Lineamientos de administración, operación y seguridad de las Tecnologías de la Información del Instituto Electoral del Estado de Guanajuato

Título primero
Disposiciones generales

Capítulo I
Del objeto y personas sujetas de aplicación

Objeto

Artículo 1. Los presentes Lineamientos tienen por objeto regular la administración y operación de las Tecnologías de la Información, así como las medidas de control para mantener la confidencialidad, integridad y disponibilidad de la información institucional.

Personas sujetas de los Lineamientos

Artículo 2. Los presentes Lineamientos son de observancia general y obligatoria para las personas servidoras que laboren en el Instituto y personas integrantes de partidos políticos al hacer uso de activos de TI de éste, así como personas externas cuando se transmita o comparta información por motivo del ejercicio de sus funciones.

Glosario

Artículo 3. Para los efectos de estos Lineamientos, sin perjuicio de su referencia en plural o singular, se entenderán las siguientes definiciones, siglas y acrónimos:

A. Definiciones

Acceso físico. Principal línea de defensa que se implementa sobre un lugar, para evitar que a este accedan personas no autorizadas.
Acceso lógico. Principal línea de defensa para la mayoría de los sistemas; permite prevenir el ingreso de personas no autorizadas a su información.
Activo. Cualquier información o elemento relacionado con el tratamiento de esta (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) que tenga valor para el Instituto.
Activo crítico de Seguridad de la Información. Todos aquellos recursos que utilizan los sistemas de seguridad de la información, para el cumplimiento de la funcionalidad de operaciones del Instituto.
Activo de información. Recurso de información que generan valor al Instituto por lo que deben protegerse.
Activo tecnológico. Recurso exclusivamente relativo a hardware o sistemas de software que tienen valor para el Instituto.
Acuerdo de confidencialidad y no divulgación. Documento legal celebrado entre el Instituto y su personal, personas integrantes de partidos políticos o personas externas, al compartir material confidencial o conocimiento para ciertos propósitos, restringiendo su uso público.
Amenaza. Causa potencial de un incidente no deseado que puede provocar daños a un sistema o al propio Instituto.

Antimalware. Tipo de programa diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos.
Áreas restringidas. Todas aquellas áreas de este Instituto que por su naturaleza y propósito comprometerían la operación de este si sufrieran algún incidente de Seguridad, tales como la bodega electoral, los IDF, los sites, la cabina de producción y transmisión de la sala de usos múltiples, el espacio de la planta de energía y la bomba hidráulica.
Ataque. Intento de destrucción, alteración, deshabilitación, robo, generación de un acceso no autorizado o uso no autorizado de un activo.
Auditoría. Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas objetivamente, para determinar el grado en el que se cumplen los criterios a revisar.
Autenticación. Provisión de garantía de que una característica afirmada por una entidad es correcta.
Ciberseguridad. Es el área relacionada con la informática y la telemática, que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma.
Comodato. Formato en el cual se da o recibe prestada una cosa de las que pueden usarse sin destruirse con la obligación de restituirla.
Confidencialidad. Propiedad de la información de no ponerse a disposición o ser revelada a personas, entidades o procesos no autorizados.
Control. Políticas, procedimientos, prácticas y estructuras organizativas concebidas, para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. La palabra control es también utilizada como sinónimo de salvaguarda o contramedida.
Control de acceso. Control que asegura que el acceso a activos esté autorizado y restringido, con base en los requerimientos del Instituto y de seguridad.
Control de seguridad. Cualquier tipo de protección o contramedida utilizada para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad de la propiedad física, la información, los sistemas informáticos u otros activos.
Disponibilidad. Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad o personas usuarias autorizadas.
Dispositivo móvil. Aparato portátil de un sistema de telefonía móvil.
Equipo de respuesta. Equipo de respuesta para incidentes en seguridad de la información.
Equipo Terminal. Todo equipo destinado a ser conectado a la red pública de telecomunicaciones capaz de procesar, recibir, conmutar o transmitir señales por medio de conexiones de radio o cable, a través de un punto de conexión terminal.
Evento. Ocurrencia o cambio de un conjunto de circunstancias.
Gestión de incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Grupo Interno de Seguridad de la Información. Grupo de trabajo coordinado por la o el titular de la UTSIT e integrado por las y los titulares de la DDISPE, CA, UT, OIC, así como la persona responsable del Archivo general y las jefaturas de Desarrollo de Sistemas y Telecomunicaciones y Jefatura de Sistemas de Información y Soporte Técnico.

IDF. Por sus siglas en inglés Independent Dristribution Frame, se refiere a conexiones de red en un recinto de comunicación o cuadro de distribución independiente o intermedio, que da apoyo a la estación principal.
Incidente. Evento único o serie de eventos inesperados o no deseados, que comprometen las operaciones diarias del personal del Instituto.
Incidente de Seguridad. Evento único o serie de eventos de seguridad de la información inesperados o no deseados, que poseen una probabilidad significativa de comprometer las operaciones del Instituto.
Instituto. Instituto Electoral del Estado de Guanajuato.
Integridad. Propiedad de la información relativa a su exactitud y completitud.
Inventario de activos. Listado de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) al servicio del Instituto, que tengan valor para este, y necesiten ser protegidos de potenciales riesgos.
Lineamientos. Lineamientos de administración, operación y seguridad de Tecnologías de la Información del Instituto Electoral del Estado de Guanajuato. Criterios de actuación que indican los puntos específicos que deben ser atendidos con base en políticas de seguridad de la información por parte de personas involucradas.
Malware. Todo tipo de código malicioso.
Matriz de riesgos de TI. Herramienta para identificar los riesgos más significativos en materia de Tecnologías de la Información, inherentes a las actividades del Instituto.
Medio físico. Conjunto de elementos materiales que constituyen un sistema.
Medios removibles. Dispositivos de almacenamiento externos.
Mesa de ayuda. Herramienta tecnológica que tiene por objetivo registrar y monitorear las solicitudes de servicio de tecnologías de la información por parte del personal de este Instituto.
Monitoreo. Determinación del estado de un sistema, proceso o actividad.
Personas externas. Todas aquellas personas a las que se les proporciona información del Instituto por motivos laborales, tales como proveedores o consultores.
Política. Documento de alto nivel que define las disposiciones generales sobre una actividad, proceso, o sistema, para guiar y asegurar su adecuado funcionamiento.
Proceso. Conjunto de actividades interrelacionadas o interactuantes que transforman entradas en salidas.
Riesgo. Posibilidad de que una amenaza concreta pueda presentarse para causar una pérdida o daño en un activo de información.
Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información.
Unidades Responsables. Áreas del Instituto que tienen a su cargo la administración de recursos presupuestales, su ejercicio o la ejecución de programas, procesos o proyectos y que se encuentran obligadas a la rendición de cuentas.
Vulnerabilidad. Debilidad de un activo o control que puede presentarse por una o más amenazas.

B. Siglas y acrónimos

CA. Coordinación Administrativa
DDISPE. Dirección de Desarrollo Institucional y Servicio Profesional Electoral
GISI. Grupo Interno de Seguridad de la Información.
IDF. Independent Dristribution Frame, en español recinto de distribución independiente.
JEE. Junta Estatal Ejecutiva.
OIC. Órgano Interno de Control
SLAs. Service Level Agreement, en español Acuerdo de nivel de servicio o Garantía de nivel de servicio.
TI. Tecnologías de la Información.
UR. Unidades Responsables.
UT. Unidad de Transparencia.
UTSIT. Unidad Técnica de Sistemas de Información y Telecomunicaciones.

