través de contratos, convenios, acuerdos o algún otro instrumento válido para establecer la relación con terceros, en la medida en que les sea aplicable y en las secciones que le corresponden.

Principios básicos

Los principios de la seguridad de la información son la confidencialidad, la integridad y la disponibilidad de la información a la que le dan tratamiento y de los activos de información utilizados para su gestión. La protección de la información de UFLO Universidad es el objetivo central de esta PSI. Los contenidos de este documento están alineados y se complementan con el resto de las políticas y normativas internas de la institución, que entiende la importancia de gestionar eficazmente la seguridad de la información. En consecuencia, declara su compromiso y total apoyo a la gestión de la seguridad de la información como parte integrante de la gestión del resto de los procesos establecidos en su ámbito.

Asimismo, sus autoridades se comprometen a liderar la mejora continua de los procesos de gestión de seguridad de la información, asegurando su eficacia y eficiencia. Las personas alcanzadas por esta PSI reciben una concientización periódica y pertinente a su función, respecto del compromiso que asumen para cumplir con esta PSI. Para ello, se asignan los recursos necesarios.

El incumplimiento de esta política tendrá como resultado la aplicación de sanciones disciplinarias, conforme a la magnitud y característica del aspecto no cumplido, de acuerdo con la normativa vigente. Al respecto, se establece una graduación en las responsabilidades y sanciones administrativas que se aplicarán de acuerdo con la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.

Revisión y actualización

UFLO Universidad se compromete a revisar esta PSI anualmente, adaptándola a nuevas exigencias organizativas o del entorno, así como a comunicarla a su planta de personal y a los terceros involucrados. También dispondrá las medidas necesarias para que esté a disposición de los alcanzados en todo momento.

Adicionalmente, procederá a su revisión y eventual modificación, cada vez que se produzca un cambio significativo en la plataforma tecnológica, una modificación de la normativa vigente aplicable, un cambio en los objetivos estratégicos del organismo o cualquier otro evento que lo amerite.

Alineación con estándares internacionales

Todas las definiciones de la presente PSI están alineadas con los estándares internacionalmente aceptados para la práctica de seguridad de la información, particularmente respecto de: NORMA IRAM/ISO/IEC 27002:2013 Código de Buenas Prácticas para la Seguridad de la Información.

Alineación con regulaciones argentinas en relación con la materia

Todas las definiciones de la presente PSI están alineadas con los requerimientos particulares de: Ley N° 25.326 sobre PROTECCIÓN DE LOS DATOS PERSONALES Y REGLAMENTACIÓN DEL Artículo N° 43 DE LA CONSTITUCIÓN NACIONAL (conocida como Ley de Habeas Data) y Ley N° 11. 723 sobre Propiedad Intelectual (y sus reglamentaciones relacionadas).

Capítulo 2: Términos de referencia

2.1 Seguridad de la Información

La Seguridad de la Información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** Garantiza que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ella.
- **Integridad:** Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** Garantiza que las/los usuarias/os autorizadas/os tengan acceso a la información y a los recursos relacionados con esta, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

- **Autenticidad:** Validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el/la emisor/a para evitar suplantación de identidades.
- **Auditabilidad:** Todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación:** Asegura que una transacción solo se realiza una (1) vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **No repudio:** Refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad:** Cumplimiento del ordenamiento jurídico (leyes, reglamentaciones, procedimientos, etc.) al que está sujeto el Ministerio, y en particular, aquel que hace a la seguridad.

- **Confiabilidad de la Información:** La información generada debe ser adecuada para sustentar la toma de decisiones y la ejecución

2.1.1 Definiciones:

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, clasificación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- **Tecnología de la Información:** Se refiere al hardware y software operados por el Ministerio, o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Ministerio, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

- **Propietaria/o de la Información:** Define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

2.2 Evaluación de Riesgos

Se entiende por Evaluación de Riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de su procesamiento, la probabilidad de que ocurran y su potencial impacto en la operatoria de la Universidad.

2.3 Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

2.4 Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo. NOTA. La Gestión de Riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

2.5 Incidente de Seguridad

Un Incidente de Seguridad es un evento adverso en un sistema de información, ya sean computadoras, red de computadoras u otros medios que contengan información, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

2.6 Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

2.7 Amenaza

Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

2.8 Vulnerabilidad

Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

2.9 Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal. NOTA. Control es también utilizado como sinónimo de salvaguarda o de contramedida.

