Lineamientos de Informática del Instituto Guanajuatense para las Personas con Discapacidad

Lic. José José Grimaldo Colmenero, Director General del Instituto Guanajuatense para las Personas con Discapacidad, con fundamento en lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 80 de la Constitución Política para el Estado de Guanajuato; 1, 3, 4, 5 de la Ley General de Inclusión Para las Personas con Discapacidad; 1, 4, 10, 11 fracciones VI, XX, XXII y XXIII, 12, fracciones IV, XII y XIII, de la Ley de Inclusión para las Personas con Discapacidad del Estado de Guanajuato; Artículo 7 fracción IV, inciso b), Artículo 29 y Artículo primero y segundo Transitorio de la Ley del Presupuesto General de Egresos del Estado de Guanajuato para el Ejercicio Fiscal de 2023; 78, sexies y 78, septies de la Ley para el Ejercicio y Control de los Recursos Públicos para el Estado y los Municipios de Guanajuato; 26, fracción XV y 27, fracción XV de la Ley Transparencia y Acceso a la Información Pública para el Estado de Guanajuato; y, en ejercicio de las facultades que me confieren el artículo 28, facción XIV del Reglamento Interior del Instituto Guanajuatense para las Personas con Discapacidad y Acuerdo **CD-IGPD/CD-19/2023**de la Segunda Sesión Ordinaria del Consejo Directivo de fecha **18 de agosto de 2023** del Instituto Guanajuatense para las Personas con Discapacidad;

C O N S I D E R A N D O

El Instituto Guanajuatense para las Personas con Discapacidad, se ha responsabilizado en normar y orientar las acciones de rehabilitación e inclusión social en nuestro Estado y con ello prestar atención al sector de la población que presenta algún tipo de discapacidad, sea esta transitoria o permanente, estableciendo parámetros que definan el grado de discapacidad existente, los potenciales remanentes y el nivel de impacto personal, familiar y/o social.

Los presentes lineamientos se alinean con la Meta Nacional o estrategia transversal del Plan Nacional de Desarrollo, en la estrategia transversal 2. Gobierno Cercano y Moderno y los Elemento del Plan Estatal de Desarrollo con el Objetivo 4.1.1. Incrementar la eficiencia y la eficacia del sector público estatal, con el involucramiento corresponsable de la sociedad, así como con los Objetivos del Desarrollo Sostenible ODS, objetivo 10, Reducción de las desigualdades y, Elemento del Plan Estatal de Desarrollo, Objetivo 1.3.1, Asegurar las condiciones para el desarrollo pleno e igualitario de los grupos prioritarios del Estado.

La estrategia del Instituto en materia de atención Integral a personas con discapacidad y asistencia social, así como el objetivo primordial que es el empoderamiento a los beneficiarios de programas institucionales, generar conciencia, capacitación y uso racional de los servicios, nos plantea como meta la suficiencia en los servicios otorgados y, principalmente, el capital humano en la optimización de los recursos, presupuesto e insumos indispensables para la prestación de servicios a los beneficiarios de los programas sociales.

El rápido avance y evolución de la de tecnológica en los últimos años, ha hecho que las tecnologías de la Información, Comunicaciones y la Seguridad Informática, se hayan vuelto parte fundamental en el desarrollo de nuestras actividades cotidianas no solo laborales sino también personales. Dicho crecimiento ha sido tan acelerado que no nos ha dado tiempo de asimilar la información y conocimientos necesarios para el uso responsable del inmenso mundo de tecnología que tenemos hoy a nuestro alcance.

Es por ello que, en el Instituto, a través de la coordinación de Informática y telecomunicaciones considera necesario reeducar al personal operativo y Directivo en el buen uso de las tecnologías de la información y comunicación, para promover el buen uso, resguardo y custodia de la información que se genera en la aplicación de la política pública que al interactuar con nuestros beneficiarios generamos información y resguardo de datos personales.

NORMATIVIDAD APLICABLE
Constitución Política de los Estados Unidos Mexicanos
Constitución Política del Estado de Guanajuato
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
Ley de Responsabilidades Administrativas para el Estado de Guanajuato
Código de Ética del poder ejecutivo
Lineamientos de Tecnologías de la Información y Telecomunicaciones de la Administración Pública Estatal
Lineamientos Generales de Control Patrimonial de la Administración Pública Estatal

Por lo expuesto y fundado en las disposiciones legales citadas, he tenido a bien expedir los siguientes:

Lineamientos de Informática del Instituto Guanajuatense para las Personas con Discapacidad

A C U E R D O

Artículo único. Se expiden los Lineamientos de Informática del Instituto Guanajuatense para las Personas con Discapacidad para quedar en los siguientes términos:

CAPITULO I
Disposiciones Generales

Objeto de los lineamientos

Artículo 1. Los presentes lineamientos tienen por objeto establecer los mecanismos que permitan la correcta administración de la seguridad, protección de datos, uso de equipo de cómputo, red institucional y sistemas de información implementados para obtener una mejor eficiencia en el trabajo y garantizar la cadena de custodia de la información de nuestros beneficiarios.

