



LINEAMIENTOS DE SEGURIDAD INFORMÁTICA

ÍNDICE

Introducción		3
Alcance		3
Normatividad aplicable		3
Lineamientos		3
Capítulo 1	De la seguridad informática en la institución	3
Capítulo 2	Del buen uso de los activos informáticos	5
Capítulo 3	De la clasificación de la información	5
Capítulo 4	Del intercambio de información	6
Capítulo 5	De la prestación de servicios por terceros	6
Capítulo 6	De la protección contra código malicioso (virus)	6
Capítulo 7	De los servicios informáticos en la red	6
Capítulo 8	Del uso de cuentas de usuario	8
Capítulo 9	Del uso del código telefónico	9
Capítulo 10	Del monitoreo del uso de los servicios informáticos	9
Capítulo 11	Del uso del Internet	9
Capítulo 12	Del uso del correo electrónico y mensajería instantánea	10
Capítulo 13	Del uso del software	11

1. INTRODUCCIÓN.

Los Lineamientos de Seguridad Informática, son directrices que tienen como objetivo promover el buen uso y cuidado de los recursos de tecnologías de información entre autoridades, personal académico, personal no académico, alumnos y terceros; mediante la comunicación de las medidas y formas que deben cumplir y utilizar para proteger los componentes de los sistemas informáticos del ITSON, sin menoscabo de los derechos humanos y la autonomía universitaria.

Norman la forma como el ITSON previene, protege y administra los riesgos relacionados con tecnologías de información en las instalaciones, equipos, información, servicios y soluciones informáticas.

2. ALCANCE.

Todo el personal académico, administrativo, alumnos, proveedores y demás personas relacionadas con nuestra institución y que hagan uso de nuestros servicios e infraestructura de cómputo y comunicaciones, deben de dar cumplimiento a los Lineamientos de Seguridad Informática Institucional; tanto en el interior de las instalaciones de todos los Campus ITSON, como en el exterior; de manera física y lógica vía internet.

3. NORMATIVIDAD APLICABLE.

Los ordenamientos jurídicos administrativos vigentes que regulan la operación de las actividades o tareas específicas a normar a través de los lineamientos de seguridad informática, entre otros, son:

- Constitución Políticas de los Estados Unidos Mexicanos.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Orgánica de Instituto Tecnológico de Sonora.
- Reglamento General de la Ley Orgánica del Instituto Tecnológico de Sonora.

4. LINEAMIENTOS.

Capítulo 1. De la seguridad informática en la institución.

El presente documento de Lineamientos de Seguridad Informática debe ser revisado anualmente por la DSI, debe ser actualizado cuando sea necesario y todo cambio debe ser autorizado por el Rector.

Los términos y definiciones utilizados en el presente documento son:

ITSON: Instituto Tecnológico de Sonora.

DSI: Dirección de Servicios de Información.

DTSI: Departamento de Tecnologías y Servicios Informáticos.

Usuario: Todo empleado o prestatario de servicios autorizado por ITSON, alumnos y terceros que haga uso de los activos o servicios informáticos de la institución, para el desempeño de sus funciones, consulta o atención al servicio.

Activo informático: Son recursos de sistemas informáticos o relacionados con este, que son necesarios para el desempeño de las funciones usuario, tales como equipos de cómputo, impresoras, video proyectores, teléfonos, equipos de telecomunicaciones, software, información, entre otros.

Equipo móvil: Es todo activo informático físico que tiene la facilidad de movilidad, como laptops, tabletas, teléfonos inteligentes, entre otros.

Servicio informático: Bien intangible que se proporciona para satisfacer los requerimientos de los usuarios, relacionado con el uso de activo informático.

Medio de almacenamiento removible: Medio externo al equipo de cómputo en el que se almacena información, como disquetes, CD, DVD, memorias (USB, SD, otras), cartuchos de respaldo, discos externos y otros.

Base de datos: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Derecho de autor: Protección legal que cubre las actividades y trabajos de creación de productos de cualquier tipo que sean plasmados de forma tangible o material de conformidad con el marco aplicable en la materia. Las leyes de derecho de autor garantizan al creador el derecho exclusivo de reproducir, creación de derivados o hacer público su trabajo.

Derechos de propiedad industrial: Protección legal destinada a proteger las invenciones individuales e industriales y que prohíben la copia, venta, reproducción o importación de determinado producto sin autorización explícita del dueño de los derechos de propiedad intelectual.

Software institucional: Software con licenciamiento de uso y/o propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por la institución.

Software libre: También conocido como freeware, shareware, software demo. Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.