Capítulo 3: Cláusulas

Entrega de equipamiento

- Notebook:
  Marca:
  Modelo:
  Memoria:
  HD:
- Teléfono:
  Marca:
  Modelo:

- Accesorios:
- Otros:

Al recibir tu nuevo equipamiento, estás aceptando:

- Hacerte responsable del mismo, su custodia, cuidado y buen uso.
- De igual manera debes tener presente que es un equipo delicado, razón por la cual debes manipularlo de manera adecuada.
- El equipamiento entregado es de uso personal e intransferible, disponibilizado con el fin de realizar tus tareas institucionales. Queda prohibida la cesión de portátiles entre usuarios sin autorización expresa de la institución.

- Debes reportar inmediatamente cualquier anomalía en cuanto a condiciones físicas y de funcionamiento.
- No está permitido manipular el hardware y el software instalado originalmente en el equipo. Así mismo, debes abstenerte de descargar programas o apps en el equipo que no estén autorizadas por la institución.
- La salvaguarda y confidencialidad de los datos de la portátil y/o celular corporativo son de tu responsabilidad.
- El programa antivirus y/o el firewall deben estar siempre activos, así mismo los equipos podrán disponer de una herramienta de gestión y monitoreo remoto que podrá ser usada por el Departamento de Soporte técnico de la Universidad.
- La pérdida, extravío, hurto o robo del equipo, deberá ser informado de manera inmediata vía correo electrónico al área de Personal una vez detectado el infortunio. Además, podremos solicitarte la denuncia policial correspondiente en el transcurso de los días posteriores.
- Ante la devolución del equipo, el mismo deberá estar acompañado de los accesorios entregados juntos al mismo, tales como mouse, cargador y/o dispositivos de almacenamiento.
- El equipamiento podrá ser auditado por personal de la Universidad, sin mediar actos previos.
- La propiedad del equipamiento es de UFLO Universidad y podrán ser retirados si se verifica un uso inadecuado.

POLITICAS DE USO - INTERNAS

UFLO Universidad provee el acceso a todo el personal a fuentes de información nacional e internacional y promueve un ambiente digital que fomente la difusión del conocimiento, el proceso de creación y el trabajo colaborativo, en el marco del Propósito Superior de la Organización.

Los usuarios deben hacer uso responsable y ético tanto del equipamiento asignado como de los softwares utilizados en la operatoria de

la institución. Cada usuario es responsable por la integridad de estos recursos y tiene el deber de respetar los derechos de los otros usuarios, la integridad de las instalaciones físicas y sus métodos de control, además de respetar toda licencia pertinente y acuerdo contractual que esté relacionado con los sistemas de información de la Organización.

Los usuarios tienen la responsabilidad de informar a su jefe inmediato, al responsable de Informática o a quien haga sus veces, de los incidentes relacionados con el uso indebido de los sistemas de información. La Universidad puede restringir o prohibir el uso de sus sistemas de información en cualquier caso en el que se demuestre alguna violación de estas políticas o de alguna ley.

No está permitido el uso del wifi institucional con fines diferentes a los propios de las actividades académicas, del medio o tareas administrativas de la Universidad.

Las identificaciones y claves de acceso a la red empresarial, plataformas que dan soporte a la operatividad de la institución o los sistemas de información propios de la organización son para uso estrictamente personal e intransferible. La responsabilidad en su manejo recae exclusivamente en el usuario a quién se le asignen.

Queda prohibido:

- El uso de la red corporativa para la operación de software de descarga y distribución de archivos de música, videos y similares.
- Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
- Utilizar los sistemas de información para propósitos ilegales o no autorizados.
- Enviar cualquier comunicación electrónica fraudulenta.
- Usar las comunicaciones electrónicas para revelar información privada sin la autorización explícita de la institución.
- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo utilizando herramientas de la Institución.

- Utilizar cualquier sistema de información de la Organización para acceder, descargar, imprimir, almacenar, reenviar, transmitir o distribuir material no permitido o correos electrónicos de tipo “cadenas”.
- De acuerdo con las normas locales e Internacionales relativas a los derechos de propiedad intelectual, el único software que será instalado en el computador del usuario será aquel que previamente haya sido estandarizado y/o autorizado por la Organización.

Correo electrónico, medios de difusión y redes sociales

El correo electrónico debe usarse de manera profesional y cuidadosa dada su facilidad de envío y redirección. Los usuarios deben ser especialmente cuidadosos con los grupos de destinatarios, chats y foros de discusión. Las leyes de derechos de autor y licencias de software también aplican para correo electrónico.