Glosario

Artículo 2. Para efectos de estos lineamientos, se entiende por:

Glosario de términos:

I. **Activo informático**. Son todos los recursos de Hardware y Software que forman parte del entorno de trabajo y son propiedad del Instituto.
II. **Acceso Remoto**. Es el acceso a sistemas informáticos desde otra red (comúnmente vía internet) para operar los sistemas como si estuvieran físicamente conectados a la red local.
III. **Aplicaciones en la Nube**. Son sistemas de software que se utilizan vía Internet sin la necesidad de descargarlos o instalarlos físicamente en el equipo.
IV. **Antivirus**. Software que permite proteger nuestros equipos contra daños ocasionados por virus informáticos.
V. **Beneficiario**: Persona que recibe en forma directa la atención médica o psicológica.
VI. **BIOS**. El BIOS (sistema básico de entrada / salida, por sus siglas en inglés), es el software integrado como chip en las computadoras portátiles y de escritorio el cual es responsable de que se pueda iniciar correctamente nuestro sistema.
VII. **Coordinación de Informática**. La Coordinación de Informática del Instituto, es el área encargada de administrar los recursos informáticos y de telecomunicaciones que contribuyen al desempeño de las actividades laborales del personal del instituto.
VIII. **Copias ilegales de Software**. Software que se obtiene por diversos medios pero que no cuenta con licencia para ser utilizado.
IX. **Correo SPAM**. Información no solicitada que se distribuye masivamente por correo electrónico y proviene de remitentes o fuentes desconocidas.
X. **Cuota de Espacio**. Es el límite en la capacidad de almacenamiento en el servidor establecido por el administrador del sistema para cada usuario de la red.
XI. **Equipo de cómputo**. Computadora portátil o de Escritorio asignada al usuario para el desempeño de sus actividades laborales.
XII. **Estructura de Carpetas**. Forma en que se organizan carpetas y archivos en una computadora, la cual se compone por carpetas principales, subcarpetas y archivos, esto con la finalidad de mantener un mejor orden en el manejo de la información almacenada en los equipos.
XIII. **Firewall**. Es un dispositivo de hardware o software que tiene como finalidad mantener la seguridad de la red. Incluye un conjunto de instrucciones configurables que le permiten decidir si permite o bloquea ciertos flujos de información o conexiones desde la red local hacia internet y viceversa.
XIV. **Gestor de descargas**. Es un tipo de software para programar y realizar descargas de grandes volúmenes de información de internet de manera automática sin necesidad de monitoreo permanente por parte del usuario.

XV. **Hardware**. Son todos los elementos físicos que constituyen una computadora o un sistema informático. Es decir, sus componentes eléctricos, electrónicos, electromecánicos, mecánicos y cualquier elemento físico que esté involucrado.

XVI. **Helpdesk**. Es un sistema informático también llamado "Mesa de Servicio" que tiene como finalidad atender de manera organizada las solicitudes de servicio que realizan los usuarios.

XVII. **Herramientas de Filtrado Web**. Conjunto de instrucciones que permiten o bloquean el acceso a determinadas páginas web ya sea por grupo de páginas o por páginas web individuales.

XVIII. **Instituto**. Instituto Guanajuatense para las Personas con Discapacidad.

XIX. **Licencias de uso de software**. Es la autorización que otorga un autor o empresa que permite a terceras personas utilizar software de su propiedad bajo las condiciones o políticas de uso que el autor o la empresa establezcan.

XX. **Navegación Anónima**. Es la posibilidad de acceder a sitios web sin que se pueda identificar a la persona o el equipo que esté accediendo a determinados servicios vía internet.

XXI. **PBX**. Es el equipo que permite interconectar las líneas de telefonía y administrar el servicio de llamadas telefónicas entre los usuarios.

XXII. **Perfil de Navegación**. Determina los sitios permitidos y de acceso denegado de acuerdo a las actividades laborales de cada usuario.

XXIII. **Privilegios de Acceso**. Son las actividades que un usuario tenga permitidas en el uso de un sistema informático tales como editar, eliminar, o modificar configuraciones que puedan afectar el correcto funcionamiento de los sistemas.

XXIV. **Programas Portables**. Son programas informáticos (software) que no requieren ser instalados en el equipo para poder utilizarlos.

XXV. **Respaldo de información**. También llamado "Backup", es una copia exacta de los datos importantes de un dispositivo primario (computadora) en uno o varios dispositivos secundarios como servidores o medios de almacenamiento externo.

XXVI. **Red Institucional**. Conjunto de equipos que se encuentran interconectados ya sea por cable o de manera inalámbrica para la transmisión de datos, lo que permite entre otras cosas: navegación en internet, utilización de sistemas administrativos, accesos a impresoras en la red, comunicación de equipos, entre otros.

XXVII. **Riesgo de Seguridad**. Es toda amenaza que tenga como finalidad vulnerar uno o varios activos que afecten el funcionamiento de un sistema, y que pueda llevar derivarse en daños físicos o perdida de información.

XXVIII. **Software**. Es un programa informático, que incluye un conjunto de instrucciones, algoritmos y partes visuales que nos permiten interactuar con nuestros equipos y dispositivos electrónicos para llevar a cabo diversas actividades.

XXIX. **Streaming**. Tecnología que permite reproducir contenido de Audio o Video desde internet u otra red sin tener que descargar previamente los datos al dispositivo desde el que se visualiza y/o escucha el archivo.

XXX. **Spyware**. Es un software que se instala sin consentimiento informado del usuario, ya sea una computadora personal, una aplicación en el navegador web o algún dispositivo móvil con la finalidad de compartir información personal con el atacante.

