APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE AYSÉN.

COYHAIQUE, 30 de diciembre de 2024

RESOLUCIÓN UNIVERSITARIA EXENTA

N° 368 de 2024

VISTOS: Lo dispuesto el Decreto con Fuerza de Ley N° 7, de 05 de agosto de 2016, del Ministerio de Educación, que fija los Estatutos de la Universidad de Aysén; la Ley N° 21.094, sobre Universidades Estatales; la Ley N° 20.800 sobre administración provisional, la Ley N°19.628 sobre Protección de la Vida Privada, la Ley N°19.223 que define y Penaliza los Delitos Informáticos, la Ley N°19.799 sobre Documentos Electrónicos, la Resolución Exenta N°10, de 04 de enero de 2024, de la Superintendencia de Educación Superior que contiene el nombramiento del Administrador Provisional; la Resolución TRA N°121418/4/24 que nombra Secretario General de la Universidad de Aysén; y las resoluciones 6 y 7 de 2019 de la Contraloría General de la República y otras normas legales pertinentes.

CONSIDERANDO:

1. Que, es necesario proteger la información institucional en todas sus formas contra el acceso no autorizado, divulgación, alteración, destrucción o interrupción, en el contexto de una creciente dependencia de las tecnologías de la información.
2. Que, existe la necesidad institucional y legal de asegurar la confidencialidad, integridad, y disponibilidad de la información gestionada por la Universidad de Aysén, en línea con los principios de seguridad de la información reconocidos nacional e internacionalmente.
3. Que, es de vital importancia cumplir con los requisitos legales y reglamentarios aplicables a la seguridad de la información y la protección de datos personales, incluyendo la Ley N°19.628 sobre Protección de la Vida Privada, la Ley N°19.223 que Define y Penaliza los Delitos Informáticos, la Ley N°19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma.
4. Que, resulta conveniente el adoptar y adherir a las mejores prácticas y estándares internacionales en seguridad de la información, como las normas ISO/IEC 27001 y ISO/IEC 27002, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente la seguridad de la información

RESUELVO

1) APRUEBASE la Política General de Seguridad de la información de la Universidad de Aysén y cuyo texto es el siguiente:

"**Política General de Seguridad de la Información de la Universidad de Aysén.**

Índice

Compromiso Institucional

La efectividad de la gestión de riesgos depende del compromiso y la colaboración de todas/os en la Universidad. Por lo tanto, se espera que todos los(as) funcionarios(as) participen activamente en la identificación de riesgos y en la implementación de estrategias de tratamiento. La formación y concienciación en seguridad de la información serán proporcionadas regularmente para asegurar que todos los miembros de la comunidad universitaria comprendan su papel en la protección de los activos de información.

Introducción y Propósito

La Universidad de Aysén, consciente del valor crítico que la seguridad de la información representa para la integridad y el resguardo de sus activos informativos, establece mediante esta Política General de Seguridad de la Información (PGSI) las directrices esenciales para la protección efectiva contra cualquier amenaza, ya sea interna o externa, deliberada o accidental. Esta política no solo define el marco de referencia para la salvaguarda de la información, sino que también actúa como el mecanismo principal para entregar directrices claras y concisas sobre la materia, promoviendo una cultura organizacional que prioriza la seguridad en el manejo de la información y los sistemas de información. Es esencial para asegurar la confidencialidad, integridad y disponibilidad de nuestros recursos informativos, y abarca a toda nuestra comunidad universitaria, incluyendo personal de colaboración, académicos y académicas, estudiantes y terceros vinculados. La efectiva implementación de esta PGSI es fundamental para cumplir con nuestras obligaciones legales, reglamentarias, y contractuales, y para sostener la confianza depositada por estudiantes, personal, y socios externos en nuestra capacidad para proteger su información.

Alcance

Esta Política General de Seguridad de la Información se aplica a toda la comunidad universitaria de la Universidad de Aysén, incluyendo funcionarios y funcionarias, académicos y académicas (tanto de planta, contrata y honorarios), estudiantes, contratistas, socios comerciales, y cualquier tercero que acceda o gestione información en nombre de la Universidad. El alcance de esta política abarca toda la información, en cualquier forma de expresión (digital, papel, oral), sistemas de información, infraestructuras tecnológicas, redes de comunicaciones, y todos los procesos de negocio que involucran el manejo de datos e información de la Universidad. Además, se extiende a todos los dominios de la Institución, sus direcciones, departamentos, y cualquier unidad organizativa que maneje o almacene activos de información institucionales

Son activos de información **"toda información o recurso relacionado para la creación, almacenamiento, manejo o transmisión de dicha información de la Universidad, incluyendo los** recursos y sistemas informáticos de la Universidad de Aysén.

En materia de equipamiento, comprenderán como mínimo:

- Equipamiento e infraestructura de la red de datos y de telecomunicaciones de la Universidad.
- Los servidores institucionales.
- Las plataformas de software instaladas para proporcionar servicios a la comunidad universitaria.
- Los sistemas informáticos desarrollados internamente, o sistemas externos y/o software debidamente licenciados.
- Todo el equipamiento es propiedad de la Universidad, lo que incluye equipos computacionales, periféricos computacionales, y todo otro equipamiento tecnológico conectado a la red corporativa. Entre otros se incluyen: computadores, impresoras, proyectores, cámaras, etc.