Capítulo II
Grupo Interno de Seguridad de la Información

Objeto e integración

Artículo 4. El Grupo Interno de Seguridad de la Información, es el órgano conformado por la o el titular de la UTSIT, e integrado por las y los titulares de la DDISPE, CA, UT, OIC, así como la persona responsable del Archivo general y las jefaturas de Desarrollo de Sistemas y Telecomunicaciones y Jefatura de Sistemas de Información y Soporte Técnico.

Atribuciones generales

Artículo 5. Se entenderán como atribuciones generales del GISI:

I. Vigilar la correcta aplicación y cumplimiento de los presentes Lineamientos, como las atribuciones específicas previstas en la Política Digital y Política de Seguridad de la Información, de este Instituto, así como de efectuar las modificaciones o adecuaciones que se consideren necesarias para tal efecto;
II. Dar cumplimiento a las disposiciones previstas por las leyes generales y locales en materia de TI, con el fin de evitar el mal uso de ella y dar certeza sobre el actuar del Instituto;
III. Crear, mantener, difundir, concientizar y vigilar la aplicación de estos Lineamientos en todos los niveles de la estructura orgánica del Instituto, y
IV. Sesionar de acuerdo con lo previsto en las Reglas de operación del Grupo Interno de Seguridad de la Información, del Instituto.

Título segundo
De los activos tecnológicos

Capítulo I
Del inventario de activos

Gestión del inventario de activos

Artículo 6. Respecto al Inventario de activos, la UTSIT deberá:

I. Generar un inventario de activos de TI y activos críticos de Seguridad de la Información, que contenga:

   a. Responsables.
   b. Marca.
   c. Modelo.
   d. Número de serie.
   e. Tipo de activo.
   f. Descripción del activo.
   g. Dirección IP.
   h. Clasificación.
   i. Dependencias con otros activos.
   j. Ubicación física.
   k. Cargo o puesto responsable del resguardo del activo.

II. Mantener un inventario actualizado de toda la infraestructura tecnológica (hardware y software) con las características de cada uno de los componentes, con la finalidad de controlar la integridad de los equipos, que están bajo responsabilidad de las personas usuarias y de la propia UTSIT.

Asignación de bienes tecnológicos

Artículo 7. La asignación de bienes muebles de orden tecnológico deberá efectuarse en apego a, los Lineamientos generales de racionalidad, austeridad y disciplina presupuestal vigentes al momento de su asignación, mediante el procedimiento que para tal fin disponga la Coordinación Administrativa.

Disponibilidad de bienes tecnológicos

Artículo 8. Durante el mes de agosto de cada ejercicio fiscal, la UTSIT proporcionará a las UR el listado con la disponibilidad existente de bienes tecnológicos.

Requerimientos de bienes tecnológicos

Artículo 9. Las UR deberán comunicar a la UTSIT el total de bienes tecnológicos que requerirán, para el desarrollo de sus proyectos en el ejercicio fiscal siguiente, al menos, siete días hábiles previos al inicio de la actividad de presupuestación.

Disposición de bienes tecnológicos

Artículo 10. La UTSIT proporcionará a las UR los bienes tecnológicos con los que se cuenta al inicio de la actividad de presupuestación, con el objeto de que sus titulares aseguren sus requerimientos o, en su caso, contemplen los bienes tecnológicos para cubrir sus necesidades durante el ejercicio fiscal siguiente.

Solicitud de bienes tecnológicos

Artículo 11. La solicitud de bienes tecnológicos a la UTSIT, para asignación a la persona responsable deberá atenderse mediante los formatos y condiciones establecidas por la Coordinación Administrativa, y conforme a lo dispuesto en los Lineamientos generales de racionalidad, austeridad y disciplina presupuestal vigentes al momento de su solicitud, con una anticipación mínima de:

I. Cuarenta y ocho horas previas a su instalación, para el uso cotidiano en la atención de actividades propias del personal o en su caso para la asignación de nuevo ingreso, y

II. Siete días hábiles previos a la fecha de atención de actividades especiales como eventos, talleres, cursos, entrevistas, páneles, entre otros.

Capítulo II
Del uso de los activos tecnológicos

Medidas preventivas de uso adecuado

Artículo 12. Para ejecutar un uso adecuado de los activos tecnológicos el GISI, deberá:

I. Definir las condiciones de uso y protección de los activos de información;

II. Definir el proceso de administración de los activos tecnológicos;

III. Definir controles de seguridad en los activos tecnológicos del Instituto para monitorear, alertar y prevenir incidentes de seguridad que se puedan derivar de un mal manejo de estos;

IV. Supervisar la implementación, operación y mantenimiento de las configuraciones adecuadas para los activos tecnológicos, con el fin de preservar la Seguridad de la Información que estos contienen, transmiten o procesan, y

V. Supervisar el suministro del soporte, mantenimiento y actualización de los activos tecnológicos del Instituto.

Uso adecuado de los activos tecnológicos

Artículo 13. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que hagan uso de los activos tecnológicos de éste, deberán:

I. Emplear los activos tecnológicos, equipo telefónico o dispositivos móviles que se le asignen, o personales autorizados a conectarse en la red institucional, atendiendo lo establecido en el artículo 50 de estos Lineamientos, únicamente para las funciones de trabajo encomendadas en el ejercicio de su cargo o puesto;

II. Aceptar que, en caso de realizar cualquier tipo de uso no adecuado de los activos del Instituto, será sujeto a las medidas que se indiquen en cuanto a lo referido en la reparación y pago de deducibles de bienes muebles previstas por la normativa aplicable;

III. En caso de detectar algún comportamiento anómalo en el funcionamiento u operación de los activos asignados, reportarlo de forma inmediata a la UTSIT;

IV. Evitar la manipulación inadecuada de los activos tecnológicos, así como su sustracción de las instalaciones del Instituto, con excepción de cuando esto fuese expresamente permitido por su titular para la atención de actividades laborales;

V. Operar los activos tecnológicos en un entorno seguro, atendiendo las disposiciones de escritorios limpios dispuestas en los presentes Lineamientos;

VI. Evitar abrir o desarmar los activos tecnológicos, en los casos en que así se requiera se deberá pedir el apoyo y diagnóstico previo de la UTSIT, quien será la única autorizada para la manipulación de los equipos;

VII. Ser responsable del uso y custodia de los activos tecnológicos, telefonía o dispositivos móviles que tenga bajo su resguardo;

VIII. Responder por los activos de TI, telefonía o dispositivos móviles, que tenga bajo su resguardo, por lo que se debe evitar su préstamo, y

IX. Reportar de inmediato a la UTSIT y a la Coordinación Administrativa en caso de robo, extravío o pérdida del activo tecnológico.