XXXI. **SITE**. Es el área destinada concentrar y centralizar los equipos encargados de administrar los servicios de red tales como servidores, nodos de la RED, router, switch, etc.

XXXII. **Servidor**. Es un equipo destinado al almacenamiento información y la administración de recursos y servicios de red.

XXXIII. **Switch**. Es un dispositivo de Hardware que se encarga de interconectar los equipos de cómputo para permitir el trabajo en red.

XXXIV. **Servidor NAS**. Servidor de almacenamiento de datos conectado y accesible desde la red local, y destinado principalmente para actividades de respaldo de información.

XXXV. **VPN**. (Vitual Private Netword). Es una red privada virtual que permite crear una conexión de red privada entre dispositivos para la transmisión de datos de manera segura y anónima por medio de Internet.

XXXVI. **USUARIOS**. todo el personal del Instituto y todas las personas relacionadas con la institución que hagan uso de los servicios, infraestructura de tecnologías de la información y comunicación.

Objetivo General de los Lineamientos

Artículo 3. Establecer medidas preventivas y de seguridad, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos institucionales aprovechando la tecnología y mecanismos de control físico y tecnológico que aseguren el correcto uso de la tecnología y protección de datos.

Objetivos Específicos de los Lineamientos

Artículo 4. Son objetivos específicos de estos lineamientos:

I. Promover el acceso pleno a los Derechos Humanos de las Personas con Discapacidad
II. Promover los Derechos de los Jóvenes con Discapacidad
III. Establecer medidas de seguridad para la salvaguarda de información y datos personales de los beneficiarios
IV. Asegurar que las unidades administrativas apliquen las medidas y controles de acceso a información para el resguardo y custodia de datos sensibles de nuestros beneficiarios.

Capitulo II
Alcance

Alcance de los lineamientos

Artículo 5. Los presentes lineamientos emitidos con apoyo de la Coordinación de Informática, son aplicables a todo el personal del Instituto, usuarios, y a todas las personas relacionadas con nuestra institución, que hagan uso de los servicios e infraestructura de Tecnologías de la Información y Comunicación.
La inobservancia, de los presentes lineamientos será causal de las responsabilidades administrativas, civiles o penales que correspondan atendiendo a mal uso o extracción de información sensible.

CAPITULO II

Sección Primera
Bienes Informáticos y Software

Activo Informático

Artículo 6. 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.
La coordinación de informática y su personal adscrito, son los únicos autorizados para implementar acciones para el correcto funcionamiento de los equipos de tecnologías de la información y comunicaciones, ya sean actividades preventivas o correctivas de igual forma la Coordinación de Control Patrimonial y Servicios Generales es la responsable de la asignación, registro de bienes, así como la salida fuera de las instalaciones del Instituto en periodos no laborales.

Queda estrictamente prohibido para todos los usuarios utilizar herramientas de hardware o software de uso exclusivo del área de Informática, tales como analizadores de red, escaneo de puertos, monitoreo de red, auditoría de contraseñas, etc.

Clasificación de la Información Digital

Artículo 7. Los Directores, Coordinadores y jefes de área que tengan personal a cargo informaran a sus colaboradores de la clasificación de la información digital a su cargo para su adecuado tratamiento, conforme a los Programas, Reglas de operación, Lineamientos, Manuales de Archivo, Cuadro de Clasificación Archivística y Lineamientos establecidos para ello.

Resguardo de Información

Artículo 8. 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.

Así mismo 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 del titular de los datos.

Acceso a información restringida

Artículo 9. Todos los usuarios que hacen uso de información clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas.

Solución Antivirus y Firewall

Artículo 10. Todo equipo de cómputo institucional debe contar con solución antivirus y un firewall administrado por el personal de la Coordinación de Informática, con el objetivo de proteger el equipo de programas maliciosos, mismos que serán definidos por la coordinación.

Mesa de Servicio Helpdesk

Artículo 11. Todo Usuario que identifique una anomalía en su equipo de cómputo deberá reportarla a la coordinación de informática mediante sistema de mesa de servicio (Helpdesk), misma que será atendida en el orden que le corresponda de acuerdo al ticket asignado y a la prioridad que será definida por el personal de informática.

No se atenderá ninguna solicitud de servicio que se haga llegar de manera verbal, telefónica o correo electrónico, si esta no se encuentra debidamente capturada en el portal dispuesto para ello por parte de la coordinación de informática en el siguiente link: http://soporteingudis.gob.mx/glpi

De la Solicitud de refacciones y accesorios

Artículo 12. La solicitud de refacciones y accesorios de equipo de cómputo debe contar con el visto bueno y autorización de la Coordinación de Informática.

Únicamente personal autorizado por la coordinación de Informática, está facultado para abrir los gabinetes de las computadoras personales o de cualquier otro equipo de cómputo propiedad del Instituto.

Autorización para conexión a red de equipos personales

Artículo 13. Para conectar una computadora a la red Institucional que no esté bajo el control administrativo del Instituto (computadoras personales), se deberá solicitar autorización a la coordinación de Informática para que ésta inspeccione el equipo y compruebe que no constituye un riesgo para la seguridad de la Institución.

Los equipos de cómputo de carácter personal solo tendrán acceso al servicio de internet y a las impresoras institucionales, en ningún momento se les proporcionará el servicio de mantenimiento preventivo y/o correctivo.