Esta inclusión garantiza que la seguridad de la información se gestione de manera integral, cubriendo todos los recursos tecnológicos y sistemas de información que soportan las operaciones académicas,

investigativas, y administrativas de la Universidad.

Principios de Seguridad de la Información:

La Universidad de Aysén gestiona los activos de información en consonancia con los principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad.

- Confidencialidad: Asegurar que la información solo sea accesible para aquellos autorizados a tener acceso, protegiendo la información contra accesos o divulgaciones no autorizadas.
- Legalidad: Las operaciones deben cumplir con las reglamentaciones legales vigentes. Es responsabilidad indelegable de cada funcionario el velar por el cumplimiento de este principio en su ámbito de competencia, debiendo resolver cualquier duda ante las instancias pertinentes.
- Integridad: Mantener la precisión y completitud de la información y los métodos de procesamiento, previniendo la alteración no autorizada de la información.
- Disponibilidad: Garantizar que las personas usuarias autorizadas tengan acceso a la información y a sus activos asociados cuando lo requieran.
- Propiedad: Todos los derechos de propiedad de la universidad de Aysén deben estar adecuadamente establecidos y protegidos. Será responsabilidad de cada gestor de procesos. productos o iniciativas que contengan o generen derechos de propiedad, velar por el cumplimiento de este principio.
- Protección de Datos Personales: Cumplir con la Ley N° 19.628 sobre la protección de la vida privada y el tratamiento de datos personales, respetando los principios de consentimiento para el tratamiento de datos, el derecho de las personas a acceder, rectificar y cancelar sus datos, y la finalidad específica del uso de estos datos. La confidencialidad y seguridad de los datos personales serán garantizadas en todas las etapas de su tratamiento.

Estos principios se aplican a toda la información que maneja la Universidad, independientemente de su forma, soporte, origen o método de creación, para asegurar que las prácticas de seguridad de la información estén alineadas con los objetivos institucionales.

Estándares de Seguridad de la Información

Para los propósitos de esta Política General de Seguridad de la Información, se entenderá por "estándar" cualquier política, proceso, procedimiento, norma, lineamiento, protocolo, o cualquier otro documento desarrollado para cumplir y sostener los objetivos de seguridad de la información de la Universidad.

Compromiso con los Estándares de Seguridad:

La Universidad de Aysén se compromete a desarrollar, implementar y mantener los estándares necesarios para proteger la información contra accesos no autorizados, divulgación, alteración, destrucción o pérdida, de manera coherente con los principios de seguridad de la información establecidos en esta política y en alineación con la norma ISO/IEC 27001.

Los estándares desarrollados bajo este marco abordarán, entre otros, los siguientes temas:

1. Gestión de la seguridad de la información: Establecimiento de un marco de gestión para asegurar la continuidad de la protección de la información en toda la organización.
2. Evaluación y tratamiento de riesgos: Identificación, análisis y tratamiento de los riesgos de seguridad de la información.
3. Seguridad operacional: Implementación de controles operacionales y procedimientos para garantizar la seguridad de los procesos y la información.
4. Seguridad física y del entorno: Protección de las instalaciones y equipamiento contra amenazas físicas y daños.
5. Gestión de accesos: Restricción del acceso a la información y los sistemas de información únicamente a quienes tienen autorización.

6. Seguridad en recursos humanos: Asegurar que las personas empleadas, proveedores y terceros conozcan sus responsabilidades y estén adecuadamente capacitados para cumplirlas.
7. Gestión de incidentes de seguridad de la información: Preparación y respuesta ante incidentes de seguridad para minimizar los impactos.

Revisión y Actualización de los Estándares:

La Universidad se asegurará de que los estándares sean revisados y actualizados regularmente para reflejar los cambios en el entorno de seguridad, tecnología, negocio y requisitos legales y reglamentarios, garantizando así su relevancia y efectividad continua.

Capacitación y Concienciación:

La Universidad implementará programas de capacitación y concienciación, bajo la supervisión del OSI o del personal designado para asumir sus funciones, dirigidos a todos los miembros de la comunidad universitaria. Estos programas están diseñados para asegurar que las personas comprendan sus responsabilidades en relación con la protección de la información y estén equipados con el conocimiento para identificar y prevenir riesgos de seguridad. La formación incluirá aspectos fundamentales como el manejo seguro de datos personales, la identificación de intentos de phishing y buenas prácticas para la creación de contraseñas seguras, entre otros temas críticos para la seguridad de la información.

Roles y Responsabilidades:

La seguridad de la información es una responsabilidad compartida de todos quienes integran la Universidad de Aysén. A continuación, se detallan las responsabilidades específicas asignadas a distintos roles dentro de la organización:

Alta Dirección:

- Aprobar y tomar las medidas pertinentes para disponibilizar los recursos necesarios para la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI).
- Promover una cultura de seguridad de la información al interior de la Universidad.
- Promover la integración de las políticas de seguridad en los procesos organizacionales.

