UNIVERSIDAD DE TARAPACA
ARICA-CHILE

CREA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE TARAPACÁ.

DECRETO EXENTO N° 00.187/2020.

Arica, 17 de marzo de 2020.

Con esta fecha la Rectoría de la Universidad de Tarapacá, ha expedido el siguiente decreto:

VISTOS:

Lo dispuesto en el DFL N°150, de 11 de diciembre de 1981, del Ex Ministerio de Educación Pública; Resolución Nº 6, de 2019, de la Contraloría General de la República; Resolución Exenta Universitaria CONTRAL. Nº 0.01/2002, de enero 14 de 2002; Resolución Exenta Universitaria CONTRAL. N°0.01/2018, de abril 23 de 2018; Carta U.D.T., de la Universidad de Tarapacá N° 030/2020, de marzo 11 de 2020; Carta D.A.L. de la Universidad de Tarapacá N° 178/2020, de marzo 13 de 2020; Carta VRD, de la Universidad de Tarapacá N° 029/2020, de marzo 17 de 2020; Carta de Rectoría N° 558/2020, de marzo 17 de 2020; los antecedentes adjuntos, y las facultades que me confiere el Decreto TRA Nº335/129/2018, de julio 25 de 2018.

CONSIDERANDO:

Lo dispuesto en la norma ISO 27001 y 27002 sobre el tema de seguridad de la Información de la institución y sus funciones, se requiere creación de un documento denominado "Política General de la Información de la Universidad de Tarapacá", el cual informará sobre la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información, estrategias y soluciones específicas para la implementación de los controles necesarios para materializar las políticas de seguridad establecidas y soluciones ante las situaciones de riesgo detectadas.

El mérito a lo solicitado por la Sra. Bernardina Cisternas Arapio, Directora de Planificación y Proyectos, en Traslado DIPLAN N°005/2020, de fecha 13 de marzo de 2020.

El visto bueno de la Sra. Gladys Acuña Rosales, Directora de Asuntos Legales, en carta D.A.L N°178/2020, de fecha 13 de marzo de 2020.

DECRETO:

1. Apruébese la creación del documento ***Política General de Seguridad de la información de la Universidad de Tarapacá,*** compuesto por las siguientes materias:

- Introducción.
- Declaración Institucional.
- Objetivo de la Política y Sistema de Seguridad de la Información.
- Alcance de la Política General de Seguridad de la Información.
- Revisión de la Política General de Seguridad de la Información.
- Roles y Responsabilidades.
- Dominios y Responsables.
- Definiciones y Normativa Vigente.
- Monitoreo y Revisión.
- Mecanismo de Difusión de la Política.
- Anexo 1: Implementación de Política de Seguridad de la Información.
- Políticas de Control de Acceso a la Información.

2. Publíquese, en el sistema informático conforme lo señalado en el art. 7 de la Ley N°20285 de 2008, del Ministerio Secretaria General de la Presidencia, sobre Acceso a la Información pública.

Anótese, y remítase a la Contraloría de la Universidad, para su control y registro. Comuníquese una vez tramitado totalmente el acto.

PAULA LEPE CAICONTE
Secretaria de la Universidad

SECRETARIA DE LA UNIVERSIDAD ARICA

UNIVERSIDAD DE TARAPACÁ CONTRALOR ARICA

ALFONSO DÍAZ AGUAD
Rector (S)

UNIVERSIDAD DE TARAPACÁ RECTOR ARICA

ADA.PLC.amr.

18 MAR 2020

Universidad de Tarapacá

Política General de Seguridad de la Información Universidad de Tarapacá

ENERO 2020

Dirección de Planificación y Proyectos
General Velásquez 1775 Arica - Chile
Teléfono: 56-58205308
E-mail: diplan@uta.cl

POLITICA GENERAL
DE SEGURIDAD DE LA INFORMACION
UNIVERSIDAD DE TARAPACÁ

1. Introducción

Los datos y la información, como otros activos de la Universidad de Tarapacá, pues son esenciales para la operación y continuidad de los servicios y requiere en consecuencia una protección adecuada, lo cual es especialmente importante en ambientes de negocio cada vez más interconectados.