Del fondo de pantalla

Artículo 14. Todas las computadoras conectadas a la red del Instituto contarán obligatoriamente con un fondo de pantalla definido por la Coordinación de Comunicación Social, quien definirá la temática a difundir, a fin de perseverar la imagen institucional.

Sección Segunda
Sobre el uso de software

Administración de Software

Artículo 15. La Coordinación de Informática, es la única área autorizada para llevar a cabo la administración del software del Instituto, por lo que dentro de sus responsabilidades tiene:

I. Mantener bajo resguardo las licencias de uso de software.
II. Llevar un control exacto de las licencias en operación y el equipo en el cual se encuentra en uso.
III. Establecer lineamientos para el uso de software, previa aprobación por parte de la Dirección Administrativa.
IV. Realizar un análisis de necesidades y requerimientos de software, con la finalidad de presentárselo a la Dirección Administrativa, quien autorizará la adquisición.

La Coordinación de Informática es el área responsable, de realizar la instalación del software y de proporcionar soporte del mismo en todas las computadoras de la Institución.

Software institucional

Artículo 16. La Coordinación de Informática determinará en base al análisis de necesidades y de acuerdo a las actividades de cada área, un estándar de software para ser utilizado por las áreas usuarias. Todo equipo de cómputo nuevo o que se haya ingresado a mantenimiento, antes de ser entregado al usuario final deberá contar con dicho software, que es considerado Software Institucional. Así mismo existe software adicional utilizado para el desarrollo de soluciones automatizadas y que es de uso exclusivo del personal de Informática, mismo que podrá ser incluido de manera temporal o permanente en los equipos de los usuarios según se requiera.

Software no autorizado

Artículo 17. Queda estrictamente prohibido que el usuario instale sin autorización, copias ilegales de cualquier programa, software descargado de Internet, software que no sea identificado como Institucional, ni software adquirido para uso personal o recreativo (sin fines institucionales). Si al ingresar un equipo a mantenimiento o durante las revisiones periódicas llevadas a cabo por el personal de Informática, se detectara la presencia de software no autorizado, éste será desinstalado del equipo sin necesidad de autorización por parte del usuario.

Si algún usuario requiere determinado software instalado en su computadora que no esté incluido en el estándar definido por la Coordinación de Informática, deberá solicitarlo mediante el portal de mesa de servicio (helpdesk), donde también deberá adjuntar un documento donde justifique la necesidad y que incluya el visto bueno de su jefe inmediato.

Software portable

Artículo 18. Queda estrictamente prohibido el uso de programas portables en los equipos propiedad del Instituto sin previa autorización de la Coordinación de Informática.

Aplicaciones en la nube

Artículo 19. La utilización de aplicaciones en la nube tales como agenda, calendario, documentos, hojas de cálculo, etc., es responsabilidad del usuario, jefe de área o coordinador que autorice su uso entre su personal, no responsabilizando al área de Informática del Instituto por el soporte o perdida de información generada por este tipo de software.
Se deberá notificar al Coordinación de Informática la existencia y utilización de software que sea enviado por parte de cualquier organismo ajeno al Instituto, así como entregar una breve descripción de la función, requerimientos de hardware y utilización de éste.

Sección Tercera
Sobre el Uso de Internet

Servicios de Internet

Artículo 20. Los servicios de acceso a Internet y Correo Electrónico son administrados por la Coordinación de Informática. Sin embargo, el proveedor del servicio de Internet es responsable de garantizar la disponibilidad del mismo, así como de los anchos de banda y velocidad contratados.

Monitoreo de los Accesos a Internet

Artículo 21. La Coordinación de Informática tendrá la facultad de monitorear periódicamente los accesos a Internet de cada uno de los usuarios con la finalidad de vigilar el cumplimiento de los lineamientos internos del presente documento, manteniendo la confidencialidad de la información.
El servicio de Internet es considerado como herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para actividades que contribuyan al cumplimiento de objetivos y metas del Instituto.
Todos los jefes de área pueden solicitar la restricción total o parcial de acceso a Internet del personal a su cargo con el fin de eficientar el uso de los recursos de TIC.

Filtrado de acceso

Artículo 22. La Coordinación de Informática podrá implementar herramientas de filtrado para restringir el acceso a sitios de internet que no tengan relación con el trabajo o que se consideren inseguros.

Del Streaming

Artículo 23. Queda estrictamente prohibido la reproducción de música o videos en línea (también llamado streaming), ya que ello provoca una disminución considerable en la velocidad del internet, lo cual afecta las actividades laborales de los usuarios que dependen de este servicio.

Los usuarios con equipos personales que por alguna razón necesiten conexión a Internet tendrán que solicitarlo a la Coordinación de Informática para su configuración en caso de que proceda la solicitud.

Uso y Distribución del internet

Artículo 24. Queda prohibido utilizar cualquier medio ya sea por software o en línea que tenga como finalidad navegar de forma anónima, tal es el caso de ventanas de incognito o servicios de VPN dispuestos para tal fin.
No se deberá utilizar el acceso a Internet como un medio de acceso y distribución de materiales o actividades que vaya en contra de las actividades del Instituto.
La Coordinación de Informática asignará a cada usuario acceso a Internet con un perfil de navegación de acuerdo a las actividades que le correspondan, como resultado de esto, el usuario:

I. Tendrá bloqueado automáticamente el acceso a páginas con contenido ofensivo o malicioso para el Instituto, o que simplemente resulten innecesarias para el trabajo.
II. Deberán solicitarlo vía portal (helpdesk) adjuntando documento de justificación autorizado por su jefe inmediato para el acceso a plataformas de redes sociales, páginas de internet o alguna otra plataforma que se requiera para el cumplimiento de las actividades.
III. Los usuarios no podrán redistribuir el servicio de internet del Instituto por cualquier medio, así como difundir servicios personales de red inalámbrica dentro del Instituto.