Capítulo III
De la gestión de capacidad de TI

Planeación y gestión de la capacidad

Artículo 14. Para gestionar la capacidad la UTSIT deberá:

I. Desarrollar un Plan de Capacidad que contemple lo siguiente:

a) Los niveles de servicio acordados y/o previstos (SLAs).
b) Niveles de rendimiento esperados.
c) Impacto de la aplicación o servicio en los procesos sustanciales del Instituto.
d) Márgenes de seguridad y disponibilidad.
e) Informes de monitorización de los niveles de servicio.

i. El uso de recursos.
ii. Desviaciones de la capacidad real sobre la planificada.
iii. Análisis de tendencias en el uso de la capacidad.
iv. Métricas establecidas para el análisis de la capacidad y monitorización del rendimiento.
v. Impacto en la calidad del servicio, disponibilidad y otros procesos TI.

f) Costes asociados a los equipos de hardware y otros recursos TI necesarios.
g) Las previsiones sobre necesidades futuras basadas en tendencias, previsiones de negocio y SLAs existentes, con el objeto de garantizar que, en caso de presentarse un incidente derivado a la falta de capacidades necesarias, se tomen las medidas preventivas necesarias para que no vuelva a ocurrir.

II. Supervisión de la capacidad y administración a través de la herramienta tecnológica Mesa de ayuda;

III. Garantizar que el procedimiento de monitoreo y planeación de la capacidad, cuente con los elementos necesarios para identificar de forma clara y oportuna las necesidades previstas, a fin de que éstas, sean cubiertas en tiempo y forma;

IV. Reportar los requerimientos que se tengan, a nivel tecnológico, en materia de capacidades instaladas contra las utilizadas, y

V. Suministrar el soporte, mantenimiento y actualización de la infraestructura necesaria para la gestión de la capacidad.

Solicitud y atención de servicio

Artículo 15. Las personas servidoras del Instituto deberán hacer uso de la Mesa de ayuda, para toda requisición de servicio de soporte técnico, asesoría y actualización de sistemas, a través de la cual se atenderá conforme a lo siguiente:

I. La persona usuaria plantea la solicitud de servicio en la Mesa de ayuda.

II. La solicitud de servicio se asigna a una persona técnica de servicio de la UTSIT.

III. La persona técnica evalúa la solicitud y procede a realizar su clasificación y atención.

IV. La persona técnica cierra el ticket después de atender la solicitud de servicio.

V. Se concluye con un seguimiento de satisfacción con el resultado por parte de la persona usuaria.

Título tercero
De la Seguridad de la Información

Capítulo I
De la protección y clasificación de la información y datos personales

Clasificación de la información

Artículo 16. Respecto a la clasificación de la información el Instituto deberá:

I. Por parte de todo el personal, atender la Ley General de Transparencia y Acceso a la Información Pública, Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato, Ley General de Protección de Datos Personales en posesión de Sujetos Obligados, Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato, Reglamento de Protección de Datos Personales del Instituto Electoral del Estado de Guanajuato, y el documento de Política de Seguridad de la información del Instituto Electoral del Estado de Guanajuato, así como la Ley de Archivos del Estado de Guanajuato para la clasificación y valoración de la información, de tal forma que se permita identificar el nivel de confidencialidad que la misma requiere, así como la demás normativa aplicable en la materia.

II. Contar con mecanismos criptográficos que ayuden a proteger la confidencialidad de la información digital, y

III. Por parte de todo el personal de este Instituto, contar con los mecanismos definidos por la UTSIT que ayuden a proteger la confidencialidad de la información que se encuentra en medios físicos.

Medidas de seguridad y protección de la información

Artículo 17. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que manejen información de este, deberán:

I. Evitar dejar a la vista contraseñas, información digital o física en la estación de trabajo;

II. Renovar sus contraseñas de acceso a la computadora y sistemas informáticos conforme al tiempo indicado por la UTSIT;

III. Almacenar la documentación importante bajo llave, y retirar inmediatamente de las impresoras compartidas la documentación que se remita a impresión, o se coloque para su digitalización;

IV. Atender a lo dispuesto en estos Lineamientos en cuanto al equipo de usuario desatendido;

V. Ser responsables de las credenciales de acceso y contraseñas que se le asignen, en virtud de que éstas son personales e intransferibles;

VI. Notificar a la UTSIT sobre solicitudes sospechosas, en cuanto al uso de las credenciales de acceso y contraseñas para su inmediata atención;

VII. Verificar que los sitios web a los que accede se identifiquen como sitios seguros para su privacidad;

VIII. Usar los sistemas informáticos con la finalidad exclusiva de cumplir con las funciones de su cargo;

IX. Atender los lineamientos de seguridad en cuanto al uso de medios removibles;

X. Evitar el uso de herramientas para almacenamiento en internet que no sean las establecidas por la UTSIT;

XI. Evitar el uso de dispositivos móviles personales (teléfonos, tabletas, laptops) que no estén expresamente autorizados por la Secretaría Ejecutiva para almacenar o procesar datos laborales;

XII. Mantener la configuración predeterminada de los sistemas;

XIII. Verificar que la información del ámbito de su competencia sea clasificada e inventariada, conforme a la legislación y normatividad administrativa vigente en materia de archivos, así como a lo dispuesto por los Lineamientos y demás criterios que emita el GISI;

XIV. Cumplir con lo establecido en los presentes Lineamientos en materia de seguridad física y resguardo de documentos, y

XV. Atender cualquier otra recomendación del GISI en materia de Seguridad de la Información.

Gestión de incidentes de seguridad

Artículo 18. El protocolo de gestión de incidentes propuesto por la UTSIT, deberá:

I. Contar con un catálogo de servicios e incidencias alineado con una Matriz de riesgos de TI y de procedimientos adecuados para gestionar la atención de dichos incidentes;

II. Actualizar el catálogo de servicios e incidencias con el propósito de establecer tiempos de respuesta, plan de acción y comunicación, e impacto para cada uno de los incidentes;

III. Contar con un equipo de respuesta capacitado para la atención de incidentes, y

IV. Crear una estrategia de concientización continua para todo el personal del Instituto, con el fin de reducir incidentes que pudiesen ser causados por desconocimiento de las personas usuarias y, asimismo, para orientar una correcta gestión de recursos.

Reporte de incidentes de seguridad

Artículo 19. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que hagan uso de los activos de TI de éste, deberán reportar de forma inmediata a la UTSIT en caso de acontecer los siguientes eventos o incidentes de Seguridad de la Información:

I. Las condiciones del entorno representen un factor de riesgo para la información, los servicios tecnológicos o la operación de los procesos;

II. La información esté expuesta y pueda ser objeto de algún daño o acceso sin autorización;

III. El funcionamiento de aplicaciones informáticas, páginas o sistemas institucionales pongan en riesgo la confidencialidad, integridad y disponibilidad de la información;

IV. Se presente un daño en la información;

V. No se cumpla con las políticas, lineamientos o protocolos en materia de Seguridad de la Información;

VI. El acceso no autorizado a las áreas o instalaciones restringidas;

VII. Exista alteración, pérdida total o parcial de la Información, y

VIII. Cualquier circunstancia que comprometa la Seguridad de la Información.

Comunicación oficial para el reporte de incidentes

Artículo 20. Se deberá hacer uso de la herramienta tecnológica Mesa de Ayuda, para reportar los incidentes presentados durante el desempeño de sus funciones, conforme a lo dispuesto en el artículo 15 de estos Lineamientos.