Como consecuencia de esta creciente interconectividad, la información está ahora expuesta a un número mayor, y variado de amenazas y vulnerabilidades. La información adopta diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en películas o grabada. Cualquiera sea la forma que tome la información o los medios por los que se comparta o almacene, la misma debería ser siempre protegida adecuadamente.

La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños al negocio y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles deberían ser establecidos, implementados, supervisados, revisados y mejorados cuando fuere necesario para asegurar que se cumplen los objetivos específicos de seguridad de la organización.

En este contexto, se vuelve necesario definir lineamientos claros en materia de seguridad de la información de acuerdo al marco normativo vigente, a saber:

- Ley 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Decreto Supremo 83: Norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Norma Chilena Oficial NCh-ISO 27002.0f2009, cuya norma indicada está basada en la norma internacional ISO/IEC 27002:2005.
- Ley 19.223: Ley de delitos informáticos
- Ley 19.628: Ley de protección de la vida privada
- Ley 19.927: Sobre delitos de pornografía infantil
- Ley 17.336: Ley de propiedad intelectual
- Ley 18.620: Código del Trabajo

2. Declaración Institucional

La seguridad de la información es de responsabilidad de todos los organismos de la Universidad, por lo cual es necesaria integrar a todas las unidades administrativas y académicas para garantizar el apoyo manifiesto de las autoridades a las iniciativas tecnológicas y de seguridad.

Dicho apoyo permitirá promover e impulsar la implementación de la presente política, la cual estará siempre alineada con la misión y la visión de la Universidad de Tarapacá.

La Universidad de Tarapacá facilitará las herramientas, acceso a servicios y condiciones que permitan ejecutar la labor propia de cada miembro de la comunidad universitaria.

UNIVERSIDAD DE TARAPACA
SECRETARIA DE LA UNIVERSIDAD
ARICA

Dichos servicios deben ser utilizados en materias relacionadas directamente con la respectiva función de cada miembro de la comunidad universitaria o con el quehacer propio de la Universidad de Tarapacá.

En este sentido, se establece que los usuarios no podrán hacer uso de los sistemas o herramientas para propósitos personales de carácter comercial, con fines políticos u otro que no tenga relación con el ámbito universitario.

Cada miembro de la comunidad universitaria, tiene la responsabilidad de proteger la información confidencial de la universidad. El uso inapropiado de la información confidencial, expone a la Universidad de Tarapacá a riesgos de seguridad como filtración de información sensible, suplantación de identidad, accesibilidad a los servicios, litigios por aspectos legales, entre otros.

3. Objetivos de la Política y Sistema de Seguridad de la Información

- Realizar un catastro de activos de información, definiendo los procesos propios de cada facultad/organismo que estén involucrados con estos activos.

- Analizar los riesgos que permitan diseñar y establecer medidas que los disminuyan y que estén de acuerdo a la normativa vigente.

- Capacitar a toda la comunidad universitaria, sobre su responsabilidad en el cumplimiento de los objetivos establecidos en esta Política de Seguridad de la Información y su alcance, así como la incorporación progresiva de buenas prácticas laborales relacionadas con estos.

- Establecer los lineamientos para el marco de la elaboración de políticas, instructivos, estándares y procedimientos en materia de seguridad de la información a ser desarrollados en la Universidad de Tarapacá.

- Realizar evaluaciones y seguimientos permanentes de los eventos que generen impacto en los ámbitos de la seguridad de la información, como también analizar y aplicar las oportunidades de mejora que sean identificadas.

- Establecer los medios y oportunidades de difusión y comunicación de esta política y sus objetivos a todos los niveles de la universidad, los cuales permitan promover el cumplimiento de normas y procedimientos de seguridad.

SECRETARIA DE LA UNIVERSIDAD

4. Alcance de la Política General de Seguridad de la Información

La presente política de seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el fin de apoyar eficazmente la gestión de seguridad de la información en los sistemas informáticos y recursos tecnológicos de la Universidad.

Los ámbitos a desarrollar en materia de seguridad de la información, se abordarán en lo relacionado a la definición de documento electrónico y a los sistemas de información vigentes.

Además se deberán elaborar los documentos necesarios para su correcta implementación, considerando al menos los siguientes:

- Política Seguridad Física
- Política de Control de Acceso a la información (cuentas de usuarios, contraseñas, firmas electrónicas, etc.)
- Política de uso de Datos en la Red (Wifi, VPN, Servidor Seguro, transacciones seguras, etc.)
- Política de respaldos.(A nivel de servidores, usuarios, y documentos críticos)
- Política de uso de Correo Electrónico
- Política de uso y desarrollo de software.