Gestores de descargas

Artículo 25 Queda prohibido para los usuarios la utilización de gestores de descargas o cualquier otro medio que tenga como finalidad la descarga masiva y excesiva de información, ya sea audio, video o software sin contar con la autorización de la Coordinación de Informática.

Sección Cuarta
Sobre el Correo Electrónico

Del correo Electrónico

Artículo 26. El correo electrónico institucional es para uso exclusivo del personal activo del Instituto, y éste deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.
El medio para el envío y recepción de correo electrónico será determinado por la Coordinación de Informática, esto con la finalidad de tener una mejor administración de la información que circule por este medio.

Modificación al Correo

Artículo 27. Toda solicitud de alta, baja o cambio de correo institucional, debe ser solicitado por el jefe de área mediante el sistema de mesa de servicio (helpdesk) adjuntando el formato proporcionado por el área de informática el cual deberá ir debidamente llenado con los datos del usuario.

Del Spam

Artículo 28. Queda prohibido utilizar el correo electrónico institucional para envíos de correo basura (spam), cadenas, mercadotecnia, religiosos, propaganda política, actos agresivos e ilegales y cualquier otro contenido que no tenga relación con el trabajo.

Responsabilidad de usuarios del correo

Artículo 29. El contenido de los mensajes enviados es responsabilidad del usuario, esto incluye entre otros: Contenido de material ofensivo u obsceno, cualquier quebrantamiento de propiedad intelectual, copyright o cualquier información ilegal que afecte la imagen e integridad del instituto.
El envío de correos electrónicos masivos, deberá solicitarse a la Coordinación de Informática mediante el formato dispuesto para ello.

Reportes del correo electrónico

Artículo 30. Es responsabilidad de los usuarios de correo electrónico institucional, notificar al personal de Informática cuando tenga la sospecha de uso o acceso no autorizado de su cuenta.
Toda persona que termine relación laboral con el Instituto, se le inhabilitará su cuenta de correo sin que se le genere un respaldo del mismo.

Sección Quinta
De la red de datos

Uso de la Red de Datos

Artículo 31. La persona usuaria que necesite acceso a la red de datos cableada deberá solicitar autorización a la Coordinación de Informática mediante una orden de servicio. El equipo de cómputo que forma parte de la red de datos institucional no deberá tener instalado software malicioso de conexión punto a punto o catalogado como Sniffer, proxys etc., en virtud de que comprometen la integridad y seguridad de esta.
El equipo de cómputo deberá contar con dispositivos de conectividad como tarjetas de red y adaptadores, estos accesorios no serán proporcionados por la Coordinación de Informática, en todo caso, deberá remitirse a los procedimientos señalados para la adquisición de refacciones de equipos.

Disponibilidad de la infraestructura de red

Artículo 32. La persona usuaria no deberá desconectar de la red de datos equipos en uso de las áreas operativas del Instituto, para conectar su equipo personal.
El servicio de red local estará sujeto a disponibilidad de la infraestructura de la red.

Solicitud de servicio de red

Artículo 33. El servicio de internet se proporcionará a usuarios internos; en caso de requerir el servicio para personas externas, el área solicitante deberá realizar la solicitud por el jefe de área mediante el sistema de mesa de servicio (helpdesk) adjuntando el formato proporcionado por el área de informática el cual deberá ir debidamente llenado con los datos del usuario.

De las configuraciones de red

Artículo 34. Queda estrictamente prohibido que las personas usuarias modifiquen configuraciones, alteren la funcionalidad y traten de acceder a otros equipos ajenos a los de su área mediante la red de voz y datos del Instituto, el personal que sea sorprendido se reportará al Órgano Interno de Control y a la Coordinación Jurídica, para la aplicación de la sanción que corresponda. El personal de la Coordinación de Informática es el único autorizado para realizar configuraciones en dicha red.

Sección Sexta
Sobre el Respaldo de Información

De la propiedad de archivos, sistemas y aplicaciones

Artículo 35. Todos los usuarios que utilizan equipo de cómputo propiedad del Instituto deben estar conscientes de que los datos que ellos crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico durante el desarrollo normal de sus actividades laborales, son propiedad del Instituto.

De los respaldos

Artículo 36. La Coordinación de Informática determinará los medios y periodicidad de los respaldos de los equipos ya sea de forma manual o automatizada, ya sea en servidor NAS o en el servicio de nube privada del Instituto.

Solo se respaldará la estructura de carpetas que determine la Coordinación de Informática tomando como base las carpetas que se integran por default en cada perfil de usuario como son **Escritorio, Documentos, Imágenes y videos (no se incluye la carpeta de Descargas)**. Dentro de estas carpetas base se permitirá como máximo 3 subcarpetas donde ser recomienda empezar por el año, ejemplo:

<Usuario>\Escritorio\2022\Control Interno\Actividades de control\<Nombre del Archivo>

Se permiten solo 3 sub carpetas ya que a medida que se van generando más de estas sub carpetas, se incrementa considerablemente el nombre de los archivos, lo cual impide que se generen correctamente los respaldos al omitir información por exceder en número de caracteres permitidos.