Cifrar: Técnicas bajo las cuales se transforma la información (de texto claro a texto secreto) y que solo puede ser accedida si se cuenta con las llaves o contraseñas.

Web, www (World Wide Web): Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de Internet en una forma fácilmente accesible.

Sistema avanzado para navegar a través de Internet.

Sistema JDEdwards: Sistema utilizado para la administración de alta calidad de organizaciones, inventarios, equipos, finanzas y personas que están estrechamente integrados y previamente incorporados en una sola base de datos utilizado por el ITSON bajo la debida licencia.

CIA: Sistema utilizado para la administración escolar, integrados en una solución de bases de datos y aplicativos informáticos.

Virus: Programa informático creado para producir daño en el equipo informático.

Capítulo 2. Del buen uso de los activos informáticos.

Artículo 1. Los usuarios que tengan activo informático asignado de manera personal para uso de sus funciones, son los únicos responsables de su utilización, así como también de la información contenida en los mismos, por lo que debe evitar compartirlos.

En caso de requerir compartirlo o prestar el activo informático, será solamente para cuestiones laborales y sin liberarlo de su responsabilidad.

Artículo 2. Toda movilización de activo informático dentro o fuera de las instalaciones de la institución es responsabilidad del resguardante.

Capítulo 3. De la clasificación de la información.

Artículo 3. El dueño de un servicio informático ofrecido por la institución es responsable de la información que este servicio genera y procesa.

Artículo 4. Los titulares de cada dependencia deben informar a sus colaboradores de la clasificación de la información a su cargo para su adecuado tratamiento.

Artículo 5. Todo empleado responsable de resguardo de información, debe asegurar que la información esté protegida para asegurar su integridad y confidencialidad, acorde a su clasificación. La información puede estar disponible de manera electrónica, impresa en papel, magnética, óptica y otro medio.

Artículo 6. Todo usuario deberá hacer uso de la información a la que tenga acceso únicamente para propósitos relacionados con el cumplimiento de sus funciones, debiendo resguardar principalmente la relativa a datos personales, absteniéndose de comunicarlos a terceros sin el consentimiento expreso de la persona a la que se refieren.

Artículo 7. Todos los usuarios que hacen uso de información clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas.

Capítulo 4. Del intercambio de información.

Artículo 8. Toda persona que intercambie información reservada y/o confidencial con personal de ITSON o terceras personas, debe asegurar la identidad de la persona a la que le es entregada la información, ya sea por medio físico o electrónico, dejando constancia que es procedente la entrega de información.

Artículo 9. Todo convenio de ITSON con terceras personas para compartir información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales.

Capítulo 5. De la prestación de servicios por terceros.

Artículo 10. Todo proveedor que proporcione servicios informáticos a ITSON y que tenga acceso a información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique a ITSON.

Artículo 11. Todo servicio informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación, para asegurar que se cumplan con los términos estipulados en los acuerdos o contratos de ITSON.

Capítulo 6. De la protección contra código malicioso (virus).

Artículo 12. Todo equipo de cómputo institucional debe contar con solución antivirus definida por el DTSI. Si la solución no cubre a la plataforma utilizada, el personal notificará al DTSI para buscar una alternativa de solución.

Artículo 13. Todo Usuario que identifique una anomalía en su equipo de cómputo deberá reportarla al DTSI mediante sistema de mesa de servicio del DTSI.

Capítulo 7. De los servicios informáticos en la red.

Artículo 14. Todo personal, alumnos y terceros son responsables del buen uso de los servicios informáticos institucionales alojados en nuestras instalaciones y en la nube, asignados para realizar sus funciones administrativas y académicas.

Artículo 15. Personal de seguridad informática del DTSI queda facultado para acceder a los equipos de cómputo institucionales, aun en aquellos que no están a su resguardo, para:

- la realización de revisiones en base a cumplimiento de medidas de seguridad informática como antivirus y actualizaciones,
- el inventario de software y hardware,
- por ausencia del personal en base a petición del jefe inmediato y que se requiera acceder a información y servicios en base a sus funciones,
- y a petición de la Contraloría Interna para realizar una revisión de seguridad informática y descartar uso no debido (daños intencionales a información, equipo, a personas) del equipo de cómputo, bajo previa notificación al usuario, como se especifica en artículo 28 y artículo 31 del presente documento.

En caso de ausencia e imposibilidad de localizar al usuario, la notificación se realizará al jefe inmediato.

Artículo 16. Todo titular del área con sistemas de información, es responsable de autorizar el nivel de acceso con privilegios mínimos necesarios para que el personal académico y administrativo realice sus funciones.

