LINEAMIENTOS DE SEGURIDAD INFORMÁTICA DEL ISIFE

El Grupo de Trabajo de Tecnologías de Información y Comunicaciones

Ing. Carlos Rivas Lizaola

Arq. Carlos Roberto Salinas Amao

Lic. Fco. Javier Meza Radilla

Ing. Martín Estrada Núñez

Ing. Alberto Jesús Ayala Mendoza

Edgardo MTZ.

Lic. Edgardo Daniel Martínez Grijalva

La Paz, Baja California Sur, septiembre de 2019.

Contenido

I. 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 todo el personal; mediante la comunicación de las medidas y formas que deben cumplir y utilizar para proteger los componentes de los sistemas informáticos del Instituto Sudcaliforniano de la Infraestructura Física Educativa (ISIFE).

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

II. Alcance

Todo el personal 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 este instituto, como en el exterior; de manera física y lógica vía internet.

III. 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:

- Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur.
- Ley De Protección De Datos Personales En Posesión De Sujetos Obligados Para El Estado De Baja California Sur
- Ley de la Infraestructura Física Educativa del Estado de B.C.S.
- Ley De Responsabilidades De Los Servidores Públicos Del Estado Y De Los Municipios De Baja California Sur.
- Código de Ética del ISIFE.

IV. Lineamientos

Capítulo 1. De la seguridad informática en la institución.

El presente documento de Lineamientos de Seguridad Informática debe ser revisado anualmente por el área de sistemas del ISIFE, debe ser actualizado cuando sea necesario y todo cambio debe ser autorizado por el grupo de trabajo de tecnologías de información y comunicaciones.

Los términos y definiciones utilizados en el presente documento son:

ISIFE: Instituto Sudcaliforniano de la Infraestructura Física Educativa.

Usuario: Todo empleado 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 del 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.

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.

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.

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 usuario 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 área deben informar a sus colaboradores de la clasificación de la información a su cargo para su adecuado tratamiento.

Artículo 5. Todo usuario 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 digital, impresa en papel, magnética y otro medio.
Todos los usuarios que hacen uso de información clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas.

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, dando cumplimiento a la Ley de Protección de Datos Personales de Baja California Sur.

Capítulo 4. Del intercambio de información.

Artículo 7. Toda persona que intercambie información reservada y/o confidencial con terceras personas, debe asegurar la identidad de quien solicita la información, ya sea por medio físico o electrónico, dejando constancia que es procedente la entrega de información.

Artículo 8. Todo convenio de ISIFE 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 9. Todo proveedor que proporcione servicios informáticos a ISIFE 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.

Artículo 10. Todo servicio informático otorgado por terceros debe ser monitoreado y revisado por el área de sistemas, para asegurar que se cumplan con los términos estipulados en los acuerdos o contratos de ISIFE.

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

Artículo 11. Todo equipo de cómputo institucional debe contar con solución antivirus definida por el área de sistemas. Si la solución no cubre a la plataforma utilizada, los usuarios pueden notificarlo al área de sistemas para buscar una alternativa de solución.

Artículo 12. Todo Usuario que identifique una anomalía en su equipo de cómputo deberá reportarla al área de sistemas.

Capítulo 7. De los servicios informáticos en la red.

Artículo 13. Todo usuario es responsable del buen uso de los servicios informáticos institucionales alojados en nuestras instalaciones y en la nube, asignados para realizar sus funciones.

Artículo 14. Personal del área de sistemas queda facultado para acceder a los equipos de cómputo institucionales 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,
- 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 29 del presente documento.

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

Artículo 15. El responsable del área de sistemas, autorizara el nivel de acceso con privilegios mínimos necesarios para que el usuario realice sus funciones.

Artículo 16. Ningún usuario debe 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 17. Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información en la red ISIFE, 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 área de sistemas, éstas son habilitadas, suspendidas o canceladas, derivado de solicitudes, necesidades y conductas de los usuarios.

Artículo 18. Toda utilización de herramientas, tales como analizadores, escaneo, monitoreo de red, equipos de audio y video, serán permitidas únicamente para las

funciones de administración de las tecnologías de información y deberán estar al conocimiento del área de sistemas para garantizar el uso adecuado de dichas herramientas.

Artículo 19. 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 área de sistemas.