La pérdida de cualquier información contenida en los equipos fuera de las carpetas que se tengan contempladas para respaldo será responsabilidad del usuario. La Coordinación de Informática no se responsabiliza por la información que no fuera posible respaldar por exceder el número de caracteres permitidos para nombres de archivos.

Exclusión de respaldos

Artículo 37. No se incluirán en los respaldos archivos de música, videos o software propiedad del usuario que no estén relacionados con el trabajo, y no se podrá responsabilizar a la Coordinación de Informática por la pérdida de estos durante el proceso de respaldo.

Responsabilidad de usuarios sobre respaldos

Artículo 38. Es responsabilidad exclusiva de los usuarios solicitar acceso para revisar periódicamente la integridad de sus respaldos en los medios que designe la Coordinación de Informática.

Respaldos en la nube

Artículo 39. La Coordinación de Informática no se responsabiliza por la pérdida de información que se respalde en cualquiera de los servicios que se ofrecen en la nube (Gmail el más utilizado), por lo que el usuario deberá incluir copia de esa información en los medios dispuestos para ello por parte del área de Informática.

Servidor NAS

Artículo 40. Para los usuarios o áreas que requieran espacio en el servidor de almacenamiento de red (NAS), la cuota de espacio será determinada por el área de informática en base a las actividades de cada usuario o área.

Solicitud de espacio en la nube

Artículo 41. Todos los usuarios que requieran de espacio en la nube privada del Instituto deberán solicitarlo mediante el formato proporcionado por la Coordinación de Informática, mismo que deberá ser autorizado por el jefe inmediato y por la Dirección Administrativa del Instituto.

Sección Séptima

Sobre Seguridad Informática y uso de contraseñas

Identificación de equipos en la red

Artículo 42. Todos los equipos de cómputo ya sea portátiles o de escritorio, deberán tener una nomenclatura que permita identificarlos dentro de la red local de cada uno de los edificios del Instituto (CEDDIS, CEREVI, CER, CAIJ). De igual manera, todos los equipos de cómputo ya sea portátiles o de escritorio, deberán contar con un perfil de usuario que permita identificar de forma única a un usuario individual y se le aplicarán políticas de seguridad para que la información que genere con su perfil sea inaccesible por otros usuarios desde la red o incluso teniendo acceso físico al equipo.

Bloqueo de equipos inactivos

Artículo 43. Cuando un usuario se vea en la necesidad de abandonar su puesto de trabajo, deberá bloquear su equipo de forma obligatoria de manera que únicamente el usuario pueda volver a activarlo mediante su contraseña personal.

De igual forma los equipos portátiles o de escritorio que presenten inactividad por un periodo de tiempo previamente determinado por el área de Informática, se protegerán en automático mediante el protector de pantalla que se menciona en el Artículo 14 de los presentes lineamientos.

De los requisitos de seguridad

Artículo 44. Todos los usuarios internos del Instituto requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo que tengan asignado y ésta deberá cumplir con los requisitos de seguridad definidos por la Coordinación de Informática y que se indican en los presentes lineamientos, así como los privilegios otorgados a cada cuenta o perfil de usuario.

De las contraseñas

Artículo 45. Se deberá utilizar contraseñas de entre 64 y 128 bits, las cuales deben contar una longitud mínima de 8 caracteres imprimibles sin espacios (se recomiendan 16) y deberán construirse considerando lo siguiente:

I. Debe contener letras mayúsculas y minúsculas.
II. Debe contener por lo menos un número del 0 al 9
III. Incluir mínimo uno de estos caracteres: ¡@#$%^&*() _+|~- \` { }[ ]:";'<>?,./)
IV. No deben ser predecibles, y en particular no deben ser fácilmente asociadas con el usuario, tales como
V. nombres o iniciales, referencias de su edificio de adscripción, meses del año, u otros criterios de fecha.
VI. No utilizar números de teléfono.

Los usuarios deberán cambiar sus contraseñas por lo menos cada tres meses, según lo determine la Coordinación de Informática.

Seguridad en las contraseñas

Artículo 46. Todas las contraseñas de acceso a los equipos de cómputo, sistemas y servicios de red e Internet del Instituto, son personales y no deben ser reveladas a terceros para actividades ajenas al Instituto.

Sección Octava

Salida de equipos fuera de oficinas

Protección de Activos Informáticos

Artículo 47. Todo equipo portátil que por actividad laboral tenga que salir del edificio deberá contar con el conocimiento de su jefe inmediato, adicional a ello deberá contar con contraseña de protección de arranque del BIOS y protección de acceso al disco duro para la protección de información y no sea sustraída para fines distintos, de igual forma, será responsabilidad del usuario solicitar esta medida de protección a la Coordinación de Informática del Instituto.

Respaldo de Activos Informativos

Artículo 48. Es responsabilidad de cada usuario asegurarse de que los equipos que salgan de oficina estén debidamente respaldados de acuerdo a lo indicado en los presentes lineamientos.

Notificación por Pérdida o Robo

Artículo 49. En caso de robo o extravío de equipos fuera de oficina, se deberá notificar de inmediato al área de Informática y al área de control patrimonial para la implementación de acciones ante el Seguro de bienes patrimoniales, y bloqueo a distancia de equipos.