Capítulo II
De la concientización y capacitación en Seguridad de la Información

Plan de concientización en Seguridad de la Información

Artículo 21. El GISI, en tema de concientización en Seguridad de la Información, deberá:

I. Supervisar que se cuente con un plan de concientización y sensibilización para el personal de este Instituto, acorde a los requerimientos de Seguridad de Información definido por la UTSIT, y

II. Asegurar que se cuente con los recursos (difusión de información, medidas preventivas, recomendaciones) necesarios para cumplir con el plan de concientización y sensibilización definido por la UTSIT y aprobado por la JEE.

Aplicación de medidas de Seguridad de la Información

Artículo 22. Las personas servidoras del Instituto, así como integrantes de partidos políticos y externas, que hagan uso de los activos de TI de éste, deberán:

I. Atender a la información y materiales que brinde el GISI en materia de Seguridad de la Información;

II. Conocer y adquirir las competencias laborales necesarias, para el debido manejo y resguardo de la información del Instituto, conforme a las herramientas brindadas por el plan de concientización y sensibilización en materia de TI, y

III. Aplicar las medidas de seguridad necesarias para el cumplimiento de sus funciones, con el debido conocimiento de las acciones por ejecutar de acuerdo con el alcance de sus responsabilidades.

Capítulo III
De la continuidad en Seguridad de la Información

Planeación de continuidad en Seguridad de la Información

Artículo 23. Para la planeación de la continuidad y Seguridad de la Información propuesta por el GISI deberá:

I. Determinar los requerimientos de continuidad y Seguridad de la Información crítica, que apliquen en caso de situación adversa y pongan en riesgo la operación del Instituto;

II. Implementar procesos, procedimientos y controles para garantizar el nivel requerido de continuidad para la Seguridad de la Información durante una situación adversa;

III. Probar, verificar y evaluar los recursos, procesos y controles de continuidad y Seguridad de la Información implementados en intervalos regulares;

IV. Aplicar los mismos criterios para el caso de productos y servicios proporcionados por terceros;

V. Asegurar contar con redundancia para cumplir con los requisitos de seguridad, continuidad y disponibilidad que sean definidos;

VI. Mantener la operación de la infraestructura tecnológica que soporta los sistemas y servicios críticos de la institución para garantizar la continuidad de los procesos sustantivos del Instituto, y

VII. Suministrar el soporte, mantenimiento y actualización de la infraestructura necesaria para la continuidad y Seguridad de la Información del Instituto.

Atención a las actividades de continuidad

Artículo 24. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que hagan uso de la información de éste, deberán:

I. Participar en las actividades de continuidad y Seguridad de la Información que sean definidas por el GISI, y

II. Reportar a la UTSIT cualquier incidente de Seguridad de la Información que pudiere afectar la continuidad de las operaciones e información generada por el Instituto.

Título cuarto
De la seguridad física y lógica de los activos de información

Capítulo I
De las medidas de seguridad y prevención en accesos físicos

Seguridad en accesos físicos

Artículo 25. El Instituto respecto a los accesos físicos deberá:

I. Contar con un mecanismo de monitoreo de accesos a las áreas restringidas, así como el listado del personal preautorizado para su ingreso a las mismas, y

II. Contar con un mecanismo de seguridad que controlen los accesos del personal.

Medidas de seguridad en accesos físicos

Artículo 26. Las personas servidoras del Instituto, deberán:

I. Portar una identificación institucional vigente, y

II. En caso de requerir acceso a las áreas restringidas del Instituto, solicitar autorización al titular o titulares a cargo de la seguridad de éstas.

Medidas preventivas del equipo de usuario desatendido

Artículo 27. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que hagan uso de los activos tecnológicos de éste, deberán:

I. Cerrar la sesión del sistema o bloqueo de pantalla cuando se ausente de su lugar de trabajo;

II. Para el desbloqueo de los equipos terminales, la persona usuaria deberá utilizar su usuario y contraseña asignado, y

III. El personal que detecte el incumplimiento a lo definido en cuanto a equipo de usuario desatendido, deberá avisar de forma inmediata a la UTSIT, de cualquier incidente que pudiere afectar la Seguridad de la Información del Instituto.

Disposiciones preventivas en la estación de trabajo

Artículo 28. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que hagan uso de los activos tecnológicos de éste, deberán:

I. Mantener limpias y seguras las estaciones de trabajo que se encuentren bajo su resguardo;

II. Mantener orden, limpieza y la menor cantidad posible de objetos sobre su escritorio físico o lugar de trabajo;

III. Evitar mostrar algún tipo de información sensible, a partir de la pantalla de su equipo de cómputo, o bien, por medio de notas u objetos colocados en su sitio de trabajo;

IV. Evitar dejar líquidos o algún material que pudiera dañar la infraestructura tecnológica del Instituto;

V. Procurar el almacenamiento seguro y la protección de la información en el desarrollo de sus actividades laborales;

VI. Evitar consumir alimentos e ingerir bebidas durante el uso del equipo tecnológico asignado, colocar objetos encima u obstruir los orificios de ventilación de este, y

VII. Mantener un entorno limpio y sin humedad o exceso de calor al operar los activos tecnológicos.

De la disposición o reutilización segura del equipo

Artículo 29. Respecto a la disposición o reutilización segura del equipo, la UTSIT deberá:

I. Contar con un protocolo de identificación de activos tecnológicos obsoletos;

II. Asegurar que cualquier medio físico o intangible que contenga información, al cubrir su vida útil, pase por un proceso de borrado seguro de la información que contenga, así como para el caso de que este se desee reutilizar;

III. Verificar de forma periódica que los procesos de borrado seguro se lleven a cabo conforme a lo previsto en las fichas técnicas de valoración documental de la serie que corresponda;

IV. Mantener registro de los procesos de borrado seguro, resguardando la documentación e información resultante, para efectos de posibles auditorías, y

V. Atender a lo dispuesto en la normativa aplicable y vigente en cuanto a la baja de equipo obsoleto para su desecho.

Respaldos de la información

Artículo 30. A efecto de respaldar la información la UTSIT deberá:

I. Contar con un plan periódico que determine los tipos, periodicidad, recursos y pruebas de los respaldos de información que sean requeridos

por el Instituto conforme a lo establecido en las fichas técnicas de valoración documental de la serie que corresponda;

II. Respaldar la información que se considere necesaria;

III. Contar con un plan de pruebas simuladas y reales sobre los respaldos;

IV. Generar evidencia acerca de la realización de los respaldos y de sus pruebas;

V. Actualizar el inventario de activos de seguridad para que incluya a los respaldos;

VI. Clasificar y etiquetar los respaldos;

VII. Asignar una persona responsable de los respaldos;

VIII. Cifrar los respaldos, y

IX. Asignar un tiempo de vida a los respaldos con base en lo dispuesto en las fichas de valoración documental de este Instituto.