Artículo 20. A todo equipo de cómputo institucional conectado a la red ISIFE (computadoras de escritorio y portátiles), el área de sistemas deberá de configurarlo en la red de Dominio ISIFE, otorgando una cuenta de usuario para acceder a los servicios de la red del instituto.

Artículo 21. 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 y configurado por el área de sistemas, considerándose para ello la capacidad de la infraestructura de tecnologías de información de que dispone la institución.

Artículo 22. A toda persona que deje de laborar o tener relación con el ISIFE, le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales. El Departamento de Administración comunicará al área de sistemas que es el responsable 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 23. Todo hardware y software que sean considerados de riesgo para la seguridad de los servicios informáticos institucionales, deberán ser utilizados en ambiente aislado.

Capítulo 8. Del uso de cuentas de usuario.

Artículo 24. Todo usuario 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 área de sistemas.

Artículo 25. 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 por el jefe inmediato o jefe de área demandante al área de sistemas.

Artículo 26. 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 27. 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 área de sistemas que se brinde el acceso al equipo y/o servicio o sistema informático para poder dar continuidad a algún proceso institucional.
Si una persona deja de laborar en la Institución o cambia de puesto, el jefe inmediato podrá solicitar al área de sistemas el acceso al equipo institucional que ésta tenía asignado, el cual es concedido para que sustraiga la información pertinente.

Capítulo 9. Del monitoreo del uso de los servicios informáticos.

Artículo 28. Personal del área de sistemas realiza periódicamente inventarios de hardware y software del activo informático institucional, para dar atención a problemas de obsolescencia e incompatibilidades.

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

Capítulo 10. Del uso de Internet.

Artículo 29. 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 de trabajo en el ISIFE.

Artículo 30. Los titulares de las unidades administrativas pueden 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 31. Todo usuario debe omitir descargar información y archivos de Internet de dudosa procedencia, mediante el navegador web u otro medio como FTP y mensajería instantánea. Los archivos descargados de Internet pueden contener virus o software malicioso que ponen en riesgo la información del equipo de cómputo de la persona, e incluso de la Institución.

Capítulo 11. Del uso del correo electrónico y mensajería instantánea.

Artículo 32. El correo electrónico institucional es para uso exclusivo del empleado activo y personas externas a las que se les reconoce la relación con el ISIFE. Éste deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.

Artículo 33. Los responsables de área deberán solicitar por los medios establecidos por el área de sistemas, una nueva cuenta de correo electrónico para personal a su cargo.

Artículo 34. El ISIFE no es responsable de los contenidos expresados por los usuarios en texto, sonido o video, redactados y enviados mediante el correo electrónico institucional.

Artículo 35. A toda persona que termine la relación laboral con el ISIFE, una vez recibida la notificación de baja por parte del Departamento de Administración, 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 36. Toda solicitud de alta, baja o cambio de un grupo de correo institucional debe ser solicitada por el responsable del área solicitante.

Artículo 37. 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 38. Es responsabilidad de todo usuario del correo electrónico institucional notificar al personal del área de sistemas la sospecha del uso no autorizado de su cuenta.

Artículo 39. Todo usuario del correo electrónico institucional, acepta que comprende y acuerda expresamente que el ISIFE, 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 40. 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 ISIFE puede acceder a la mensajería instantánea interna solicitando al área de sistemas su usuario y contraseña e instalación de la aplicación.

Capítulo 12. Del uso del software.

Artículo 41. En todos los equipos de cómputo del ISIFE, solo se permite la instalación de software que apoye a la tarea de sus funciones asignadas por su jefe inmediato. El personal del área de sistemas es el único facultado para realizar la instalación del software.

Artículo 42. Toda persona que necesite adquirir software, podrá solicitar apoyo al área de sistemas, quien verificará los requerimientos técnicos y el completo licenciamiento, y recabar una copia de esta licencia para su resguardo.

Artículo 43. Todo empleado, 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 44. Las licencias de uso de software propiedad del ISIFE, otorgan a éste el derecho de emplearlas exclusivamente en los equipos asignados al personal de la institución.

Capítulo 13. De las Sanciones.

Artículo 45. Todo usuario que vaya en contra de las políticas y lineamientos mencionados anteriormente, o que de forma deliberada atente contra los bienes informáticos o la información digital del instituto, puede ser acreedor a una sanción, esta puede ser, económica para la reposición de un bien informático o bien la elaboración de un acta por falta administrativa.