Oficial de Seguridad de la Información (OSI)

El/la Oficial de Seguridad de la Información (OSI) es el/la responsable principal de la coordinación estratégica del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad. Sus responsabilidades incluyen:

- La planificación y coordinación de la implementación y el mantenimiento del SGSI.
- El desarrollo y la actualización de los estándares y mecanismos de seguridad de la información.
- Coordinar la estrategia integral frente a los incidentes de seguridad de la información, estableciendo directrices y protocolos para su manejo efectivo, en alineación con las políticas generales supervisadas por el Comité de Seguridad de la Información.
- Asegurar la comunicación efectiva entre todas las partes involucradas en la gestión de un incidente.
- Facilitar el análisis posterior al incidente para identificar mejoras en las políticas y prácticas de seguridad.

Para garantizar la objetividad y la independencia en la supervisión de la seguridad de la información, el OSI actuará en una capacidad estratégica y de coordinación, mientras que la supervisión directa y el control de la implementación de políticas y procedimientos de seguridad estarán a cargo del Comité de Seguridad de la Información.

Comité de Seguridad de la Información:

El Comité de Seguridad de la Información es el órgano supervisor independiente de la implementación y el cumplimiento de las políticas y procedimientos de seguridad de la información de la Universidad. Sus funciones incluyen:

- La revisión y evaluación periódica de la efectividad del SGSI, incluidos los estándares y políticas desarrollados y coordinados por el OSI.
- La recomendación de mejoras y acciones correctivas basadas en las revisiones y auditorías del SGSI.
- La supervisión de la implementación de las recomendaciones para asegurar el cumplimiento y la mejora continua de la seguridad de la información.

Profesionales de TI:

- Responsable de la intervención directa en casos de incidentes de seguridad, bajo la coordinación del OSI. Esto incluye la identificación, contención y erradicación de amenazas, así como la recuperación de los sistemas.
- Implementar y gestionar las medidas técnicas necesarias para proteger la información y los sistemas de información, siguiendo las directrices establecidas por el OSI.
- Reportar el progreso y los resultados de la gestión de incidentes al OSI para su revisión y seguimiento.
- Participar en el desarrollo y revisión de los estándares de seguridad de la información.
- Apoyar las iniciativas de capacitación y concienciación en seguridad de la información.

Comunidad Universitaria (Estudiantes, Académicos/as, y Funcionarios/as):

- Cumplir con las políticas y estándares de seguridad de la información establecidos.
- Participar en programas de capacitación y concienciación sobre seguridad de la información.
- Reportar cualquier incidente o vulnerabilidad de seguridad de la información a los canales establecidos.

Esta estructura de roles y responsabilidades asegura que todos los miembros de la Universidad de Aysén estén involucrados y sean co-responsables de la seguridad de la información, reflejando el enfoque colaborativo y multidisciplinario necesario para proteger los activos de información de la institución.

Estructura Organizativa de la Seguridad de la Información:

Para asegurar la implementación efectiva y la gestión continua de la seguridad de la información, la Universidad de Aysén establecerá un Comité de Seguridad de la Información. Este comité estará compuesto por representantes de diversas áreas críticas de la universidad, incluyendo Tecnologías de la Información (TI), administración, recursos humanos. Sus funciones incluirán:

- Supervisar la estrategia de seguridad de la información y aprobar políticas y procedimientos.
- Evaluar de manera regular los riesgos de seguridad de la información y recomendar medidas correctivas.
- Autorizar revisiones independientes de la seguridad de la información, asegurando así la mejora continua de las prácticas de seguridad.
- Revisar y actualizar periódicamente la Política General de Seguridad de la Información, para garantizar que refleje los cambios en el entorno de seguridad, los avances tecnológicos, y los nuevos requisitos legales y reglamentarios. Esta responsabilidad implica garantizar que la política se mantenga alineada con las necesidades y objetivos estratégicos de la Universidad, así como con las mejores prácticas y estándares internacionales de seguridad de la información.

Uso de Recursos de Tecnologías de Información y Comunicación (TIC)

Los miembros de la comunidad universitaria de la Universidad de Aysén y cualquier persona usuaria que utilice los recursos de TIC proporcionados por la Institución deben hacerlo en apoyo a las actividades y objetivos institucionales. El uso de estos recursos se ajustará a la legislación vigente y a las normas internas de la Universidad, quedando estrictamente prohibido cualquier uso privado y/o comercial no autorizado.

La autorización de acceso a los recursos de TIC es personal e intransferible. Cada persona usuaria es responsable de asegurar un uso adecuado de estos recursos, incluyendo el respaldo periódico de la información gestionada. Este respaldo debe realizarse preferentemente en espacios virtuales institucionales o dispositivos mantenidos por la Universidad. Además, se espera que cada persona usuaria mantenga un entorno de trabajo ordenado, tanto en su espacio físico como electrónico, y adopte todas las medidas necesarias para preservar la confidencialidad de la información a su cargo.

Prácticas Complementarias para la Seguridad de la Información en el Uso de Recursos TIC.