Artículo 17. Ninguna persona debe ver, copiar, alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del responsable del equipo o del dueño de la información, excepto en casos que se especifican en el artículo 15 del presente documento.

Artículo 18. Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información en la red ITSON, así como a los de telefonía, son personales, permitiéndose el uso bajo su responsabilidad, única y exclusivamente durante la vigencia de los derechos del usuario. La vigencia de las cuentas de usuarios es facultad del DTSI y del área dueña del servicio, éstas son habilitadas, suspendidas o canceladas por el área en consideración a las solicitudes, necesidades y conductas de los usuarios.

Artículo 19. Toda utilización de herramientas tales como analizadores, escaneo y monitoreo de red, son permitidas únicamente para las funciones de administración de las tecnologías de información y de actividades académicas bajo la supervisión del docente.

Artículo 20. Todo hardware de telecomunicaciones (switches, enrutadores, puntos de acceso inalámbrico, entre otros) y servidores (web, FTP, correo y otros) que se requiera habilitar en la red de telecomunicaciones institucional debe ser previamente autorizado por el DTSI.

Artículo 21. A todo equipo de cómputo institucional conectado a la red ITSON (computadoras de escritorio y portátiles), personal autorizado por el DTSI deberá de configurarlo en la red de Dominio ITSON, y además otorgar cuenta de usuario para acceder a los servicios de la red ITSON.

Artículo 22. Todo servicio de Red Privada Virtual (VPN) para ser utilizado en laptops fuera de la institución, será otorgado a todo el personal que lo requiera para sus funciones laborales, siendo autorizado por el DTSI, considerándose para ello la capacidad de la infraestructura de tecnologías de información de que dispone la institución.

Artículo 23. A toda persona que deje de laborar o tener relación con el ITSON, le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales. El Departamento de Personal comunicará al DTSI y a las demás áreas responsables de brindar servicios informáticos, toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de red.

Artículo 24. A todo hardware y software de uso académico que sean considerados de riesgo para la seguridad de los servicios informáticos institucionales, deberán ser utilizados en ambiente aislado.

Ejemplos de hardware y software son analizadores de tráfico de red, herramientas de análisis y diagnóstico de equipos de cómputo y telecomunicaciones, inventario de red, equipos de laboratorio de redes, entre otros.

Capítulo 8. Del uso de cuentas de usuario.

Artículo 25. Toda persona que requiera acceder a servicios informáticos institucionales, requerirá de una cuenta de usuario y contraseña u otro medio de autenticación. La cuenta de usuario y contraseña deberá ser asignada por el responsable del servicio.

Artículo 26. Toda solicitud de alta, baja o cambio de privilegios de cuentas de usuario para acceder a los servicios informáticos adicionales a su perfil de puesto debe ser solicitada a través del sistema de mesa de servicios del DTSI por el jefe inmediato o jefe de área demandante, debidamente justificado.

Artículo 27. Todo usuario debe actualizar la contraseña de su cuenta de acceso a los servicios informáticos de manera periódica (al menos cada 6 meses) o cuando sospeche de su divulgación. La contraseña debe ser de al menos 8 caracteres alfanuméricos y que sea fácil de recordar.

Artículo 28. Cuando se requiera acceder a información de un equipo de cómputo y/o cuenta de correo institucional de una persona ausente ya sea por cuestiones de salud, por estar comisionado a actividades fuera de su área de trabajo u otro motivo no especificado, el responsable del área correspondiente deberá solicitar al DTSI que se brinde el acceso al equipo y/o servicio o sistema informático para poder dar continuidad a algún proceso institucional.

Personal del DTSI únicamente proporcionará acceso al responsable del área correspondiente que lo haya solicitado a efecto de que sustraiga la información necesaria, dejando constancia de ello en un acta circunstanciada que se levante con asistencia del área jurídica, bajo previa notificación a la persona ausente.

Si una persona deja de laborar en la Institución o cambia de puesto, el jefe inmediato podrá solicitar al DTSI el acceso al equipo institucional que ésta tenía asignado, el cual es concedido para que sustraiga la información pertinente, y sin necesidad de la intervención del área jurídica.

Capítulo 9. Del uso del código telefónico.

Artículo 29. A todo usuario con servicio de telefonía se le asignará un código telefónico, haciéndose éste responsable de su uso y no divulgación.

Artículo 30. Por seguridad, todo código para el servicio telefónico será cambiado y asignado periódicamente por personal responsable de administrar el servicio de telefonía institucional del DTSI o a petición del usuario.

Capítulo 10. Del monitoreo del uso de los servicios informáticos.