Medidas de prevención de la información digital

Artículo 31. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que hagan uso de la información de éste, deberán:

I. Llevar a cabo de manera periódica los respaldos de información, que se encuentren almacenados en equipos de cómputo personal; específicamente para aquella información que se considere sensible o crítica para el cumplimiento de las funciones del responsable de ésta, y de los objetivos del propio Instituto;

II. Respaldar la información que consideren relevante cuando el equipo de cómputo sea trasladado por cualquier situación a una zona externa al Instituto, previendo así la pérdida involuntaria de información, derivada de situaciones de riesgo adversas presentadas en éste, y

III. Atender a lo establecido por estos Lineamientos respecto a la información contenida en el correo electrónico.

De la gestión de medios removibles

Artículo 32. El GISI, respecto a la gestión de medios removibles, deberá:

I. Asegurar la restricción en el uso de medios removibles, el cual solo aplicará para personal autorizado en el cumplimiento de sus funciones;

II. Mantener asegurada la información almacenada en medios removibles, libre de software malicioso y cifrada si es información confidencial;

III. Informar al personal responsable de un medio removible, sobre su obligación de buen uso y su compromiso de velar por su contenido;

IV. Establecer un protocolo de autorización para el uso de medios removibles que contemple:

a) Llevar un registro de los medios removibles autorizados.
b) Definir en qué condiciones o casos se permite su uso.
c) Definir cómo se accede y si la información debe ir cifrada.
d) Establecer las configuraciones de seguridad necesarias para poder utilizarlos.
e) Las demás especificaciones que estime necesarias.

V. Auditar de manera periódica que la aplicación de bloqueo de puertos de acceso, en toda la infraestructura tecnológica, se aplique de manera efectiva, y

VI. Definir mecanismos para la protección de la información almacenada en medios removibles, los cuales contemplen:

a) Los dispositivos que se conectan.

A través de la UTSIT:

i. Programar cambios periódicos de contraseña de acceso al dispositivo.
ii. Implementar mecanismos de autenticación de las personas usuarias.
iii. Evitar que dispositivos no registrados puedan conectarse a cualquier equipo de la organización.
iv. Desactivar la opción de autoarranque en los equipos para no permitir posibles ejecuciones automáticas no deseadas cuando los dispositivos extraíbles son insertados.
v. Deshabilitar por defecto los puertos USB.
vi. Habilitar los puertos USB para el personal que necesite dicha funcionalidad de manera periódica o gestione ficheros de gran tamaño, toda vez que su solicitud provenga con la autorización de la persona titular de la UR dueña de la información mediante oficio.

b) Sobre los documentos que se transfieren.

A través de la UTSIT:

i. Establecer un control de accesos con permisos de lectura, escritura y ejecución.
ii. Implementar mecanismos de cifrado de la documentación.

Medidas preventivas de medios removibles

Artículo 33. Las personas servidoras del Instituto, así como las personas integrantes de partidos políticos y externas, que hagan uso de los activos tecnológicos de este, deberán:

I. Evitar al máximo el uso de medios removibles, y

II. Evitar la divulgación y distribución de la información contenida en medios removibles.

Capítulo II
Del correo electrónico

Disposiciones generales

Artículo 34. El GISI, respecto al correo electrónico, deberá:

I. Concientizar y sensibilizar a todo el personal que tenga una cuenta de correo electrónico institucional, acerca del buen uso de esta herramienta;

II. Definir e implementar los controles de seguridad aplicables a la mensajería electrónica para monitorear, alertar y prevenir incidentes de seguridad.

III. Supervisar la disponibilidad y entrega de servicio de mensajería electrónica, y

IV. Asegurar la apropiada operación y administración de las plataformas empleadas para la mensajería electrónica.

Confidencialidad de la información

Artículo 35. Para el caso de aquellas solicitudes de acceso a la información, así como por autoridades competentes, que versen sobre la mensajería electrónica en las cuentas de correo asignadas por este Instituto, éstas se tratarán conforme a lo siguiente:

a) En el supuesto de ser personas usuarias que tengan una relación laboral vigente, el titular del área procesará la información que integren las respuestas a las solicitudes.

b) Al tratarse de personas usuarias que no tengan una relación laboral vigente, la UTSIT proporcionará el acceso y revelación de los correos a las personas titulares correspondientes, con el objeto de que estas procesen la información que integren las respuestas a las solicitudes.

En ambos casos se gestionará conforme a la vigencia documental determinada por la Ley de Archivos del Estado de Guanajuato.

Sección primera
De las personas usuarias del servicio de correo del Instituto

Personas usuarias de cuentas de correo electrónico

Artículo 36. Podrá utilizar una cuenta de correo electrónico del Instituto el personal activo en la estructura permanente o eventual, así como los partidos políticos para la recepción de notificaciones por parte de este Instituto.

Responsabilidad de la cuenta

Artículo 37. Cada persona que tenga una cuenta de correo es responsable de los recursos que tenga asignados y de todas las acciones que se lleven a cabo en su utilización.

Sección segunda
De las cuentas y buzones de correo

Asignación y propiedad de cuentas

Artículo 38. Las cuentas de correo electrónico que se asignen son individuales e intransferibles, por lo que cada persona usuaria la recibirá bajo su responsabilidad y de conformidad con lo establecido en los presentes Lineamientos.

Solicitud y Creación

Artículo 39. La solicitud de una cuenta de correo electrónico deberá ser realizada mediante el formato de solicitud de correo electrónico por la persona titular de la UR a la que esté adscrito la persona a quien se le pretende asignar.

Gestión del buzón de correo

Artículo 40. Corresponde a cada persona usuaria la gestión de la información contenida en su correo electrónico, por lo que atenderá a lo siguiente:

I. Revisar la bandeja de entrada y, de ser el caso, la de salida, como mínimo, una vez al día;

II. Revisar los mensajes de retorno que los sistemas de correo le envíen notificándole cualquier incidencia en la entrega de los mensajes remitidos desde su cuenta;

III. Depurar la bandeja de entrada y salida periódicamente, conservando los correos que respondan a actividades por atribuciones o funciones del cargo o puesto, y

IV. Crear y archivar en carpetas y subcarpetas que permitan una mejor gestión del buzón.

Conductas inadecuadas

Artículo 41. Las personas usuarias del servicio de correo electrónico deberán abstenerse de realizar cualquiera de las siguientes actividades:

I. Emplear la cuenta de correo electrónico facilitada por el Instituto con fines personales;

II. Utilizar la cuenta de correo electrónico para actividades profesionales ajenas al cargo o puesto que desempeñan en el Instituto, y

III. El envío de correos masivos (spam) utilizando la dirección de correo electrónico institucional.

Medidas de seguridad

Artículo 42. Son problemas de seguridad que pueden afectar al correo electrónico, los siguientes:

I. Robo de identidad;
II. Virus;
III. Spam, y
IV. Ataques con direcciones falsificadas.

Por lo anterior las personas usuarias deberán:

I. Guardar los datos de usuario y la contraseña de acceso a la cuenta de correo de forma segura y no facilitarlos a otras personas;

II. Utilizar una contraseña difícil de descifrar;

III. Omitir el uso de la opción de guardar la contraseña que se ofrece al usuario para evitar reintroducirla en cada conexión;

IV. Bloquear el acceso a la cuenta de correo y el equipamiento informático, en caso de ausentarse de su estación de trabajo durante la jornada laboral;

V. Abstenerse de abrir mensajes sospechosos que puedan provocar daños al Instituto;

VI. Evitar enviar, reenviar o responder a mensajes de correo que contengan datos sensibles sin la autorización de la persona titular de la UR, y

VII. En caso de detectar una incidencia durante el uso del correo electrónico, la persona usuaria debe ponerlo en conocimiento de la UTSIT de manera inmediata.