Sin embargo, la Política de Seguridad de la Información deberá contener los siguientes ámbitos:

- Seguridad Física y del Ambiente
- Seguridad ligada a los Recursos Humanos
- Seguridad de las Comunicaciones
- Seguridad en Control de Acceso
- Seguridad de las Operaciones
- Adquisición, Desarrollo y mantenimiento del sistema
- Administración de Activos

5. Revisión de la Política General de Seguridad de la Información

La presente política deberá ser revisada y actualizada de forma periódica y no podrá exceder de los 3 años como máximo, para asegurar su conveniencia, suficiencia y eficacia continua.

SECRETARIA DE LA UNIVERSIDAD

6. Roles y Responsables

Responsable	Rol	Funciones
Director/a Planificación y Proyectos	Liderar la definición de implementación de la Política de Seguridad de la Información	1. Generación de lineamientos y criterios generales. 2. Aprobación de políticas institucionales de seguridad de la información. 3. Evaluar el funcionamiento y efectividad del Sistema de Seguridad de la Información a intervalos planificados. 4. Proveer las instancias para la obtención de recursos según las necesidades para la Gestión de Seguridad de la Información. 5. Proponer al **Oficial de Seguridad de la Información.**
Comité de Seguridad de la Información	Coordinar los avances en la implementación y funcionamiento de la Política y sus procedimientos.	1. Asesorar al Director de Planificación y Proyectos en materias relativas a la seguridad de los activos de información. 2. Supervisar el estado de la implementación de la política de seguridad de la información. 3. Proponer y elaborar las políticas de seguridad, efectuar los controles necesarios y velar por su correcta implementación y aplicación. 4. Coordinar la respuesta a incidentes de seguridad de la información y riesgos vinculados a los activos de la información. 5. Coordinarse con otras instituciones, a fin de mantenerse al tanto de nuevas normativas o estándares a aplicar en términos de seguridad. 6. Asesorar en materias de seguridad de la información, normativa y plan de tratamiento de riesgos.
Oficial de Seguridad de la Información	Responsable de cautelas un adecuado resguardo y protección de los activos de información en la institución.	1. Diseñar e implementar políticas, normas y procedimientos de seguridad de la información. 2. Asegurar la continuidad operacional, coordinar y monitorear la implementación de la continuidad operacional e interactuar con organismos externos.

SECRETARIA DE LA UNIVERSIDAD

		3. Asesorar en forma permanente y cercana a las distintas áreas de la Institución en temas referentes a seguridad y conducir al correcto cumplimiento de los estándares de seguridad definidos. 4. Coordinar la respuesta a incidentes que afecten a los activos de información institucionales. 5. Preparar instrucciones para la seguridad de los activos de información, respecto al uso seguro del correo electrónico, la asignación de identificadores, uso de redes y servicios de red. 6. Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad.

7. Dominios y Responsables.

Nombre del Dominio	Responsable
Políticas y Organización de Seguridad de la Información	Director/a Planificación y Proyectos
Seguridad Física y del Ambiente	Director/a de Logística y Operaciones
Seguridad ligada a los Recursos Humanos	Director/a de gestión de Personas
Seguridad de las Comunicaciones	Director/a de Extensión Director/a de Logística y Operaciones Encargado/a Unidad de Desarrollo Tecnológico
Seguridad en Control de Acceso	Director/a de Logística y Operaciones Encargado/a Unidad de Desarrollo Tecnológico
Seguridad de las Operaciones	Director/a de Logística y Operaciones Encargado/a Unidad de Desarrollo Tecnológico
Adquisición, Desarrollo y mantenimiento del sistema	Encargado/a Unidad de Desarrollo Tecnológico
Administración de Activos	Director/a Administración y Finanzas
Gestión de incidentes de Seguridad de la Información	Oficial de Seguridad de la Información
Aspectos de Seguridad de la Información en la continuidad del negocio	Oficial de Seguridad de la Información
Cumplimiento de la Política	Comité de seguridad de la información

8. Definiciones y Normativa Vigente.

La presente política adopta su base de contenidos, a partir de los requisitos definidos en la Norma Chilena NCh-ISO 27001 y de los requisitos legales, normativos y contractuales relativos a la seguridad de la información, que sean aplicables al Servicio, como el Decreto Supremo Nro. 83/2004 del Ministerio Secretaría General de la Presidencia, que aprueba la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

9. Monitoreo y Revisión.

Con el fin de asegurar su vigencia, actualización y mejora continua, la presente política será revisada cada 3 años por parte del Comité de Seguridad de la Información, proponiendo las mejoras a implementar o la modificación de esta. La revisión será formalizada mediante un acta del Comité de Seguridad de la Información en una sesión de trabajo correspondiente.

