Política de seguridad de la información de la Universidad Tecnológica Nacional

Introducción

El conocimiento es el activo más importante de la Universidad Tecnológica Nacional (UTN). Estos conocimientos se adquieren gracias al análisis y el proceso de los datos e información que se generan en archivos digitales o papeles, con el fin de dar cumplimiento a la misión estratégica. En el contexto de transformación digital en el que se encuentra avanzando la UTN, se hace indispensable para su organización tener un control sobre sus archivos, manteniendo y asegurando su integridad, confidencialidad y disponibilidad de la información.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. También se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por fallos técnicos o, porque no, por catástrofes naturales.

Es por ello que esta política establece un marco organizativo y operacional para fortalecer la seguridad de los sistemas, los datos y los servicios prestados por la UTN, alineada a la DA 641/21 de la Jefatura de Gabinete de Ministros “Requisitos mínimos de Seguridad de la Información para Organismos”, que apunta a **promover una política pública que enmarque una conducta responsable en materia de seguridad de la información** en los organismos estatales, sus agentes y funcionarios.

Los agentes públicos de la Universidad, cualquiera sea el nivel jerárquico y la modalidad de vinculación, tienen la obligación de dar tratamiento y hacer un uso responsable, seguro y cuidado de los datos que utilizan en sus labores habituales, adoptando todas las medidas a su alcance para protegerlos.

La UTN debe estar preparada para prevenir, detectar, responder y recuperarse de incidentes de seguridad que puedan afectar sus activos de información.

Prevención

La Universidad debe prever y mitigar todos los riesgos para evitar que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad propuestas para los organismos nacionales, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estas medidas, los roles y las responsabilidades de seguridad de la información de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de esta Política, la UTN debe:

- Establecer los mecanismos para autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.
- Realizar continuas campañas de concientización a los miembros de la comunidad universitaria.

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

La UTN debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la Universidad.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias Informáticas o CERT (Computer Emergency Response Team) reconocidos a nivel nacional e internacional.

Recuperación

Para garantizar la disponibilidad de los servicios críticos, la UTN debe desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

A partir de lo expuesto hasta aquí se propone el siguiente modelo de Política de Seguridad de la Información para la Universidad Tecnológica Nacional, que será adoptado por todas las sedes que la integran y los procedimientos serán adaptados a las necesidades y realidades particulares de cada una.

ÍNDICE

1. Misión

Según Artículo 2° del Anexo I, del Estatuto Universitario, aprobado según Resolución de la Asamblea Universitaria N°1/2011, con fecha 14 de septiembre de 2011, aprueba que es Misión de la Universidad Tecnológica Nacional: **crear, preservar y transmitir los productos de los campos científica, tecnológico y cultual para la formación plena del hombre como sujeto destinatario de esa cultura y de la técnica, extendiendo su accionar a la comunidad para contribuir a su desarrollo y transformación.**

2. Objetivo y Alcance

Establecer lineamientos generales y mínimos, con el fin de proteger los activos de información, frente a riesgos internos o externos, que pudieran afectarlos, para así preservar su confidencialidad, integridad y disponibilidad.

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la UTN.

Debe ser informada, conocida y cumplida por todos los miembros de la comunidad educativa, tanto se trate de personal no docente, estudiantes, docentes, técnicos, graduados y funcionarios políticos sea cual fuere su nivel jerárquico y su situación de revista; y terceros vinculados a la misma.

3. Marco Normativo

Son de aplicación las leyes y normativas nacionales, provinciales y municipales en relación con seguridad de la información, protección de datos personales, propiedad intelectual y uso de herramientas de comunicaciones informáticas[1].

Leyes relacionadas a la ciberseguridad

- Ley 26.388 de Delito informático
- Ley 25.326 de Protección de Datos Personales
- Decreto Reglamentario N° 1558/2001
- Ley 25.506 de Firma Digital
- Decreto Reglamentario N° 2628/2002
- Ley 26.904 de Grooming

[1] https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa

Normativas vinculadas a las funciones de la Dirección Nacional de Ciberseguridad

- Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.
- Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información.
- Resolución 1523/2019. Definición de Infraestructuras Críticas.

Otras normativas relacionadas a la ciberseguridad

- Decreto 577/2017. Creación del Comité de Ciberseguridad.
- Decreto 480/2019. Modificación del Decreto 577/2017.
- Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.
- Resolución 141/2019. Presidencia del Comité de Ciberseguridad.
- Disposición 8/2021 Guía introductoria para la Seguridad para el Desarrollo de Aplicaciones WEB
- Resolución 87/2022 SIGEN: Normas de Control Interno para Tecnología de la Información - Sector Público Nacional

4. Organización de la seguridad de la información

Para administrar la seguridad de la información dentro de la UTN y establecer un marco gerencial para iniciar y controlar su implementación, se requiere definir roles y distribuir funciones y responsabilidades.

4.1 Roles, funciones y responsabilidades de seguridad

Propietario de la Información

El Propietario de la Información de la UTN tendrá las siguientes funciones:

- Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma,
- Documentar y mantener actualizada la clasificación efectuada
- Establecer los requisitos de la información en materia de seguridad.

- Trabajar en colaboración con el Responsable de Seguridad de la Información y el Responsable del Sistema en el mantenimiento del mismo.
- Decidir los niveles de riesgo residual aceptables que afecten a la información y promover la aplicación de las medidas de seguridad correspondientes.