Los mensajes de correo electrónico, redes sociales o cualquier elemento de difusión que escoja la Organización en el dominio de la misma deben ser utilizados **para uso estrictamente laboral.**

Para hacer una óptima utilización de la capacidad del buzón de mensajes, los mensajes de correo electrónico en los dominios pertenecientes a la institución, deben ser borrados una vez que la información contenida en ellos ya no sea de utilidad.

Participar en una cadena de correos es una violación de las Políticas de Uso Aceptable.

En ningún caso está permitido suplantar las cuentas de usuarios ajenos.

En el caso de poseer una cuenta de correo institucional, la misma es para uso estrictamente académico y/o de gestión, queda prohibido:

- La utilización de la misma con fines personales y/o comerciales.
- El envío de SPAM desde dicha cuenta.
- Participar en una cadena de correos es una violación de las Políticas de Uso Aceptable.
- La responsabilidad es netamente del poseedor
- Ante cualquier anomalía detectada, la institución se reserva el derecho de cerrar dicha cuenta institucional

Incumplimiento de las políticas

En materia de irregularidades o incumplimiento en el uso del software, el usuario que no cumpla con estas políticas, será directamente responsable de las acciones disciplinarias o sanciones por entes externos, que por la responsabilidad laboral, penal y/o civil se incurra, derivadas de sus propios actos. Igualmente será responsable de los costos y gastos en que pudiera incurrir la Organización derivados de la defensa por el uso no autorizado o indebido de licencias de software. En razón de lo anterior, no es permitido alegar ignorancia ni a estas políticas, ni a la documentación que en las licencias de software se menciona, incluyendo por supuesto las demás licencias en uso.

La privacidad de los usuarios no está garantizada.

Cuando los sistemas de información de la Organización funcionan correctamente, un usuario puede considerar que sus datos generados son información privada, a menos que él mismo realice alguna acción para revelarlos a otros. Los usuarios deben ser conscientes que ningún sistema de información es completamente seguro, por lo cual, personas dentro y fuera de la Organización pueden encontrar formas de tener acceso a la información. De acuerdo con lo anterior, la Organización no puede garantizar la confidencialidad absoluta de la información almacenada en cualquier dispositivo perteneciente a la empresa y por ende la privacidad de los usuarios.

Sobre las instalaciones

Dejar las instalaciones y equipamiento general en las mismas condiciones de limpieza y orden en que los recibió al inicio de la jornada.

Queda prohibido:

- La ingesta de alimentos y bebidas en los laboratorios y salas. Se deberán utilizar los espacios destinados a tales fines.
- El acceso a los laboratorios a personas no autorizadas.
- Desconectar los equipos o cualquiera de sus componentes.
- El uso de los laboratorios como salas de estudio o juegos.
- Cambiar de sitio los equipos, sus componentes, las sillas, mesas, y cualquier otro material que se encuentre en los laboratorios.

Resguardo de información

Considerando que la información producida en la Universidad es el principal activo, ya sea en producciones finales o como facilitador de la gestión de la misma, es por eso que:

- Posee distintos medios y herramientas de resguardo considerados seguros.
- Se encuentra en constante búsqueda de nuevos medios y actualización de los medios existentes, conforme van cambiando dinámicamente las normas que rigen sobre dichos temas.
- Posee políticas de backups de la información de acuerdo al origen, medio, importancia y celeridad de recuperación de la misma ante una catástrofe.

Visto y considerando, la institución determina:

- Es responsabilidad de cada equipo de trabajo el solicitar los espacios necesarios para alojar la información producida, mediar en los accesos permitidos y restricciones de acceso tanto del propio equipo interno como por integrantes externos.

- Cada Líder de equipo es responsable de que la información producida dentro de su ámbito de acción sea respaldada en los medios que la universidad provea.

- UFLO Universidad, como ente superior, posee el derecho de acceso total a todos los repositorios y la potestad de auditar los contenidos y los usos de dichos espacios con el fin de garantizar que toda la información institucional se encuentre en un lugar resguardado y accesible. Así mismo, conserva la potestad de modificar, actualizar o aggiornar las herramientas utilizadas para tales fines.

POLITICAS DE USO GENERALES EXTERNOS

No está permitido el uso del wifi institucional con fines diferentes a los propios de las actividades académicas, del medio o tareas administrativas de la Universidad.

Cada alumno o docente es responsable del equipamiento que esté utilizando.

Se debe informar cualquier irregularidad encontrada en los equipos y/o materiales disponibles para el desempeño regular de la tarea a realizar.

Cuando se termine de utilizar un equipo informático, se deberá apagar por completo.