Uso inadecuado del correo electrónico

Artículo 43. Se consideran usos inadecuados del correo electrónico institucional, los siguientes:

I. El uso de contenido o información en mensajería electrónica que pueda ser considerado como difamatorio, hostil, ilegal, discriminatorio u ofensivo;

II. Generar o compartir información que pueda ser considerada como inapropiada u obscena;

III. Descargar, copiar o compartir videos, música, gráficos o ejecutables para fines ajenos a las funciones desempeñadas por el cargo o puesto;

IV. El uso de dispositivos de codificación no autorizada por la UTSIT;

V. La visualización de contenido considerado como spam, o ajeno a las funciones desempeñadas por el cargo o puesto en la mensajería recibida, y

VI. Cualquier otro uso que no apoye el desempeño de las funciones propias de las personas servidoras de este Instituto.

Sección tercera
De la vigencia, desactivación y eliminación de cuentas de correo

Vigencia de cuentas

Artículo 44. Las cuentas del Instituto permanecerán hasta en tanto el personal cause baja o cuando se proceda a la pérdida del registro para el caso de los partidos políticos.

Cambio de contraseña por causa de baja o cancelación jurídica

Artículo 45. Cuando se presente la baja de personas o la pérdida del registro para el caso de los partidos políticos, la UTSIT procederá al cambio de la contraseña asignada a dicha cuenta.

Respaldo de cuentas

Artículo 46. Es responsabilidad de la UTSIT realizar el respaldo inmediato de las cuentas de correo electrónico del personal que haya concluido la relación laboral con el Instituto.

Los respaldos permanecerán almacenados en la infraestructura que la UTSIT disponga para ello, por un plazo de dos años posteriores a su creación.

Desactivación temporal de cuentas

Artículo 47. Las cuentas institucionales que correspondan a personal que haya terminado su relación laboral con el Instituto, tendrán una vigencia de sesenta días naturales para efectos de consultas solicitadas por la o el superior jerárquico inmediato.

Eliminación de cuentas

Artículo 48. Una vez concluido el plazo de sesenta días naturales referidos en el artículo anterior, la UTSIT procederá a eliminar la cuenta.

Capítulo III
De los dispositivos móviles

Medidas de prevención de seguridad

Artículo 49. El Instituto, a través de la UTSIT y respecto a los dispositivos móviles deberá:

I. Mantener un control de comodatos e inventario del equipo asignado;

II. Especificar a las personas usuarias que el dispositivo móvil no es para uso personal, y

III. Aplicar los mecanismos de seguridad, a nivel tecnológico, que sean definidos por el GISI.

Atención a medidas de seguridad en la red inalámbrica

Artículo 50. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que cuenten con acceso a la red institucional, deberán:

I. Considerar y atender que el uso de dispositivos móviles con acceso a la red, servicios y aplicaciones del Instituto es exclusivamente para las actividades relacionadas con las necesidades del cargo o puesto que desempeña;

II. Considerar y atender que las personas usuarias de dispositivos móviles que hacen uso de la red, de los servicios y las aplicaciones del Instituto, deberán avisar de forma inmediata a la UTSIT de cualquier incidente que pudiere afectar la seguridad de la información del Instituto;

III. Evitar hacer uso de redes inalámbricas de dominio público que puedan resultar inseguras para transmitir información, así como, conectar los dispositivos institucionales a equipos ajenos a la institución;

IV. El acceso a la red inalámbrica deberá ser solicitado por la persona titular de la UR justificando la necesidad de esta solicitud mediante oficio anexando el formato de filtrado de contenido, y

V. Considerar que cuando se le proporcione acceso a la red, a los servicios y aplicaciones del Instituto tienen conocimiento y aceptan que:

a) Serán sujetos a tráfico limitado de navegación.
b) Esta prohibída la transmisión de archivos que contengan información interna, confidencial o no autorizada.
c) Se prohíbe la descarga de software sin la autorización de la UTSIT.
d) La temporalidad del acceso a la red inalámbrica es de seis meses a partir de la atención de su solicitud.

Capítulo IV
Videoconferencias

Uso de videoconferencias

Artículo 51. Las actividades que requieran ser realizadas mediante videoconferencias deberán contar con una persona responsable preferentemente de la misma UR organizadora, o en su caso a la coordinación de comisiones de este Instituto para tales actividades, quien fungirá como administradora y operadora de estas reuniones, y deberá:

I. Generar direcciones de acceso a videoconferencias;

II. Agendar las sesiones;

III. Convocar a personas participantes;

IV. Administrar y grabar las sesiones, y

V. Respaldar de manera local las grabaciones.

Creación de direcciones de acceso para videoconferencias de sesiones

Artículo 52. Las direcciones de acceso a videoconferencias deberán crearse conforme a lo siguiente:

I. Siete días hábiles previos a su utilización;

II. Veinticuatro horas previas, cuando la naturaleza de la actividad sea urgente o por cuestiones específicas para el desempeño de las actividades asignadas, y

III. Al inicio de cada ejercicio fiscal, siempre y cuando la fecha y hora ya estén previstas en actividades que pertenezcan al Programa Anual de Trabajo vigente de las UR solicitantes.

Direcciones de acceso para videoconferencias de actividad ordinaria

Artículo 53. Las UR dispondrán de la herramienta informática que les permita crear direcciones de acceso para videoconferencias con el objeto de atender sus actividades ordinarias en los términos dispuestos en el artículo 51.

Respaldo seguro

Artículo 54. La UTSIT proporcionará la infraestructura y capacitación necesaria para que las UR almacenen los respaldos derivados de las videoconferencias.

Temporalidad adecuada para la realización de respaldos

Artículo 55. Las UR deberán realizar respaldos periódicos de las grabaciones que realicen considerando no sobrepasar la capacidad de almacenamiento con la que cuente la licencia administrada.

Capítulo V
Del control de red

Medidas de prevención en el control de red

Artículo 56. La UTSIT, respecto al control de red, deberá:

I. Concientizar a todo el personal que utilice la red del Instituto que son responsables de la protección y buen uso de la información que se transmita por dicho medio;

II. Definir mecanismos para la protección de la información transmitida por medio de la red institucional, tales como el uso de herramientas antimalware en el equipo desde donde se establezca la conexión, uso de claves robustas para llevar a cabo la conexión, cierre de la conexión después de tiempo máximo permitido o sin uso, validación y eliminación de cuentas no vigentes, entre otros;

III. Aplicar auditorías periódicas sobre los controles de red que hubiesen sido definidos, que aseguren que los equipos cuenten con un mínimo de mecanismos de Seguridad de la Información (control de puertos, cifrado de información, accesos controlados, entre otros);

IV. Aplicar los mecanismos de seguridad, a nivel tecnológico, que sean definidos por el propio GISI;

V. Implementar controles de seguridad de red para monitorear, alertar y prevenir incidentes de seguridad;

VI. Restringir el uso de la red del Instituto, permitiendo los accesos solo al personal autorizado y por los períodos establecidos, asimismo, conforme con las labores desempeñadas, y

VII. Supervisar el suministro del soporte, mantenimiento y actualización del hardware y software empleado para los mecanismos de seguridad, requeridos para el control de red.