Además de las directrices establecidas para el uso de los recursos de Tecnologías de Información y Comunicación (TIC), es crucial enfatizar la responsabilidad individual en la protección de la información y los sistemas de la Universidad. En este sentido, se destacan las siguientes prácticas complementarias:

- Responsabilidad sobre las contraseñas: Es imperativo que cada persona usuaria genera y mantenga contraseñas seguras. Una contraseña segura combina diferentes tipos de caracteres (letras, números y símbolos) y debe tener una longitud adecuada para proteger efectivamente la información institucional. Las contraseñas deben actualizarse periódicamente y nunca deben compartirse con otras personas. La Universidad proporcionará orientaciones específicas sobre la creación y gestión de contraseñas seguras. .
- Prevención de Malware: Los usuarios pueden instalar en los computadores y dispositivos de la Universidad únicamente programas (software) que necesiten para sus funciones académicas o administrativas. Estos programas deben ser legales, ya sea con licencia pagada o gratuitos de código abierto, y deben descargarse siempre desde sitios web oficiales. Se prohíbe la instalación de programas que puedan poner en riesgo la seguridad institucional, como programas de descarga ilegal, herramientas de hackeo, o cualquier programa de origen desconocido o dudoso. Esta medida es fundamental para proteger la red de la Universidad contra virus y otras amenazas informáticas..
- Reporte Proactivo de Incidentes de Seguridad: Todo miembro de la comunidad universitaria debe reportar inmediatamente cualquier evento o sospecha que pueda afectar la seguridad de la información institucional. Los reportes deben dirigirse al Director General de Administración y Finanzas y al Oficial de Seguridad de la Información (OSI). Se considera incidente de seguridad cualquier situación que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de la información universitaria, incluyendo accesos no autorizados, pérdida de datos o funcionamiento anómalo de los sistemas...
- Uso Adecuado del Correo Electrónico: Evitar el envío de contenido sensible o confidencial sin la debida protección. Además, se prohíbe el uso del correo institucional para fines no institucionales.
- Navegación Responsable: Abstenerse de visitar sitios web con contenido inapropiado o ilegal y utilizar los recursos de Internet de manera ética y alineada con los objetivos de la Universidad.
- Prohibición de Prácticas Maliciosas: Queda estrictamente prohibido intentar hackear, alterar o comprometer la seguridad de los servicios y sistemas de la Universidad.
- Instalación de Software y Levantamiento de Servicios no autorizados: Los usuarios pueden instalar en los computadores y dispositivos de la Universidad únicamente programas (software) que necesiten para sus funciones académicas o administrativas. Estos programas deben ser legales, ya sea con licencia pagada o gratuitos de código abierto, y deben descargarse siempre desde sitios

web oficiales. Asimismo, se prohíbe la habilitación o configuración de servicios informáticos (como servidores web, servicios de almacenamiento en red, servicios de correo, o cualquier otro tipo de servicio que pueda ser utilizado por otros usuarios) sin la autorización expresa de los profesionales de TI designados por la Dirección de Administración y Finanzas. .

- Educación y Concienciación: Las personas usuarias deben participar en las iniciativas de formación y concienciación sobre seguridad de la información ofrecidas por la Universidad, para mantenerse actualizados sobre las mejores prácticas y las amenazas emergentes.

Estas medidas son esenciales para complementar el uso responsable de los recursos TIC y fortalecer la cultura de seguridad de la información dentro de la comunidad universitaria de la Universidad de Aysén.

Gestión de la Información Física y Política de Escritorios Limpios:

La Universidad de Aysén implementa una política de escritorios limpios para la gestión segura de la información física, especialmente l tratándose de la información sensible o confidencial contra accesos no autorizados, riesgos de pérdida o daño, para lo cual todo el personal deberá adoptar las siguientes medidas:

- Almacenamiento Seguro: Toda información en papel considerada sensible o confidencial debe ser almacenada de manera segura cuando no esté en uso, tales como armarios, cajones con llave o cualquier otra forma de almacenamiento seguro.
- Escritorios Limpios: Siempre que el escritorio del usuario esté desatendido, se debe asegurar que todos los documentos sensibles sean guardados adecuadamente para minimizar los riesgos de exposición accidental o intencionada a terceros no autorizados.
- Destrucción de Información: La información en papel que ya no sea necesaria y que contenga datos sensibles o confidenciales debe ser digitalizada y registrada antes de su destrucción. La destrucción debe ser aprobada por una jefatura o director responsable, y el proceso deberá ser informado al Oficial de Seguridad de la Información (OSI). Además, se dejará constancia de la fecha, el tipo de información y la persona encargada de la destrucción. La información en papel se destruirá mediante trituradoras de papel o servicios confiables para garantizar que no pueda ser recuperada ni expuesta.
- Impresión Segura: Se debe minimizar la impresión de documentos sensibles. Cuando sea necesario imprimir, se debe utilizar la funcionalidad de impresión segura y recoger los documentos inmediatamente después de la impresión para evitar que queden expuestos.
- Sensibilización y Formación: Se ofrecerán programas de formación y sensibilización sobre la importancia de la gestión segura de la información en papel y la implementación de la política de escritorios limpios, asegurando que todos los miembros de la comunidad universitaria comprendan su rol en la protección de la información.
- Tránsito seguro de documentación: Los documentos confidenciales deben ser conducidos a través de sobre cerrado o entregados personalmente a su destinatario.

La adopción de estas prácticas es esencial para garantizar un enfoque holístico hacia la seguridad de la información, abarcando tanto los aspectos digitales como físicos de nuestra operación. Cumplir con estas directrices es responsabilidad de todos los miembros de la Universidad de Aysén, contribuyendo a un entorno seguro y protegido para nuestra comunidad.