Dejar las instalaciones y equipamiento general en las mismas condiciones de limpieza y orden en que los recibió al inicio de la jornada.

Queda prohibido:

- La ingesta de alimentos y bebidas en los laboratorios.
- El acceso a los laboratorios a personas no autorizadas.
- Desconectar los equipos o cualquiera de sus componentes.
- El uso de los laboratorios como salas de estudio o juegos.
- Cambiar de sitio los equipos, sus componentes, las sillas, mesas, y cualquier otro material que se encuentre en los laboratorios.

En el caso de poseer una cuenta de correo institucional, la misma es para uso estrictamente académico o actividades relacionadas a la organización, como así también queda prohibido:

- La utilización de la misma con fines personales y/o comerciales.
- El envío de SPAM desde dicha cuenta.
- Participar en una cadena de correos es una violación de las Políticas de Uso Aceptable.
- La responsabilidad es netamente del poseedor
- Ante cualquier anomalía detectada, la institución se reserva el derecho de cerrar dicha cuenta institucional.

ACUERDO DE CONFIDENCIALIDAD

COMPROMISO DE CONFIDENCIALIDAD.

En la Ciudad Autónoma de Buenos Aires, a los ..... días del mes de ..... del año 202...., el Sr./a ....., titular del documento de identidad tipo DNI Nº:....., con domicilio real en la calle .....Piso...Dpto..... ,Localidad....., Provincia....., en adelante EL CONTRATADO, quien se desempeña como.....en el área de ..... en Sede....., declara conocer que los datos e información a los que tendrá acceso con motivo del desarrollo de sus funciones se encuentran amparados por la siguiente legislación: Ley de Hábeas Data Nº 25.326, Ley de Confidencialidad Nº 24.766, Reglamento General Uflo y Normas Académicas y Administrativas de la Universidad y el Código Penal de la República Argentina.
Sin perjuicio de las obligaciones de secreto y reserva previstas en la normativa referida precedentemente, EL CONTRATADO mediante la suscripción del presente se compromete en forma irrevocable ante la Universidad a dar cumplimiento a lo dispuesto en las siguientes cláusulas:

PRIMERA: EL CONTRATADO se obliga a no revelar, divulgar o facilitar bajo cualquier forma a ninguna persona física o jurídica Información Confidencial, siendo entendida ésta como toda información que no sea pública y de la que EL CONTRATADO tenga conocimiento o tenga acceso por cualquier medio o circunstancia en virtud del desarrollo de sus funciones. Se incluye dentro de la misma la relacionada con el funcionamiento de la Universidad, de su gestión académica, de investigación, de extensión, de transferencia tecnológica, como así también la referida a su infraestructura, hardware, software, datos, usuarios, claves de acceso a sistemas y toda otra información técnica, jurídica, administrativa, contable, financiera y estratégica de la Universidad de Flores.
Se obliga también a no utilizar para su propio beneficio o para beneficio de cualquier otra persona toda la información relacionada con el

ejercicio de sus funciones, su participación en proyectos de investigación, desarrollo de software, sistemas de información aún cuando éstos se encuentren en etapa experimental o de desarrollo.

SEGUNDA: EL CONTRATADO se compromete a guardar máxima reserva y secreto sobre el usuario y contraseña de acceso a los sistemas que le fueren concedidos para el desarrollo de sus funciones, debiendo utilizarlos solamente para el fin específico asignado.

TERCERA: EL CONTRATADO asume la obligación de reserva y confidencialidad acordada por el presente compromiso durante todo el período que mantenga la relación contractual con la Universidad y por un plazo adicional de CINCO (5) años contados a partir de la extinción del vínculo con esta Universidad.

CUARTA: Se deja constancia que la violación o el incumplimiento de la obligación de confidencialidad a cargo del CONTRATADO, así como la falsedad de la información que pudiere brindar a terceros, generará responsabilidad administrativa y facultará a LA UNIVERSIDAD para aplicar al CONTRATADO las sanciones que le correspondan, conforme el régimen disciplinario que le comprenda, pudiendo la falta cometida dejarlo incurso en el delito de violación de secreto tipificado en el Artículo 156 del Código Penal de la Nación, siendo facultad de LA UNIVERSIDAD formular la denuncia del caso y constituirse en parte querellante. Además de ello, la facultad de la UNIVERSIDAD de requerir el resarcimiento económico de los daños ocasionados y/o el perjuicio sufrido conforme el artículo 11 de la Ley 24.766.-

Firma y aclaración del CONTRATADO

UFLO
UNIVERSIDAD

Política de Seguridad de la Información