10. Mecanismos de difusión de la política.

La difusión de la presente política se realizará mediante comunicaciones internas informando, a todos los funcionarios de la institución, las políticas vigentes, y permitiendo la revisión del documento.

SECRETARIA DE LA UNIVERSIDAD

Glosario de términos

1. **Activo de información:** toda la información que tenga valor para la institución, como por ejemplo: documentos digitales y bases de datos, correo electrónico, documentación de sistemas, manuales de usuarios, procedimientos operativos o de soporte, planes de continuidad, configuración del soporte de recuperación, entre otros. Dentro de los activos de información, se puede agregar a su vez a las personas como fuentes o almacenadoras de información no documentada.

2. **Documento electrónico:** toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior. (Definición Ley 19.799)

3. **Firma electrónica**: es cualquier sonido, símbolo proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor. (Definición Ley 19.799)

4. **Decreto supremo:** es un mandato escrito que emana del Presidente de la República en uso de las facultades que ejerce en el marco de la potestad reglamentaria y puede ser modificado o dejado sin efecto mediante otro 0.5. (definición derecho administrativo).

5. **Norma:** Es un documento de conocimiento y uso público, aprobado por un organismo reconocido. La norma establece, para usos comunes y repetidos, reglas, criterios o características para las actividades o sus resultados y procura la obtención de un nivel óptimo de ordenamiento en un contexto determinado.

6. **Amenaza:** representa una fuente potencial de eventos adversos para la seguridad informática.

7. **Sistema de información:** es un conjunto organizado de elementos, que pueden ser personas, datos, actividades o recursos materiales en general. Estos elementos interactúan entre sí para procesar información y distribuirla de manera adecuada en función de los objetivos de una organización.

8. **Riesgo:** amenaza de impactar y vulnerar la seguridad del documento electrónico y su posibilidad de ocurrencia (definición D.S.N"83).

9. **Proceso:** es un conjunto de actividades o eventos coordinados que se realizan bajo ciertas circunstancias con un fin determinado.

10. **Procedimiento:** es el modo de ejecutar determinadas acciones que suelen realizarse de la misma forma, con una serie común de pasos claramente definidos.

11. **Incidente de seguridad informática:** se define como un evento que atente contra la confidencialidad, integridad y disponibilidad de un documento electrónico o sistema computacional o asimismo el acto de violar explícita o implícitamente una política de seguridad.

SECRETARIA DE LA UNIVERSIDAD

FRR

ANEXO 1

IMPLEMENTACION
DE POLITICA DE SEGURIDAD DE LA INFORMACION

1. POLITICAS DE SEGURIDAD FISICA

1.1. Se debe habilitar un lugar donde se localicen e instalen los servidores institucionales de información y servicios. Este lugar debe contar con una instalación eléctrica adecuada y respaldada redundantemente. Entre sus características debe contar con tierra física y sistemas de alimentación ininterrumpida o de emergencia, UPS (Uninterruptible Power Supply), y un generador adicional para asegurar continuidad de operaciones.

1.2. Mantener los servidores principales de la Institución alejado de cualquier tipo de agente que pueda causar algún daño o interfiera con su rendimiento como son: fuego, humo, polvo, temperaturas extremas, rayos solares, vibraciones, insectos, ruido eléctrico, equipo industrial, agua, etc.

1.3. Todos los servidores deberán ubicarse en lugares de acceso físico restringido y deben tener para acceder a ellos puertas con cerraduras.

1.4. El área donde se encuentren los servidores deberá cumplir con los estándares de cableado estructurado. Se debe conservar limpio, organizado, y despejado de objetos extraños o ajenos para el uso al cual está destinada.