Integración de la Gestión de Riesgos en la Política General de Seguridad de la Información:

La gestión de riesgos es un componente esencial de la política general de seguridad de la información. Para garantizar su efectividad y coherencia con las operaciones diarias, la Universidad de Aysén integra la gestión de riesgos dentro de sus procesos estándar, asignando responsabilidades claras a roles específicos:

- Identificación de Riesgos: Cada dirección, departamento o unidad, será responsable de identificar riesgos potenciales en sus operaciones, con el apoyo del(la) Oficial de Seguridad de la Información (OSI), quien proporcionará las herramientas y metodologías necesarias.
- Evaluación de Riesgos: La evaluación de los riesgos identificados se realizará en colaboración con el OSI y las jefaturas de cada dirección, departamento o unidad, utilizando criterios estandarizados para determinar la probabilidad y el impacto.
- Tratamiento de Riesgos: Basado en la evaluación, se desarrollarán estrategias de tratamiento específicas, que pueden incluir la mitigación, aceptación, transferencia o evitación de riesgos. Estas estrategias serán implementadas por los departamentos correspondientes bajo la supervisión del OSI.
- Monitoreo y Revisión: El(la) OSI coordinará revisiones regulares de la gestión de riesgos para asegurar que las estrategias de tratamiento sean efectivas y para identificar nuevos riesgos. Este proceso será parte de una revisión periódica de seguridad de la información a nivel institucional.

Identificación de Activos de Información:

La Universidad de Aysén reconoce la identificación de activos de información como un paso crítico en la protección y gestión de sus recursos informativos. Esta sección establece el proceso a seguir para identificar, clasificar y asignar responsabilidades sobre los activos de información, asegurando su adecuada protección a lo largo de su ciclo de vida.

Proceso de Identificación:

1. Inventario de Activos: Los propietarios o encargados de activos, con el apoyo y supervisión del Oficial de Seguridad de la Información (OSI), realizarán un inventario de los activos de información relevantes. Este inventario incluirá datos o documentos en formatos digitales y físicos, aplicaciones, sistemas, tecnologías de la información y comunicaciones que procesan, almacenan o transmiten dicha información.
2. Clasificación de Activos: Cada activo de información será clasificado según su nivel de confidencialidad, integridad y disponibilidad, basándose en el impacto que tendría sobre las operaciones universitarias, su reputación y obligaciones legales.
3. Asignación de Propietarios: Se asignarán propietarios a los activos de información relevantes, quienes serán responsables de su adecuada gestión de seguridad. Los(as) propietarios(as) de activos serán identificados dentro del personal que tiene autoridad y responsabilidad sobre la información y su uso.

Criterios para la Identificación:

La sensibilidad y valor de la información determinarán su clasificación de seguridad.

- La importancia operativa y estratégica de la información influirá en su nivel de protección requerido.
- Los requisitos legales y reglamentarios guiarán las medidas de protección y gestión de los activos.

Revisión y Actualización:

- El inventario y la clasificación de activos se revisarán y actualizarán de manera periódica y cada vez que haya cambios importantes en la infraestructura tecnológica, para asegurar que reflejen la situación actual de la información de la Universidad...

Responsabilidades:

- Los(as) propietarios(as) de activos son responsables de implementar las políticas y controles necesarios para proteger los activos de información asignados.
- El(la) Oficial de Seguridad de la Información (OSI) supervisará el proceso de identificación de

activos y proporcionará orientación y apoyo a los propietarios de activos.

Seguridad Relativa a los Recursos Humanos:

La Universidad de Aysén reconoce la importancia crítica de integrar la seguridad de la información en todas las etapas del ciclo de vida de los recursos humanos, desde el reclutamiento hasta la finalización del empleo. Las siguientes directrices se implementarán a través de la Dirección General de Administración y Finanzas:

Antes del Empleo:

- Verificación de Antecedentes: Para posiciones que tengan acceso a información sensible, se verificará que la persona cumpla con los estándares institucionales en materia de seguridad de la información. .
- Acuerdos de Confidencialidad: Toda persona que ingrese a prestar servicios en la Universidad debe firmar acuerdos de confidencialidad que reflejen sus responsabilidades en la protección de la información.

Durante el Empleo:

- Capacitación y Concienciación: Los(as) funcionarios(as)recibirán formación regular en seguridad de la información, adaptada a sus roles específicos dentro de la organización. Esta formación será coordinada por la Dirección General de Administración y Finanzas en colaboración con los(as) profesionales de TI.Gestión de Cambios de Rol: Cualquier cambio en los roles de los(as) funcionarios(as) que afecte su acceso a la información se gestionará para asegurar que los derechos de acceso sean adecuados y actualizados.

Finalización o Cambio de Empleo:

- Procedimientos de salida: Al finalizar el empleo, se seguirán procedimientos estandarizados para revocar el acceso a la información y recuperar los activos de la organización. Esto incluye la revisión de los derechos de acceso y la recuperación de equipos y documentos.
- Transiciones de Rol: En caso de cambios de rol dentro de la organización, se revisarán y ajustarán los accesos a la información para alinearlos con las nuevas responsabilidades.
- Responsabilidades: La responsabilidad de notificar a los Profesionales TI sobre la finalización o cambio de empleo recae en la Dirección General de Administración y Finanzas. Esta colaboración garantiza que el proceso se maneje de manera oportuna y eficiente.