Atención a medidas de seguridad en la red

Artículo 57. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que cuenten con acceso a la red institucional, deberán:

I. Hacer uso de la red institucional exclusivamente para las actividades relacionadas con las necesidades del cargo o puesto que desempeña para el Instituto;

II. Reportar de forma inmediata a la UTSIT, cualquier incidente que pudiere afectar la Seguridad de la Información del Instituto;

III. Cuando se le proporcione acceso a la red, tener conocimiento y aceptar que el empleo de las credenciales de acceso lógico queda restringido para uso exclusivo de la persona autorizada para tener acceso a la red, quedando expresamente prohibido compartirlas a cualquier otra persona; y

IV. Comprender que se considerará como un ataque a la Seguridad de la Información y, por ende, como una falta grave, cualquier actividad no autorizada, en la cual las personas usuarias realicen la exploración de los recursos de TI en la red del Instituto, así como de las aplicaciones y servicios que sobre dicha red operan, con fines de detectar y explotar posibles vulnerabilidades.

V. Ser consciente de que toda falta grave será sujeta a la observación por parte del Órgano Interno de Control de este Instituto.

Capítulo VI
Del uso de internet

Uso adecuado del internet

Artículo 58. Para el uso adecuado del Internet, la UTSIT deberá:

I. Definir los controles de seguridad aplicables al uso del servicio de Internet institucional, incluyendo la definición de perfiles de acceso para el personal, con base en su cargo, puesto o responsabilidad al interior del Instituto;

II. Mantener un control del uso del servicio de Internet;

III. Asegurar la apropiada operación y administración de los enlaces y tecnología empleada para la provisión y uso del servicio de Internet;

IV. Aplicar los mecanismos de seguridad, a nivel tecnológico, que sean definidos por el GISI, incluyendo la correcta aplicación de permisos específicos de uso de Internet con base en el nivel de autorización del que se disponga;

V. Implementar controles de seguridad en el uso de Internet para monitorear, alertar y prevenir incidentes de seguridad, y

VI. Suministrar el soporte, mantenimiento y actualización de la infraestructura que soporta el servicio de Internet del Instituto.

Condiciones del acceso a internet

Artículo 59. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que cuenten con acceso a la red institucional deberán atender a lo dispuesto en el artículo 27 de la Política de Seguridad de la Información.

Capítulo VII
Del control de acceso lógico

Medidas de seguridad en acceso lógico

Artículo 60. Respecto al control de acceso lógico, la UTSIT deberá:

I. Establecer un control y monitoreo de los accesos lógicos a los sistemas aplicativos y plataformas tecnologías establecidas, basado en los roles y perfiles de las personas usuarias;

II. Establecer un proceso que defina el uso de cuentas de acceso y contraseñas seguras para todo el personal que requiera acceso a los sistemas y plataformas tecnológicas;

III. Establecer el mecanismo de monitoreo de las actividades relacionadas con la administración de los sistemas aplicativos y plataformas tecnológicas por parte de las UR que reporten directamente al GISI;

IV. Asegurar un esquema de clasificación de claves y niveles de acceso, para los sistemas aplicativos y plataformas tecnológicas;

V. Asegurar el retiro o adaptación de los derechos de acceso, mediante un mecanismo formal con alcance para todo el personal, que implique la información y las instalaciones del procesamiento de esta a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio;

VI. Establecer un mecanismo de gestión de los derechos de acceso con privilegios especiales, su asignación y uso con vigencia de manera restringida y controlada;

VII. Llevar a cabo una revisión de permisos, roles y funciones de manera periódica, que apliquen a los sistemas aplicativos y plataformas tecnológicas establecidas;

VIII. Dejar registro de los accesos, actividades realizadas y salidas de los accesos a los sistemas aplicativos y plataformas tecnológicas establecidas;

IX. Otorgar solo los permisos que estén autorizados para el perfil que corresponda al usuario de acuerdo con los niveles de acceso establecidos;

X. Controlar mediante un proceso de gestión de cambios, toda solicitud de altas y bajas de claves y/o cambio de perfil de acceso a equipos de cómputo y/o aplicativos;

XI. Almacenar los registros de los accesos, por un periodo de tiempo determinado, para ser utilizados en caso necesario (gestión de incidentes de seguridad), o para la realización de auditorías;

XII. Implementar controles de seguridad en el otorgamiento, manejo y retiro de cuentas de acceso, para monitorear, alertar y prevenir incidentes de seguridad, y

XIII. Suministrar el soporte, mantenimiento y actualización del hardware y software empleado para los sistemas de control y monitoreo de los accesos lógicos a los sistemas aplicativos y plataformas tecnologías establecidas.

Atención a mediades de seguridad de acceso lógico

Artículo 61. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que cuenten con acceso a la red institucional y posean cuentas de acceso lógico, deberán:

I. Ser responsable de todas las actividades realizadas con su cuenta de acceso, por lo cual deberán abstenerse de divulgar tal información a terceras personas, así como de utilizar cuentas de acceso que no les pertenezcan.

II. Avisar de forma inmediata a la UTSIT de cualquier incidente relacionado con su cuenta de acceso, que pudiere afectar la Seguridad de la Información del Instituto, así como tener conocimiento y aceptar que:

a) Serán sujetos de monitoreo de las actividades que realizan.

b) El empleo de las credenciales de acceso lógico queda restringido para uso exclusivo de la persona autorizada, quedando expresamente prohibido compartirlas a cualquier otra.

III. Utilizar responsablemente su acceso y no para obtener información u otros sistemas de información del Instituto, a los que no haya sido autorizado previamente, y

IV. Ninguna persona usuaria debe tener acceso a sistemas que no requiera para el cumplimiento de sus funciones ni deberá contar con un nivel de acceso diferente al que le fue autorizado.

Capítulo VIII
De la seguridad contra malware

Medidas de seguridad contra malware

Artículo 62. Respecto a la seguridad contra malware, la UTSIT deberá:

I. Establecer los mecanismos de seguridad necesarios que prevengan, monitoreen, detecten y eliminen software o código malicioso catalogado como malware;

II. Asegurar que todos los medios que contengan información y que les sea posible la instalación de software, deban contar con protección contra malware;

III. Asegurar que todos los medios que tengan protección contra malware cuenten con su licencia de uso vigente;

IV. Asegurar que el antimalware esté actualizado en todo momento;

V. Atender las disposiciones para la notificación de incidentes, conforme a lo establecido en el Artículo 14 de los presentes Lineamientos;

VI. Asegurar que el equipo de respuesta de gestión de incidentes mantenga siempre activo el antimalware, descargue e instale las actualizaciones del software tan pronto como estén disponibles del sitio oficial;

VII. Monitorear con periodicidad los equipos institucionales para verificar su correcto estado libre de malware;

VIII. Asegurar que se realice siempre un análisis antimalware de cualquier unidad del disco extraíble antes de usarla;

IX. Asegurar que antes de conectar un equipo a la red que no sea de propiedad del Instituto, se realice un análisis antimalware, en caso de detectar código malicioso, informar a su propietario y negar el acceso, y

X. Registrar en la matriz de riesgos de TI, el usuario, datos del equipo e información del malware detectado, así como las acciones de control necesarias para mitigar los riesgos.