1.5. Debe contarse con extintores en las salas de cómputo acorde al tipo de fuego que pudiera aparecer y el personal debe estar capacitado en el uso de éstos.

1.6. El lugar donde se encuentren los equipos de cómputo deben contar con la temperatura apropiada (18ºC a 21ºC) y humedad adecuadas para evitar deterioro o mal funcionamiento de los equipos de cómputo.

1.7. Debe existir los controles necesarios para autorizar o no el acceso a las personas, cualesquiera que fuera su actividad o rol.

1.8. Se prohíbe el acceso a las salas de cómputo con cualquier tipo de alimento o bebida.

SECRETARIA DE LA UNIVERSIDAD

2. POLITICAS DE CONTROL DE ACCESO A LA INFORMACION.

2.1. Todo funcionario perteneciente a la Universidad de Tarapacá (U.T.A.), incluidos terceros, deberán tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la organización. El otorgamiento de privilegios y acceso a los activos de información deber están basados en las necesidades de las áreas y aprobadas por los propietarios o custodios de los activos.

2.2. Las necesidades de acceso deberán ser determinadas por las respectivas jefaturas, en función de las tareas asignadas al cargo del funcionario.

2.3. Para todo medio de procesamiento de información al que se necesite conceder accesos (Bases de datos y aplicaciones), el propietario de la información en conjunto con el Área de Desarrollo Tecnológico de la Unidad de Desarrollo Tecnológico (U.D.T.), designará un responsable quien concederá los permisos de acceso respectivos.

2.4. Los accesos a terceros deberán realizarse mediante un acuerdo firmado, con periodo de uso con fecha de expiración y tomando compromiso respecto de la confidencialidad de los datos y accesos concedidos.

2.5. La Unidad de Desarrollo Tecnológico estará siempre facultada para suspender cualquier acceso concedido frente a cualquier sospecha de uso sospechoso o riesgo de pérdida de confidencialidad, integridad o disponibilidad de la información.

2.6. Cualquier intento de acceso no autorizado será considerado un incidente grave, por lo que será reportado y se tomarán las acciones respectivas.

2.7. La administración de perfiles de usuario en las aplicaciones será responsabilidad de los usuarios administradores de cada aplicación y las unidades correspondientes.

2.8. No se otorgará acceso a ningún sistema para usuarios que no hayan completado el proceso de autorización y registro correspondiente.

2.9. Para facilitar la administración de los accesos, se definirán perfiles de acceso asignables a grupos de usuarios que, por sus responsabilidades en la organización, presenten necesidades de acceso equivalentes.

2.10. La Unidad de Desarrollo Tecnológico implementara las reglas de control de acceso solicitadas por los administradores de aplicación y las unidades correspondientes.

2.11. El otorgamiento de accesos especiales a funcionarios que no pertenecen a la U.D.T., deberán ser solicitados a la jefatura de ésta, justificando claramente la necesidad y tiempo que se requiere mediante un documento formal.

2.12. Los derechos de acceso deben ser asignados a perfiles individuales, de forma tal que las acciones que se realicen sean de responsabilidad directa del funcionario.

2.13. El otorgamiento de accesos respecto a recursos de información deberá considerar sólo la etapa en la que interviene el funcionario, de modo de que un mismo funcionario (no administrador) pueda disponer por voluntad propia, del control total de un proceso de negocio.

2.14. La Unidad de Desarrollo Tecnológico, es responsable de los accesos de los administradores de aplicaciones, de tal forma que se establezca un control desde el registro inicial de la cuenta hasta que requiera ser modificada, revocada o eliminada.

2.15. Los derechos de acceso deben ser revisados:

- En intervalos no mayores a 180 días.
- Después de cualquier cambio mayor en la organización.
- Los accesos de cuentas con mayores privilegios serán revisadas al menos 3 veces al año.

2.16. La Unidad de Recursos Humanos deberá ser responsable de abordar situaciones de cambio de cargo de funcionarios, y dar aviso para revisar permisos de acceso lógico asignados y verificar que éstos sigan siendo válidos de acuerdo a su nueva función.

2.17. La unidad de Recursos Humanos, deberá informar cuando un funcionario cesa su relación laboral con la Universidad de Tarapacá, de manera que todos los permisos y accesos deberán ser revocados. En el caso que otro funcionario ocupe su lugar, deberá crearse los accesos correspondientes con identidad nueva y a partir de la fecha en que asume el nuevo rol. Es válido enfatizar que la Unidad de Desarrollo Tecnológico deberá quedar libre de culpa ante situaciones no informadas.