Responsabilidades de la Dirección de Administración y Finanzas:

- Velar por la implementación e integración de las políticas de seguridad de la información en los procesos de recursos humanos, en colaboración con el equipo de TI y el(la) Oficial de Seguridad de la Información (OSI).
- Mantener registros de capacitación, acuerdos de confidencialidad y procedimientos de seguridad aplicables a los recursos humanos.

Responsabilidad de la Secretaría General:

- Revisar y aprobar todas las cláusulas de seguridad de la información en contratos con terceros, garantizando su conformidad con la política de seguridad de la información.

Estas prácticas garantizan que la seguridad de la información se mantenga como una prioridad constante en la gestión de recursos humanos, alineando las operaciones de recursos humanos con los objetivos de seguridad de la información de la Universidad de Aysén.

Seguridad de la Información para Relaciones con Terceros:

La Universidad de Aysén reconoce la importancia crítica de la seguridad de la información no solo internamente sino también en sus interacciones con terceros, incluidos proveedores, contratistas y socios comerciales e institucionales. Para gestionar adecuadamente los riesgos de seguridad de la información asociados con terceros, se adoptarán las siguientes directrices, en estrecha colaboración entre los(as) Profesionales de Tecnologías de la Información, el(la) Oficial de Seguridad de la Información (OSI), la Dirección de Administración y Finanzas y la Secretaría General:

Antes de la Asociación:

- Evaluación de Seguridad de Terceros: Para las relaciones con terceros que involucren el acceso o uso de sistemas de información de la Universidad, se realizará una evaluación de seguridad por el equipo de Tecnologías de la Información de la Universidad, con el fin de verificar que los terceros cumplan con los estándares aplicables de seguridad de la información. Los terceros deberán alinearse con las disposiciones de nuestra Política de Seguridad en la medida en que estas les sean aplicables o pertinentes a la relación establecida.
- Acuerdos de Confidencialidad y Seguridad: Se requerirá que los terceros firmen acuerdos de confidencialidad y seguridad obligatorios, asociados a la obligación de resguardo de toda la información confidencial o sensible con ocasión del contrato o acuerdo con la Universidad a la que tengan acceso. Tratándose de los datos personales, esta obligación tendrá el carácter de indefinido.

Durante la Asociación:

- Acceso Controlado a la Información: Se garantizará que el acceso a la información por parte de terceros está controlado y limitado a lo estrictamente necesario para el cumplimiento de los objetivos del acuerdo suscrito.
- Monitoreo y Revisión: Se establecerán procedimientos para el monitoreo continuo y la revisión periódica de las prácticas de seguridad de los terceros, para asegurar el cumplimiento continuo con nuestras políticas, mecanismos y estándares.

Finalización de la Asociación:

- Procedimientos de devolución o destrucción de archivos en poder del asociado: Al concluir la asociación, el tercero deberá tomar las medidas necesarias para asegurar la devolución o destrucción segura de toda la información de la Universidad que tenga en su poder, de acuerdo con sus propios procedimientos de seguridad. Además, deberá coordinar con la Universidad la revocación de cualquier permiso de acceso a los sistemas institucionales.

Responsabilidad de la Secretaría General:

- Revisar y aprobar todas las cláusulas de seguridad de la información en contratos con terceros, garantizando su conformidad con la política de seguridad de la información.

Estas prácticas tienen como objetivo garantizar que la seguridad de la información se mantenga como una prioridad constante en todas las etapas de nuestra relación con terceros, alineando estas operaciones externas con los objetivos de seguridad de la información de la Universidad de Aysén.

Deberes y Obligaciones de Terceros:

La Universidad de Aysén establece los siguientes deberes y obligaciones fundamentales para todos los terceros (proveedores, contratistas, socios comerciales, etc.) que acceden, manejan, o procesan información en nombre de la Universidad o en contexto con servicios prestados a la misma. Estas obligaciones son esenciales para garantizar la protección de la información y los activos de información

de la Universidad:

1. Cumplimiento de Políticas y Normativas: Los terceros deben adherir a todas las políticas, normativas, mecanismos y estándares de seguridad de la información establecidos por la Universidad de Aysén, incluidos aquellos específicos a su sector o naturaleza de servicios prestados.
2. Protección de la Información: los terceros deben implementar y mantener activas medidas de seguridad adecuadas para proteger la información de la Universidad a que tengan acceso contra el acceso no autorizado, la divulgación, alteración, destrucción o uso indebido.
3. Gestión de Incidentes de Seguridad: Los terceros están obligados a reportar de manera inmediata cualquier incidente de seguridad de la información que afecte o pueda afectar a los activos de información de la Universidad de Aysén, siguiendo los procedimientos establecidos para tal fin.
4. Confidencialidad: Deben mantener la confidencialidad de la información de la Universidad, procurando que no se divulgue a terceros sin el consentimiento expreso de la Universidad, a menos que sea requerido por ley.
5. Formación y Concienciación: Los terceros deben asegurar que su personal esté adecuadamente formado y concienciado sobre las políticas de seguridad de la información de la Universidad y sobre su papel en la protección de la información.
6. Acceso y Control de Datos: El acceso a los datos e información de la Universidad debe ser limitado al mínimo necesario para la ejecución de los servicios acordados, y debe ser gestionado a través de controles de acceso adecuados.
7. Auditoría y Cumplimiento: La Universidad se reserva el derecho de auditar a los terceros o solicitar evidencia del cumplimiento de las políticas y normativas de seguridad de la información, para asegurar la adhesión a estos deberes y obligaciones.