Artículo 31. Personal del DTSI realiza periódicamente inventarios de hardware y software del activo informático institucional, para dar atención a problemas de obsolescencia y revisiones de licenciamiento.

Además, se monitorean los servicios informáticos de red para administrar el uso del recurso informático de internet y solución de problemas.

Capítulo 11. Del uso de Internet.

Artículo 32. El servicio de Internet a través de las redes institucionales se considera como herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para apoyo a sus actividades académicas y/o administrativas en el ITSON.

Artículo 33. Todo responsable de área puede solicitar la restricción total o parcial de acceso a Internet del personal a su cargo, considerando para ello las funciones laborales que éstos realizan.

Artículo 34. Para la integración de toda solución informática basada en protocolos de internet, el área requirente debe solicitar a personal del DTSI evaluar y recomendar los recursos de infraestructura de cómputo y telecomunicaciones, con el fin de que el área requirente gestione los recursos necesarios para la puesta en producción de la solución.

Artículo 35. Todo usuario que descargue información y archivos de Internet mediante el navegador web u otro medio como FTP y mensajería instantánea, debe de omitir descargar archivos de dudosa procedencia. Los archivos descargados de Internet pueden contener virus o software malicioso que pongan en riesgo la información del equipo de cómputo de la persona, e incluso de la Institución.

Capítulo 12. Del uso del correo electrónico y mensajería instantánea.

Artículo 36. El correo electrónico institucional es para uso exclusivo del empleado activo administrativo, académico y personas externas a las que se les reconoce la relación con el ITSON. Éste deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.

Artículo 37. Los responsables de área deberán solicitar por los medios establecidos por el DTSI, a través del sistema de mesa de servicio, una nueva cuenta de correo electrónico para personal a su cargo.

Artículo 38. El ITSON no es garante de los contenidos expresados en texto, sonido o video, redactados y enviados mediante el correo electrónico institucional.

Artículo 39. A toda persona que termine la relación laboral con el ITSON, una vez recibida la notificación de baja por parte del Departamento de Personal, se inhabilitará el servicio de correo electrónico.

Transcurridos 30 días hábiles, el contenido de la cuenta de correo inhabilitada será eliminado sin generarse ningún respaldo del mismo.

Artículo 40. Toda solicitud de alta, baja o cambio de un grupo de correo institucional debe ser solicitada por el responsable del área solicitante.

Artículo 41. Queda prohibido utilizar el correo electrónico para envíos de correo basura, cadenas, mercadotecnia, religiosos, propaganda política, actos agresivos e ilegales y cualquier otro contenido no apropiado para el destinatario.

Artículo 42. Es responsabilidad de todo usuario del correo electrónico institucional notificar al personal del DTSI la sospecha del uso no autorizado de su cuenta.

Artículo 43. Todo usuario del correo electrónico institucional, acepta que comprende y acuerda expresamente que el ITSON, no es responsable directo e indirecto y sin limitación alguna, por pérdida de datos o de cualquier otra pérdida intangible en el servicio de correo electrónico.

Artículo 44. Todo usuario que desde una cuenta de correo electrónico institucional o externo, requiera enviar un correo masivo, entendiéndose como aquel que se envía a más de 50 destinatarios, ya sea en un mismo envío o en varios envíos con contenido similar, deberá previamente solicitar la autorización del Director de su área y posteriormente realizar la solicitud correspondiente en Sistema de Mesa de Servicio del DTSI vigente.

Artículo 45. Todo servicio de mensajería instantánea debe ser utilizado para el desarrollo de actividades concernientes al puesto del personal; donde cada persona es responsable del buen uso de este servicio.

Todo empleado ITSON puede acceder a la mensajería instantánea interna solicitando al DTSI su usuario y contraseña e instalación de la aplicación.

Capítulo 13. Del uso del software.

Artículo 46. En todos los equipos de cómputo del ITSON, solo se permite la instalación de software con licenciamiento vigente, ya sea de uso libre o comercial. Las áreas de Soporte Técnico Informático están facultadas para asesorar la instalación del software.

Artículo 47. Toda persona que necesite adquirir software, podrá solicitar apoyo al DTSI, quien verificará los requerimientos técnicos y el completo licenciamiento, y recabar una copia de esta licencia para su resguardo.

Artículo 48. Todo empleado, alumno y terceros que instale software sin licenciamiento vigente o malicioso en equipos de cómputo de la institución, se hace único responsable de las consecuencias que esto conlleve.

Artículo 49. Las licencias de uso de software propiedad del ITSON, otorgan a éste el derecho de emplearlas exclusivamente en los equipos asignados al personal de la institución.