2.18. Los usuarios administradores de aplicaciones deberán revisar en forma periódica los perfiles de usuarios vigentes y solicitar a la U.D.T., cualquier cambio que sea necesario para la realización correcta de sus labora; ya se ampliando o reduciendo el límite de sus privilegios en los respectivos sistemas.

SECRETARIA DE LA UNIVERSIDAD

3. POLITICAS DE USO DE RED DE DATOS

3.1 Todo usuario que esté utilizando la infraestructura de la Universidad de Tarapacá (UTA), incluidos terceros, tendrá acceso de Servicios de Internet e Intranet. Tales accesos, se conceden con el principal objetivo de entregar un servicio para el desarrollo de las actividades académicas, como así la investigación y desarrollo de las actividades curriculares.

3.2 En consideración que se provee acceso de Servicio de Internet e Intranet a toda la Comunidad Universitaria, se han definido 4 Estamentos a los cuales se les hace entrega de los Recursos Informáticos.

- 3.2.1 Estamento de Académicos.
- 3.2.2 Estamento de Funcionarios.
- 3.2.3 Estamento de Alumnos.
- 3.2.4 Estamento de Visitas.

3.3 Para cada Estamento, la U.D.T., ha definido de acuerdo a la criticidad y acceso a los recursos tecnológicos, distintos privilegios; el Acceso al Servicio Internet se proveerá conforme a la definición del perfil o credencial de acceso (estamento), y sea propio de las actividades curriculares de la comunidad universitaria, sin que cauce perjuicio o daños al normal funcionamiento de la Red UTANET.

3.4 La Unidad de Desarrollo Tecnológico, tiene la administración para realizar labores de implementación de segmentos de red en los Estamentos definidos, del mismo modo tiene las atribuciones de regular el Ancho de Banda administrado para cada estamento.

3.5 Los Estamentos Académicos, Funcionarios, Alumnos y Visitas, tienen privilegios de acceder a los Recursos Informáticos de Intranet en marco a las labores que están definidos sus perfiles o credenciales.

3.6 Para el acceso al Servicio de Internet, las directrices que se utilizan para el acceso y uso del Servicio de Datos, estará normado por la categorización que tiene la credencial o perfil de acceso.

3.7 La Unidad de Desarrollo Tecnológico de acuerdo a los cambios y tendencias de la tecnología, puede implementar nuevas políticas de seguridad que sirvan para robustecer las Políticas de Uso de Datos existentes.

3.8 La Unidad de Desarrollo Tecnológico es responsable de administrar el correcto uso del Ancho de Banda que se le entrega a cada estamento de la Comunidad Universitaria.

3.9 Se establece la administración del Ancho de Banda para los Servicios de Acceso a Internet denominados de uso "masivo" o recurrente a través de la Infraestructura que está implementada en Red UTANET.

3.10 En el caso de los Servicios de Streaming o de Video Conferencia, el Ancho de Banda será definido una vez que unidad solicitante entregue los datos técnicos necesarios para llevar a cabo el servicio.

3.11 La Unidad de Desarrollo Tecnológico está facultada para interrumpir el Servicio de Datos entregado, una vez que se detecte actividad por Ej. Descarga de software Peer-to Peer o Contenido con Protección de Derechos de Autor (COPYRIGHT) que pudiera representar un incremento en el Tráfico excesivo del Ancho de Banda.

3.12 La Comunidad Universitaria tiene Servicio Inalámbrico implementado en todas las Dependencias de la Universidad de Tarapacá. De acuerdo a los métodos de acceso implementados para el Servicio Inalámbrico, se tiene la estructura de 4 Estamentos para el acceso de los diferentes recursos informáticos. Se definen los principales métodos de acceso al Servicio Inalámbrico, mediante Portales Cautivos (Credenciales de Acceso Perfil de Usuario y Sistema antiguo de acceso mediante clave única para Dispositivo Inalámbrico.

SECRETARIA DE LA UNIVERSIDAD

3.13 La Unidad de Desarrollo Tecnológico está facultada para cortar el Servicio entregado, una vez que se detecte actividad sospechosa de distribución de Material Protegido o actividades que sean sancionables de acuerdo a la "Política General de Seguridad (Sanciones)".