Atención a medidas de seguridad contra malware

Artículo 63. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que cuenten con acceso a la red institucional, deberán:

I. Abstener el uso de cualquier clase de software que no haya sido proporcionado y validado por la UTSIT;

II. Borrar el spam, cadenas y cualquier otro tipo de correo sospechoso, sin reenviarlo a otras personas destinatarias;

III. Evitar descargar archivos de fuentes desconocidas o sospechosas;

IV. Evitar escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código conocidos como malware: virus, gusanos, phishing, spyware, ransomware o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del Instituto;

V. Dejar de usar inmediatamente el equipo si sospecha de alguna infección por virus de computadora y reportarlo a la UTSIT para la detección y erradicación del virus, y

VI. Evitar dar de baja, alterar o eliminar los servicios y las configuraciones de seguridad para detectar y/o prevenir la propagación de malware que sean implantadas por el Instituto en: antivirus, correo electrónico, paquetería, navegadores u otros programas.

Capítulo IX
Del desarrollo de sistemas, aplicativos y plataformas digitales

Del desarrollo seguro

Artículo 64. Para llevar a cabo el desarrollo seguro en el Instituto, la UTSIT deberá:

I. Asegurar que cualquier desarrollo realizado por el Instituto o terceras personas con quienes colabore cuente con controles que impidan la modificación no autorizada de código;

II. Asegurar que todos los desarrollos estén cubiertos bajo un contrato de derecho de propiedad intelectual;

III. Aplicar el uso de metodologías acreditadas para el desarrollo seguro de software;

IV. Velar por el cumplimiento de los requerimientos y controles de Seguridad de la Información en el desarrollo de aplicaciones informáticas;

V. Mantener un plan de capacitación para mejorar desarrollo seguro de software, que involucre al personal relacionado;

VI. Mantener el monitoreo, supervisión y control de la gestión de ambientes, configuración, cambios, pruebas, desempeño, incidentes, documental y mantenimiento, indicados de manera enunciativa mas no limitativa, y

VII. Mantener respaldos de Seguridad de Información y redundancia en las plataformas operativas, acordes con los requerimientos de continuidad para el proceso de desarrollo de software en caso de una contingencia.

Capítulo X
De la propiedad intelectual

Derechos de propiedad intelectual

Artículo 65. El GISI, respecto a los derechos de propiedad intelectual, deberá:

I. Establecer las medidas necesarias para garantizar que el software utilizado por los proveedores de servicio y no suministrado por el Instituto, sea de su autoría o cuenten con las licencias de uso correspondientes;

II. Establecer, mediante acuerdo que todos los sistemas informáticos que sean creados por personas externas, así como los creados por las personas servidoras de este Instituto, serán propiedad de este. El acuerdo deberá ser debidamente llenado y firmado por las personas desarrolladoras de los sistemas informáticos;

III. Establecer que queda prohibida la instalación de licencias propiedad del Instituto en equipos ajenos a este, a excepción de aquellos aprobados bajo justificación emitida por la UTSIT, y

IV. Verificar que se cuente con un programa de compra y renovación oportuna del licenciamiento requerido para el cumplimiento de las responsabilidades propias del Instituto.

Atención a los derechos de propiedad intelectual

Artículo 66. Las personas servidoras del Instituto, así como integrantes de partidos políticos y personas externas, que manejen información o conocimiento de este Instituto, deberán:

I. Conocer y aceptar que la información que utilice o genere para el desempeño de sus funciones, incluyendo los datos obtenidos en estudios, investigaciones, sistemas de información, programas y código fuente, será propiedad del Instituto;

II. Abstener la realización de copias no autorizadas del software o código fuente utilizado en los equipos de cómputo pertenecientes al Instituto, ya sea adquirido o desarrollado por este;

III. Conocer y aceptar que no se permite que el personal o personas proveedoras del Instituto cedan autorización de acceso a terceros respecto del software de propiedad o con licencia de uso del Instituto;

IV. Atender que el almacenamiento o reproducción de software solo se realizará con el consentimiento del titular de la UTSIT, y

V. En caso de violación a alguna o varias de las disposiciones anteriores, se deberá reportar de inmediato al GISI.

Capítulo XI
De la confidencialidad y no divulgación

Del Acuerdo de confidencialidad y no divulgación

Artículo 67. El Acuerdo de confidencialidad y no divulgación, seguirá el siguiente protocolo:

I. Al iniciar la relación laboral con el Instituto, el personal recibirá el Acuerdo de confidencialidad y no divulgación para su firma;

II. Se realizarán revisiones periódicas para actualizar los acuerdos, asegurando la vigencia de estos, y

III. Al término de la relación laboral se le hará presente al personal su acuerdo con el Instituto.

Capítulo XII
De las personas proveedoras

Medidas de seguridad con las personas proveedoras

Artículo 68. Para temas de Seguridad de la Información en la relación con personas proveedoras, el Instituto a través de la UTSIT en coordinación con las UR, deberá:

I. Garantizar que las personas proveedoras con las que se tiene una relación de suministro cuenten con contrato vigente donde se establezcan cláusulas que los comprometan a proteger la Seguridad de la Información a la que tenga acceso, un Acuerdo de no divulgación y de confidencialidad vigentes;

II. Solicitar respecto al desarrollo de software por parte de terceras personas, la entrega del código fuente original, los requisitos de implementación e instalación, el documento correspondiente a las acciones de mantenimiento y control de cambios, así como el documento que describa los métodos de recuperación en caso de desastres;

III. Solicitar a las personas proveedoras constancia y evidencia, que cuentan con solvencia financiera y técnica para dar cumplimiento a lo previsto en contrato;

IV. Incluir dentro del contrato los requisitos para tratar los riesgos de Seguridad de la Información asociados con la cadena de suministro de los servicios y productos del negocio;

V. Solicitar por contrato, que la persona proveedora en caso necesario efectúe y proporcione evidencia del borrado seguro de información. Así mismo el proveedor queda obligado a proporcionar evidencia de su proceso y política de Seguridad de Información ante el Instituto;

VI. Establecer un método de evaluación que permita tomar acciones correctivas y, de ser necesario, efectuar cambio del proveedor tomando las previsiones del caso en concreto;

VII. Contar con al menos una persona proveedora alternativa que pueda cubrir con la necesidad, y

VIII. Dar a conocer a todos y cada uno de los terceros las políticas de Seguridad de la Información.

Título quinto
Capítulo único
De la auditoría en seguridad de TI

Auditorías de seguridad

Artículo 69. La auditoría en materia de seguridad de la información deberá contemplar lo dispuesto en la Política de Seguridad de la Información aplicable a este Instituto considerando estándares internacionales en ciberseguridad vigentes a la fecha de aplicación.

Titulo sexto
Capítulo único
Del incumplimiento a los Lineamientos

Sanciones

Artículo 70. La inobservancia de las disposiciones contenidas en los presentes Lineamientos dará lugar a las sanciones que para tal efecto señalen los dispositivos jurídicos aplicables, respetándose en todo momento lo previsto por la Constitución General, la Ley General de Responsabilidades Administrativas y la Ley de Responsabilidades Administrativas para el Estado de Guanajuato.

TRANSITORIOS

PRIMERO. Los presentes Lineamientos iniciarán su vigencia el día siguiente a su publicación.

SEGUNDO. Las personas servidoras que laboren en este Instituto deberán firmar el acuerdo de confidencialidad y no divulgación establecido en los presentes Lineamientos al inicio de su vigencia.