Estas obligaciones forman la base de la responsabilidad de los terceros hacia la seguridad de la información de la Universidad de Aysén y son aplicables a la duración de su relación con la Universidad. El incumplimiento de estas obligaciones puede resultar en la revisión o término de los acuerdos contractuales y en acciones legales si corresponde.

Gestión de Incidentes de Seguridad:

La Universidad de Aysén implementará un protocolo detallado y eficaz para el manejo de incidentes de seguridad de la información, abarcando la identificación, reporte, gestión de respuesta y procesos de recuperación. Se insta a reportar los incidentes de manera inmediata utilizando los canales establecidos, dirigiéndolos al Oficial de Seguridad de la Información (OSI), quien coordina las estrategias a nivel global para enfrentar estos incidentes. La acción directa y técnica ante los incidentes recae en el equipo de Tecnologías de la Información (TI), interviniendo de manera efectiva, llevando a cabo las medidas necesarias para contener, erradicar la amenaza y recuperar la normalidad de los sistemas comprometidos. El(la) OSI, desde su posición estratégica, supervisa el proceso integral, verificando la adherencia a los protocolos y estándares, y promoviendo una comunicación fluida y efectiva entre todas las partes involucradas.

Continuidad del Negocio:

Para garantizar la continuidad de las operaciones en caso de un incidente grave de seguridad, la Universidad de Aysén desarrollará y mantendrá un plan de continuidad del negocio. Este plan identificará las funciones críticas de la universidad y establecerá procedimientos para su recuperación rápida y eficaz. Incluirá estrategias para mantener las operaciones académicas y administrativas durante y después de un incidente, minimizando el impacto en la comunidad universitaria y asegurando la pronta restauración de los servicios normales.

Revisión y Mejora Continua:

La Universidad de Aysén se compromete a revisar y actualizar regularmente la Política General de Seguridad de la Información para reflejar los cambios en el entorno de seguridad, la tecnología, las prácticas de negocio y la legislación aplicable. Este proceso incluirá evaluaciones periódicas de la eficacia de la política y las prácticas de seguridad, con el fin de identificar oportunidades de mejora y asegurar que la estrategia de seguridad se mantenga alineada con los objetivos y necesidades de la Universidad.

Revisión Independiente de la Seguridad de la Información:

Además del proceso de revisión y mejora continua interna, la Universidad de Aysén fomentará la realización de auditorías o revisiones independientes sobre el cumplimiento y la eficacia de la Política General de Seguridad de la Información, en base a las mejores prácticas y procedimientos generalmente aplicados en instituciones afines Estas revisiones podrán ser solicitadas por el Comité de Seguridad de la Información a una unidad interna especializada o a un organismo externo con pericia técnica y normativa , asegurando una evaluación objetiva del SGSI. Los hallazgos y recomendaciones de estas revisiones independientes estarán destinadas a orientar las acciones de mejora y asegurar el alineamiento con las mejores prácticas y estándares de seguridad de la información.

Difusión

La Política General de Seguridad de la Información al igual que las Políticas de Seguridad Específicas, Normas, Planes, deberán ser difundidos con el objetivo que estas sean conocidas y además implementadas por la comunidad universitaria.

Enmiendas y Actualizaciones:

La universidad se reserva el derecho de modificar o actualizar las cláusulas de seguridad de la información en los contratos, según sea necesario, para reflejar cambios en la legislación, en la política de seguridad de la información o en las prácticas operativas.

Sanciones por Incumplimientos de Seguridad de la Información:

La Universidad de Aysén adopta un enfoque serio hacia el cumplimiento de su política de seguridad de la información y los mecanismos asociados. Las violaciones a los lineamientos sobre la materia, dependiendo de su gravedad y las circunstancias, pueden resultar en una gama de sanciones disciplinarias. Estas incluyen, pero no se limitan a, advertencias escritas, restricción del acceso a recursos de Tecnologías de Información y Comunicación (TIC), capacitación obligatoria adicional en seguridad de la información, suspensión o incluso el término de la relación laboral o académica.

Las sanciones serán aplicadas de manera justa y proporcional al nivel de incumplimiento, asegurando un proceso que respete el derecho a la defensa y la posibilidad de apelación. La Universidad, dentro de sus posibilidades, velara porque todos los incidentes sean tratados con la debida diligencia, transparencia y respeto hacia los implicados, promoviendo así una cultura de seguridad de la información basada en la responsabilidad y el respeto mutuo.

Marco Normativo de Referencia:

La Política General de Seguridad de la Información incluye un marco referencial con normas y leyes claves para la gestión de seguridad de la información en la Universidad de Aysén:

- Ley N° 18.834, Estatuto Administrativo.
- Ley N° 18.575, de bases generales de la Administración del Estado.
- Ley N° 19.799: Regula los documentos electrónicos, firma electrónica y servicios de certificación de dicha firma
- Ley N° 19.628: Sobre la protección de la vida privada y el tratamiento de datos personales.