3.14 Para tener acceso mediante Servicio Virtual Private Network (VPN), el director del área o supervisor inmediato es responsable de solicitar la credencial de acceso para un determinado usuario.

3.15 Este Servicio será concedido siempre y cuando se especifique en Formulario los Datos solicitados, así como también el motivo del cual se requiere el Servicio.

3.16 La UDT tiene la atribución de deshabilitar la credencial, una vez que tenga antecedentes que se están realizando actividades fuera de las atribuciones entregadas o que sean sancionables de acuerdo a la "Política General de Seguridad (Sanciones)".

4 POLITICAS DE RESPALDOS

4.1 Esta política se aplica a toda información contenida en servidores, estaciones de trabajo y equipos de comunicaciones, que contengan datos, configuración y aplicaciones. Es aplicable a todos los usuarios, sin importar su estamento ni función que desempeñe hacia la Universidad de Tarapacá.

4.2 Toda información NO relevante para el quehacer de la institución y que resida en cualquier equipo, no será respaldada. La utilidad de la información en equipos centrales será determinada por la Unidad de Desarrollo Tecnológico y en equipos de escritorio por el Área de Soporte TIC's ULOO.

4.3 Todo respaldo manual o automático, deberá ser registrado. En el caso de que la información a respaldar sea confidencialidad, se deberá considerar realizar el proceso de cifrado sobre el respaldo.

4.4 Identificación de información crítica: La U.D.T., con conocimiento en los procesos de negocio que realiza la U.T.A., determinará qué información es importante a considerar en los respectivos respaldos y recuperación en casos de daño o pérdida de información.

4.5 Frecuencia y tipo de respaldo: La U.D.T., definirá los procesos y tipos de respaldos, así como la frecuencia, medios de almacenamiento, tiempo de conservación y borrado de la misma. La periodicidad con que se realicen respaldos a los equipos de escritorio, asignados a usuarios, no podrá ser bajo ninguna circunstancia superior a 1 año laboral. La periodicidad y tipo de respaldo con que se realicen respaldos a los sistemas y aplicaciones informáticas institucionales será en función de la periodicidad de cambios que éstas tengan.

4.6 Protección de los medios de respaldo: Las configuraciones de respaldo para los sistemas informáticos deberán ser probados con regularidad, a los más una vez cada dos años y ante un cambio de tecnología en los medios, que pueda generar obsolescencia, deberá generarse las acciones necesarias para el resguardo de los respaldos existentes.

4.7 Protección de la información en medios de respaldo: Para prevenir pérdidas accidentales, se deben respaldar todos los archivos, bases de datos e información existente en los Sistemas relevantes para la Institución, a su vez, disponer de la infraestructura adecuada de respaldo para cada caso, y asegurar su disponibilidad en caso de desastres o falla de un dispositivo. Toda información crítica (para asegurar la continuidad de las operaciones), deberá ser respaldada y almacenada en una ubicación remota, esta instalación deberá estar emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal. Dicho respaldo debe tener registros exactos y completos de las copias y procedimientos documentados de restablecimiento. En ámbitos críticos para la institución, se deberán almacenar al menos tres generaciones o ciclos de información de respaldo.

4.8 El respaldo de datos y software críticos se deben almacenar en un lugar protegido, con acceso controlado.

4.9 Toda información crítica grabada en respaldos que son almacenados fuera de la Institución, debe ser trasladada con los elementos de seguridad adecuados, ya sea utilizando métodos de encriptación o utilizar métodos apropiados para prevenir intentos de acceso físico no autorizado.

4.10 Periodo de existencia de las Copias de Respaldo. La U.D.T., determinará el período de retención de la información esencial para la institución, considerando cualquier tipo de requisito para archivar copias que se deberían retener de manera permanente. Lo anterior, de acuerdo con el ordenamiento jurídico vigente y el uso eficiente del espacio físico disponible para el almacenamiento. Se deberá establecer el período de existencia para las copias de seguridad y los procedimientos a seguir para su destrucción definitiva una vez concluido tal periodo.

FRR

SECRETARIA DE LA UNIVERSIDAD

4.11 Vigencia y retención de los respaldos. Cuando la información de la U.T.A. deje de ser necesaria o válida, deberá ser destruida o eliminada de manera segura.