Sección Novena
Acceso Físico a Sistemas Informáticos

Acceso físico a equipos de TIC

Artículo 50. Todo el equipo activo de Tecnologías de la Información tales como servidores, switches, PBX y equipo en general pasa uso exclusivo del área de Informática, estará centralizado en una misma denominada SITE.

Acceso a SITES

Artículo 51. Las áreas de SITE en los edificios de CER, CEREVI, CAIJ y Oficinas Centrales del Instituto, son de acceso restringido al personal de Informática, y será la Coordinación de Informática en coordinación con los enlaces administrativos de cada edificio, quien pueda autorizar el acceso de personal ajeno al área el cual deberá quedar debidamente documentado en las Bitácoras de Acceso donde se indicará entre otras cosas, la fecha, hora y el motivo por el cual se permitió el acceso.

Los privilegios de acceso a sistemas informáticos y equipos de cómputo serán controlados de acuerdo a las políticas implementadas en servidores y equipos de seguridad (Firewall) que la Coordinación de Informática haya dispuesto para este fin.

Sección Decima
Acceso remoto a Sistemas Informáticos

De la solicitud para acceso a servicios administrados por terceros

Artículo 52. Cualquier usuario que requiera acceso remoto a equipos, servidores o nube privada del Instituto, para actividades administrativas y operativas, deberá solicitarlo mediante el portal de helpdesk que la Coordinación de Informática haya dispuesto para recibir solicitudes de servicio, donde deberá adjuntar el formato de solicitud debidamente llenado y con la firma de autorización del área correspondiente, comúnmente la Dirección Administrativa.
A los usuarios que cuenten con servicio de acceso remoto, se les asignara una cuenta de usuario y contraseña siguiendo los lineamientos que se indican en los Artículos 44 y 45 de los presentes lineamientos.

Acceso SAP 4HANA

Artículo 53. Todos los accesos remotos a sistemas SAP 4HANA y equipos, se realizarán mediante la VPN con usuario Instituto, exclusivamente, utilizando de ser posible autenticación de usuario de dos factores, cuando se compartan contraseñas del sistema SAP 4HANA es conveniente que los usuarios si en el primer intento no logran el acceso deberán notificarlo a efecto de evitar el bloqueo total del usuario original del sistema.

Actualización de contraseñas de SAP 4HANA

Artículo 54. La utilización de software de acceso remoto de terceros, para actividades Administrativas, Contables y de control patrimonial, los cuales deban cumplir con un proceso o registro, el usuario se gestionará a través de la Coordinación de informática en el formato dispuesto por el proveedor de servicios y la contraseña será responsabilidad del usuario original para la actualización de manera mensual, debiendo notificar a los usuarios con los que comparte su uso para evitar el bloqueo del mismo.

Sección Décima primera
De los Planes de Contingencia

Respaldo de información en sistemas

Artículo 55. Con el fin de prevenir pérdida de información, la Coordinación de Informática es responsable de realizar los respaldos periódicamente de la base de datos y de los sitios que incluyen los módulos de SITAI, SICI y Almacén, así como de la página web institucional y software utilizado por la coordinación de informática para fines administrativos, todo acorde con el plan de respaldos de la base de datos.

De sistemas de seguridad

Artículo 56. Es responsabilidad la Coordinación de Informática verificar que existan los extintores adecuados en cada sitio de comunicación con el fin de activar el plan de contingencia en caso de incendio en las instalaciones del Instituto.

Del plan de contingencia por evento

Artículo 57. En caso de presentarse algún siniestro en las instalaciones del Instituto, la Coordinación de Informática deberá activar los planes de contingencia necesarios para el restablecimiento de los servicios acorde con alguno de los siguientes eventos:
a) Falla de software.

- Si la falla es de algún software instalado y se cuenta con acceso a internet, solicitar apoyo mediante el portal de helpdesk como se indica en el Artículo 11 de los presentes lineamientos. Mientras tanto, Iniciar y utilizar la **máquina virtual** para continuar trabajando mientras se da solución al problema por parte del área de Informática.
- Si la falla es del navegador web o no se cuenta con servicio de internet en el equipo, solicitar apoyo a algún compañero de trabajo para que les pueda prestar su equipo y solicitar el servicio mediante el portal de helpdesk.
- Si se presenta la falla en algún equipo portátil fuera de nuestras instalaciones, solicitar apoyo a la coordinación de Informática para recibir soporte ya sea vía telefónica o por acceso remoto.
- Si se trata de falla del sistema operativo (Windows no inicia) notificarlo de inmediato a la coordinación de informática para restablecer el sistema lo antes posible. De ninguna manera intentar repararlo sin autorización alguna ya que se podría dañar el sistema de archivos y dejar irrecuperable la información contenida en el equipo.

b) Siniestro.

- Notificar de inmediato vía telefónica o WhatsApp a la coordinación de Informática para que ponga en marcha (si se cuenta con el) el mecanismo de bloqueo y protección de la información, así como el posible rastreo de la ubicación del equipo.
- Solicitar el acceso al respaldo de información del usuario ya sea para consulta o para ser copiado a algún equipo que le haya sido asignado de manera temporal.

c) Falla de servidor.