- Ley N° 21.459: Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest
- Ley N° 17.336: Protege las obras intelectuales y los derechos de autor.
- Ley N° 19.880, de bases de los procedimientos administrativos.
- Ley N° 21.180: de Transformación digital del Estado.
- DS N°83.2005, Norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos
- DS N°93/2006 Norma Técnica para Minimizar la Recepción de Mensajes Electrónicos no deseados en las Casillas Electrónicas de los Órganos de la Administración del Estado y de sus funcionarios.
- Decreto N° 273 del Ministerio del Interior y Seguridad Pública; Subsecretaría del Interior: Establece la obligación de reportar incidentes de ciberseguridad, fortaleciendo la gestión de incidentes y la respuesta a amenazas en el entorno digital.
- NCh-ISO 27001/27002: Normas para sistemas de gestión de seguridad de la información.

Glosario

1. **Confidencialidad:** Garantizar que la información es accesible sólo para aquellos autorizados a accederla.
2. **Integridad:** Mantener la exactitud y completitud de la información.
3. **Disponibilidad**: Asegurar que la información esté disponible y accesible para las personas autorizadas cuando se necesite.
4. **Gestión de Riesgos**: Proceso de identificación, evaluación y tratamiento de riesgos que podrían afectar la seguridad de la información.
5. **SGSI** (Sistema de Gestión de Seguridad de la Información): Parte del sistema de gestión general, basado en un enfoque de riesgo, diseñado para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
6. **Incidente de Seguridad**: Cualquier evento adverso o amenaza potencial que pueda comprometer la seguridad de la información.
7. **Activos de Información:** Datos, información, aplicaciones, infraestructuras, y cualquier recurso tecnológico que soporta las actividades y objetivos de la Universidad de Aysén. Estos activos son esenciales para las operaciones académicas, investigativas, y administrativas de la universidad.
8. **Tratamiento de Riesgos:** Las acciones tomadas para mitigar, transferir, aceptar o evitar riesgos identificados que afectan a los activos de información, basándose en la evaluación de su probabilidad de ocurrencia y el impacto potencial.
9. **Propietario de Activos:** La persona o departamento responsable de garantizar que los activos de información sean adecuadamente protegidos, en términos de su confidencialidad, integridad, y disponibilidad.
10. **Violación de Datos:** Un incidente de seguridad que resulta en la divulgación no autorizada o acceso a datos personales.
11. **Contrato de Trabajo:** Acuerdos legales entre la universidad y sus personas empleadas, que incluyen disposiciones específicas sobre la seguridad de la información y la protección de datos.
12. **Terceros**: Cualquier entidad externa que interactúa con la información de la universidad, incluyendo proveedores de servicios, socios comerciales, y contratistas.
13. **Malware:** Software malintencionado diseñado para causar daño a un sistema informático, robar datos, o realizar acciones no deseadas. Este término abarca una variedad de amenazas, como virus, gusanos, troyanos, y ransomware.
14. **Phishing**: Técnica de engaño utilizada por ciberdelincuentes para obtener información confidencial de forma fraudulenta, simulando ser una entidad de confianza en comunicaciones electrónicas. Se caracteriza por el envío de mensajes, típicamente correos electrónicos, que parecen provenir de fuentes legítimas, con el objetivo de engañar a las personas para que revelen datos personales, como contraseñas, números de tarjetas de crédito y otra información sensible."
15. **Software no autorizado**: Se considera software no autorizado todo programa informático que:

a) no esté relacionado con las funciones académicas o administrativas del usuario en la Universidad, b) sea de origen desconocido o descargado de fuentes no oficiales, c) no cuente con licencia válida cuando esta sea requerida, o d) pueda poner en riesgo la seguridad de la información institucional (como programas de descarga ilegal, herramientas de hackeo o programas de origen dudoso).

2. PUBLÍQUESE la presente resolución, una vez totalmente tramitada, en el sitio electrónico de la Universidad, específicamente en el banner "Actos y Resoluciones con efecto sobre terceros", a objeto de dar cumplimiento a lo previsto en el artículo 7° de la Ley N°20.285 sobre Acceso a la Información Pública y en el artículo 51 de su Reglamento.

ANÓTESE Y COMUNÍQUESE Y PUBLÍQUESE.

Ismael Alfredo Castro Vizcarra
Firmado digitalmente por Ismael Alfredo Castro Vizcarra
Fecha: 2024.12.30 12:19:42 -03'00'

ISMAEL CASTRO VIZCARRA
SECRETARIO GENERAL
UNIVERSIDAD DE AYSÉN

Juan Pablo Prieto Cox
Firmado digitalmente por Juan Pablo Prieto Cox
Fecha: 2024.12.30 12:23:34 -03'00'

JUAN PABLO PRIETO COX
ADMINISTRADOR PROVISIONAL
UNIVERSIDAD DE AYSÉN

Distribución:
Administrador Provisional
Consejo Superior
Contraloría Universitaria
Dirección General Académica
Dirección General de Administración y Finanzas
Dirección General de Vínculos
Jefatura Departamento de Ciencias de la Salud
Jefatura Departamento de Ciencias Sociales y Humanidades
Jefatura Departamento de Ciencias Naturales y Tecnología
Jefatura Carrera de Obstetricia
Jefatura Carrera de Enfermería
Jefatura Carrera de Trabajo Social
Jefatura Carrera de Psicología
Jefatura Carrera de Ingeniería Civil Industrial
Jefatura Carrera de Ingeniería Civil Informática
Jefatura Carrera de Ingeniería Forestal
Jefatura Carrera de Agronomía
Secretaría General
Archivo