4.12 Respaldo de estaciones de trabajo. Los responsables de las unidades y departamentos de la U.T.A., deberán asegurarse de que la información de los funcionarios a su cargo se salvaguarde de manera satisfactoria.

4.13 Borrado de información. La información contenida en servidores centrales de la institución, que no sea necesaria o haya sido alojada sin previo aviso, será borrada. Todo equipo computacional, mayor o de escritorio que sea dado de baja, debe ser examinado por el Área de Soporte TIC's ULOO para comprobar la eliminación definitiva de la información. Todo medio de respaldo obsoleto que sea destruido, deberá ser de forma tal que garantice ninguna posibilidad de acceder a los datos contenidos.

4.14 Pruebas de realización y restauración de las Copias de Respaldo. La realización de las pruebas de restauración de las copias de respaldo confirmará el funcionamiento correcto del proceso de recuperación de copias de datos, y garantizará la integridad de los datos que contienen. Por lo que se deberán realizar pruebas respecto a la restauración de las copias de respaldo, de forma rotativa y con una periodicidad con una regularidad, a lo menos cada 2 años.

4.15 Comprobación periódica de los procedimientos de restauración. Para garantizar la eficacia de los procedimientos de restauración y la capacidad para recuperar activos desde las copias de respaldo, se establecerá el procedimiento de comprobación periódica que se detalla a continuación:

5 POLÍTICAS DE CORREO ELECTRÓNICO

5.1 El personal académico y administrativo tienen la facultad de solicitar una cuenta de correo al responsable de cómputo de su área, para el uso diario de sus actividades laborales.

5.2 Queda prohibido utilizar el correo electrónico para propósitos ajenos a la dependencia.

5.3 El usuario es la única persona autorizada para administrar su propio buzón.

5.4 Cuando la cuenta se ve involucrada en algún incidente de seguridad, el administrador podrá auditar dicha cuenta, previo aviso al responsable del área.

5.5 Los usuarios de los sistemas de correo electrónico deben ser conscientes de la información que se envía o se recibe, probablemente no esté cifrada y no debe ser considerada como confidencial o inalterable. Los correos que no estén cifrados no podrán ser utilizados para la transmisión de información personal o sensible.

5.6 Los mensajes con información considerada sensible, deben ser aprobados por las autoridades de su División, Secretaría o Coordinación, antes de su distribución y al enviarlos se debe de tomar las medidas pertinentes para su aseguramiento.

5.7 Anti-malware de detección y cuarentena deberán ser instalados en todos los servidores de correo electrónico. Estas herramientas deben estar actualizadas.

5.8 Cualquier acceso por medios ilegales a cuentas ajenas será considerado un ataque al servidor de correo y a la privacidad de los usuarios, por lo que el causante será sancionado.

SECRETARIA DE LA UNIVERSIDAD

6 POLÍTICAS DE DESARROLLO DE SOFTWARE Y USO DE SOFTWARE GENUINO

6.1 El desarrollo de sistemas, herramientas y software en general cuyo propósito sea el de apoyar, facilitar y agilizar las actividades académicas, de investigación o de docencia, así como los distintos proyectos en colaboración con alguna otra organización interna o externa, en caso que éstos no existan de manera particular para alguna tecnología, se debe de seguir las metodologías internas en cada dependencia considerando la compatibilidad entre sistemas.

6.2 Es necesario el desarrollo de documentación que permita dar seguimiento a las aplicaciones de software durante todo su ciclo de vida, siguiendo la metodología que la dependencia considere adecuada para dicho fin.

6.3 La elección de la tecnología de desarrollo y bases de datos debe ser realizada en referencia a la compatibilidad con los demás sistemas con los que la aplicación pueda interactuar.

6.4 Los desarrollos deben de incluir bitácoras de uso, nativas a la aplicación e independientes a las de la plataforma de software donde resida.

6.5 Previa a la liberación de los sistemas de información debe de realizarse un análisis de seguridad en un ambiente de pruebas, corrigiendo la totalidad de los fallos que sean detectados.

6.6 No estará permitido el uso de software comercial sin contar con la licencia respectiva de uso.

SECRETARIA DE LA UNIVERSIDAD

DIRECCIÓN DE ASUNTOS LEGALES FRR BYR