- En caso de falla del servidor central, la coordinación de Informática pondrá en marcha el servidor secundario que contendrá una copia exacta de aplicaciones e información contenida en el servidor primario a fin de mantener la continuidad y operatividad de las actividades laborales de nuestro personal.
- En caso de falla en el servidor de alguno de los edificios, **la coordinación de informática** pondrá en marcha el servidor virtual secundario dispuesto para estos casos.
- Si el servidor de oficinas centrales o de alguno de los edificios queda temporalmente inutilizable, se ejecutará en algún equipo de oficina, un servicio virtual que contenga lo mínimo para mantener la operatividad en el edificio mientras se soluciona el problema del servidor físico.

d) Falla de energía eléctrica.

- Si el problema es que la energía electica es inestable, desconectar el equipo de SITE (servidores, switches, pbx, routers) y notificarlo al área de informática. (quien lo desconectara y con autorización de quien, con autorización escrita, verbal, llamada telefónica o correo electrónico) esto en atención a lo manifestado en numeral 51 de los presentes lineamientos.
- Si el problema fue interrupción de energía, notificarlo al área de informática una vez que se restablezca el servicio, a fin de que la coordinación les de las instrucciones correctas para restablecer la operación de los equipos de red.

e) Falla en el servicio de telefonía.

- Notificarlo al área de Informática, quien se encargará de diagnosticar el problema y le dará solución de ser posible.
- Si el área de Informática dictamina que la falla no es reparable internamente, reportar el problema al servicio de soporte de la compañía telefónica.

f) Falla en el servicio de internet.

- Si alguno de los edificios interconectados (CEDDIS, CER, CEREVI) se queda sin servicio de internet, notificarlo vía telefónica o WhatsApp a la coordinación de informática a fin de que habilite el servicio compartido mediante el sistema de interconexión con el que se cuente (inalámbrico o fibra óptica), esto mientras se restablece el servicio por parte del proveedor de servicios de internet (ISP).
- Si se presenta falla en el servicio de internet en un edificio no interconectado (CAIJ en este caso), notificarlo al área de informática y al mismo tiempo, reportarlo al servicio de soporte del proveedor de servicios de internet (ISP). Si hay disponibilidad del usuario y se encuentra en un caso de extrema urgencia para envío o recepción de información importante, solicitar apoyo al área de Informática para que brinde asesoría en compartir el servicio de datos de telefonía celular a su equipo de cómputo.

Sección Décima Segunda
Sanciones

De la notificación de la Sanción

Artículo 58. En caso de que personal del Instituto, usuarios y cualquier persona relacionada con nuestra institución, que hagan uso de los servicios e infraestructura de tecnologías de información y comunicación cometa una falta, la Coordinación de Informática, podrá realizar la notificación al Órgano Interno de Control del Instituto a efecto de que se apliquen las sanciones correspondientes de acuerdo a sus atribuciones y alcances atendiendo a la ley de responsabilidades administrativas para el estado de Guanajuato y a los demás ordenamientos aplicables y vigentes.

Tipos de sanción

Artículo 59. Las sanciones que podrán aplicarse a quienes violen las disposiciones de este Instrumento o cometan daños o cualquier acto sancionado y relacionado con los servicios de informática, son:

a) Llamada de atención verbal.
b) Llamada de atención escrita.
c) Suspensión temporal del servicio.
d) Suspensión definitiva del servicio.

e) Las que dicten las autoridades correspondientes, en función de la gravedad de la falta cometida, atendiendo a la legislación de la materia.

Aplicación de Sanciones

Artículo 60. las sanciones podrán ser aplicadas de inmediato por la persona titular de la Coordinación Jurídica del Instituto, quien las registrará y reportará al expediente personal de la persona infractora, corriendo traslado a la Coordinación de Recursos Humanos y jefe inmediato.

Notificación al Órgano Interno de Control

Artículo 61. las faltas cometidas a los presentes lineamientos que cometan las personas usuarias y todas las personas relacionadas con nuestra institución, que hagan uso de los servicios e infraestructura de tecnologías de la información y comunicación, serán reportadas a la persona titular del órgano interno de control para determinar la existencia o inexistencia de faltas administrativas contempladas en la ley de responsabilidades administrativas para el estado de Guanajuato, así como calificar la falta e iniciar el procedimiento administrativo correspondiente. independientemente de las sanciones señaladas en el artículo 59 de estos lineamientos.

Suspensión temporal de Servicios

Artículo 62. La acumulación de dos llamadas de atención verbal y/o escrita por una persona usuaria, ameritará la suspensión temporal del servicio informático.
La suspensión temporal a una persona usuaria podrá contemplar de 1 a 3 días y se le comunicará por escrito impidiendo sus actividades.

Suspensión definitiva de Servicios

Artículo 63. La persona usuaria será suspendida definitivamente de los servicios informáticos de acuerdo con los siguientes criterios:
a) Reincidencia en el mal comportamiento.
b) Daños o alteraciones a las instalaciones materiales y/o equipos ocasionados con dolo o negligencia.
c) Robo de material y/o equipo.
d) Conducta inapropiada.

Transitorios

PRIMERO. Las situaciones no previstas en los presentes lineamientos serán presentadas ante la Dirección General del Instituto Guanajuatense para las Personas con Discapacidad.

SEGUNDO. Los presentes lineamientos entrarán en vigor al día siguiente de su aprobación.

TERCERO. Una vez que entren en vigor los presentes lineamientos difúndase en el correo y la página web del Instituto, http://ingudis.guanajuato.gob.mx/.

Aprobado por:

José José Grimaldo Colmenero

Director General del Instituto Guanajuatense

para las Personas con Discapacidad