UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Contraloría General

Sobre el adecuado uso de los recursos tecnológicos y de los activos de información de la Universidad

A la comunidad universitaria

La Contraloría General y su área de Cumplimiento Institucional junto con el Oficial de Seguridad de la Información los invita a revisar la siguiente información sobre el uso adecuado de los recursos tecnológicos de nuestra Casa de Estudios y la importancia de nuestro comportamiento.

Uso de los Recursos Tecnológicos Institucionales

Toda actividad desempeñada utilizando recursos tecnológicos institucionales deberá responder a los más altos estándares de comportamiento, cumpliendo con los reglamentos y normativa interna y leyes vigentes.
Los recursos tecnológicos de la Universidad están comprendidos por:

- PC de Escritorio
- Notebook
- Tablet
- Celulares u otro dispositivo institucional utilizado para almacenar información.
- Sistemas, programas y aplicaciones instaladas con licencias respectivas.
- Conexión a la red de Internet (en sus instalaciones o mediante VPN)

Está prohibido instalar aplicaciones, programas o sistemas no autorizados por la Universidad o que no cuenten con las licencias respectivas por los graves riesgos asociados.

- Riesgos legales al infringir ley de propiedad intelectual. (Ley N°17.336)
  Los medios tecnológicos actuales permiten a los fabricantes de sistemas estar atentos y monitorear el correcto uso de sus sistemas, de manera que la Universidad recibirá notificaciones en caso de que se detecte pirateo exponiéndose a sanciones penales, civiles y tributarias. Además, desde diciembre del año 2022, se incorporan delitos informáticos estipulados en la Ley N°21.459 a la Ley N°20.393 sobre Responsabilidad Penal de las Personas Jurídicas.

- Riesgos de Seguridad al bajar junto con el programa sin licencia aplicaciones con malware. El malware es capaz de robar contraseñas, imitar sitios de bancos, registrar todo lo que se digita en el teclado, redirigir búsquedas de internet, recopilar información del computador, enviar emails falsos, robar información confidencial, permitiendo además el libre acceso a personas no autorizadas al computador y a la red interna.

No instales software que no cuenten con la licencia respectiva. En caso de dudas, consulta con mesa de servicios de la DTI. (mesadeservicios.dti@usm.cl)

Uso de los Activos de Información Institucionales

Todos los colaboradores que tengan acceso a los activos de información institucionales deben tener en cuenta que la destrucción, bloqueo de acceso, modificación indebida de la información o cualquier obstrucción para acceder a información, además de la difusión indebida está contemplada en la ley como delito. (Ley N°21.459)

Los activos de información institucionales están comprendidos por:

- Correo electrónico
- Bases de datos
- Archivos y carpetas compartidas
- Sistemas de información y documentación
- Almacenamiento electrónico y
- Todos los medios que se utilizan para trabajar

Además, de estar contemplada en la normativa legal, el adecuado uso de los recursos tecnológicos y de los activos de información se encuentran normado en el Código de Ética Institucional y en nuestro Reglamento Interno de Orden Higiene y Seguridad (RIOHS).

Finalmente, reforzar que el correcto uso de los recursos tecnológicos y de los activos de información institucionales son fundamentales para la consecución de la misión de la Universidad, y como tal debemos poner el debido cuidado y la debida diligencia en todo nuestro quehacer laboral.

Publicación sobre delitos informáticos Ley N° 21.459

En el mes de diciembre de 2022 comenzó a regir la Ley N° 21.459 sobre delitos informáticos y en su artículo 21, establece que se incorporan dichos delitos a la Ley N° 20.393 sobre Responsabilidad Penal de las Personas Jurídicas. Los delitos son[1]:

1. Ataque a la integridad de un sistema informático: Comete este delito el que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.

2. Acceso ilícito: Comete este delito el que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático.

[1] Los delitos son los indicados en las Ley 21.459, en sus artículos 1° al 8°.

3. Interceptación ilícita: Comete este delito el que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos. El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos.

4. Ataque a la integridad de los datos informáticos: Comete este delito el que indebidamente altere, dañe o suprima datos informáticos, siempre que con ello se cause un daño grave al titular de estos mismos.

5. Falsificación informática: Comete este delito el que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos.

6. Receptación de datos informáticos: Comete este delito el que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en 2,3 y en 5.

7. Fraude informático: Comete este delito el que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático.

8. Abuso de los dispositivos: Comete este delito el que para la perpetración de los delitos previstos en 1 a 4 o de las conductas señaladas en el artículo 7° de la ley N° 20.009 (delito de uso fraudulento de tarjetas de pago y transacciones electrónicas), entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos.

CONTRALORIA GENERAL USM.