Responsables de los servicios

El responsable de cada servicio tendrá las siguientes funciones:

- Establecer los requisitos del servicio TIC en materia de seguridad.
- Trabajar en colaboración con el responsable de Seguridad de la Información y el Responsable de Sistema en el mantenimiento de los sistemas.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes (relacionados con el servicio) y por su cumplimiento.
- Decidir los niveles de riesgo residual aceptables que afecten al servicio y promover la aplicación de las medidas de seguridad correspondientes.

Responsable de Seguridad de la Información

El responsable de Seguridad de la Información tendrá las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas en su ámbito de responsabilidad.
- Realizar y/o promover revisiones periódicas que permitan verificar el cumplimiento de las obligaciones de la UUNN en materia de seguridad.
- Promover la formación y concientización del personal de la UUNN en materia de seguridad de la información.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad de los sistemas.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de control implementados en los sistemas.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el propietario de los sistemas y a las autoridades de la UUNN, incluyendo los incidentes más relevantes del periodo.
- Aprobar los procedimientos de seguridad elaborados por el responsable del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en los sistemas.
- Elaborar la normativa de seguridad de la información de la UUNN.

- Promover la capacitación y concientización en el uso de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Ser el referente con la autoridad competente en materia de seguridad de la información.
- Convocar a una reunión con el comité de seguridad en caso excepcional ante la ocurrencia de un incidente.

Responsables de los sistemas

El responsable de cada sistema tendrá, dentro de sus áreas de actuación, las siguientes funciones:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y los procedimientos de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba de este.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Colaborar en el proceso de análisis y gestión de riesgos en el Sistema.
- Elaborar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada área o entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
- Velar por el cumplimiento de las obligaciones de los administradores de los sistemas de información para que las medidas de seguridad que les afecten en el ámbito de sus competencias sean implementadas.
- Promover la investigación de los incidentes de seguridad que afecten al sistema y comunicar al responsable de Seguridad de la Información o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

- Acordar, de ser necesaria, la suspensión del servicio con los propietarios de la información y el responsable del servicio afectado, y el responsable de seguridad de la información.
- Elaborar los procedimientos de seguridad necesarios para la operativa en el sistema.

Responsable del Área de Recursos Humanos

- Notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.
- Comunicar la presente Política a todo el personal, los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad de la información.
- Promover las campañas de concientización en seguridad de la información.

Responsable del Área Informática

- Cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la UTN.

Responsable del Área Legal o Jurídica

- Verificar el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la UTN con el personal y, en caso de existir, con los terceros. Asimismo, asesorará en materia legal a la UTN, en lo que se refiere a la seguridad de la información.

Toda la comunidad

- Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente, en los aspectos que correspondan.
- Asistir a las actividades relacionadas con las campañas de concientización y capacitación en seguridad de la información.

4.2 Conformación del Comité de Seguridad de la Información

La conformación aquí establecida incluye los roles que son necesarios mínimamente. Cada organización también podrá incluir otros roles que lo conformarán de acuerdo con sus características y funcionamiento.

1. Responsable de seguridad de la información.
2. Responsable(s) de TI (del área central).
3. Responsable del área RRHH.
4. Responsable del área legal.
5. Responsable del área económica.

El Comité podrá incorporar a sus reuniones a las personas que considere oportuno en función de los temas a tratar.

El Comité propondrá la designación del Coordinador que será aprobado por las autoridades de la UTN.

Funciones y Responsabilidades

- Revisar y proponer al Consejo Superior para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
- Controlar cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área[2].
- Acordar y aprobar metodologías y procesos relativos a seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información; evaluará y coordinará la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Resolver los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

[2] Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo a sus competencias, elevándolas a la máxima autoridad, a través del Comité de Seguridad, con relación a la seguridad de la información del Organismo. Dichas iniciativas deben ser aprobadas luego por la máxima autoridad del Organismo.

Coordinador del comité de seguridad de la información

- Coordinar las acciones del Comité de Seguridad de la Información; y de
- Impulsar la implementación y cumplimiento de la Política de seguridad de la información y de toda la normativa que se desprenda de ella.

5. Gestión de riesgos

La Institución evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo. Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.

Se debe repetir la evaluación:

- Regularmente, con la frecuencia que el Comité de Seguridad de la Información defina.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados, o cuando haya un cambio significativo en la plataforma tecnológica.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

6. Obligaciones de la comunidad universitaria

Todos los miembros de la UTN tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados definidos en el alcance de la presente política.

Se debe establecer un programa de concientización continua para atender a todos los miembros de la comunidad universitaria, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

7. Terceras partes

Cuando la UTN preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la respuesta ante incidentes de seguridad.

Cuando la UTN utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la referida normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concientizado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se refiere en los párrafos anteriores, se requerirá un informe del responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los propietarios de la Información y de los responsables de los servicios afectados antes de seguir adelante.

8. Normativas de seguridad

La política de seguridad de la información se desarrollará en normativas específicas que permitan la implementación de la presente política.

Se proponen las siguientes temáticas:

- Política de Seguridad de la Información del organismo
- Aspectos Organizativos de la Seguridad
- Seguridad Informática de los Recursos Humanos
- Gestión de Activos
- Autenticación, Autorización y Control de Accesos
- Uso de herramientas criptográficas
- Seguridad física y ambiental
- Seguridad operativa
- Seguridad en las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Relación con proveedores
- Gestión de incidentes de seguridad
- Aspectos de seguridad para la continuidad de la gestión
- Cumplimiento

Las normativas por desarrollarse deben incluir las temáticas anteriormente listadas, pero no limitarse a las mismas.