Política de Seguridad de la Información del Instituto Electoral del Estado de Guanajuato

IEEG
INSTITUTO ELECTORAL
DEL ESTADO DE GUANAJUATO

Política de Seguridad
de la Información del
Instituto Electoral del
Estado de Guanajuato

Capítulo I
De las disposiciones generales

Objeto

Artículo 1. La Política de Seguridad de la Información del Instituto Electoral del Estado de Guanajuato tiene por objeto:

I. Asegurar la información que posee el Instituto Electoral del Estado de Guanajuato en cualquier medio que la contenga, ya sea físico, digital, tangible o intangible, con el fin de proteger su confidencialidad, integridad y disponibilidad;
II. Establecer las disposiciones generales respecto a la gestión de la seguridad de la información, aplicables a este Instituto, y
III. Orientar las acciones de seguridad de la información que emprenda el Grupo Interno de Seguridad de la Información, para que estén alineadas con los objetivos de este Instituto.

Sujetos de la Política y responsabilidad

Artículo 2. La Política de Seguridad de la Información es de observancia general y obligatoria para las personas servidoras que laboren en este Instituto y personas integrantes de partidos políticos al hacer uso de activos de TI de este Instituto, así mismo cuando se transmita o comparta información con personas externas por motivo del ejercicio de sus funciones; la cual se emite conforme a los principios que rigen la función electoral: certeza, imparcialidad, independencia, legalidad, objetividad, y máxima publicidad.

El Comité de Adquisiciones, Enajenaciones, Arrendamientos y Contratación de Servicios así como las y los titulares de órganos de dirección, ejecutivos, técnicos, de control y demás órganos colegiados del Instituto, son responsables de que en el proceso de contratación o intercambio de información con entes externos se observen las disposiciones contenidas en la presente Política, la Política Digital del Instituto Electoral del Estado de Guanajuato y los Lineamientos de administración, operación y seguridad de las Tecnologías de la Información del Instituto Electoral del Estado de Guanajuato; así como de los otros instrumentos normativos o administrativos de este Instituto emitidos con el mismo fin.

Interpretación de la política

Artículo 3. La interpretación de la presente Política y lo no previsto por la misma, será resuelto por el Grupo Interno de Seguridad de la Información que al efecto se integre.

Glosario

Artículo 4. Para los efectos de esta Política, sin perjuicio de su referencia en plural o singular, se entenderán las siguientes definiciones, siglas y acrónimos:

A. Definiciones

I. **Activo.** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) que tenga valor el Instituto.

II. **Acuerdo de confidencialidad y no divulgación.** Documento legal celebrado entre el Instituto y su personal o personas externas al compartir material confidencial o conocimiento para ciertos propósitos, restringiendo su uso público.

III. **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.

IV. **Confidencialidad.** Propiedad de la información de no ponerse a disposición o ser revelada a personas, entidades o procesos no autorizados.

V. **Control de acceso.** Control que asegura que el acceso a activos esté autorizado y restringido con base en requerimientos de negocio y de seguridad.

VI. **Disponibilidad.** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

VII. **Dispositivo móvil.** Dispositivos que pueden ser fácilmente transportados por las y los usuarios.

VIII. **Escritorio lógico.** Pantalla principal que se observa una vez que se inicializa la computadora, en la que se ubican los Iconos de uso más frecuente y donde se despliegan las aplicaciones en el momento en que se ejecutan.

IX. **Estación de trabajo**. Espacio físico asignado al personal del Instituto para el desempeño de sus actividades.

X. **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.

XI. **Grupo Interno de Seguridad de la Información (GISI).** 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.

XII. **Instituto.** Instituto Electoral del Estado de Guanajuato.

XIII. **Integridad.** Propiedad de la información relativa a su exactitud y completitud.

XIV. **Inventario de activos.** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) al servicio del Instituto, que tengan valor para este y necesiten, por tanto, ser protegidos de potenciales riesgos.

XV. **Lineamientos.** Criterios de actuación que indican los puntos específicos que deben ser atendidos en las políticas de seguridad de la información por parte de las personas involucradas. Para fines de esta Política, se entenderá como los Lineamientos de administración, operación y seguridad de Tecnologías de la Información.

XVI. **Malware.** Engloba a todo tipo de código malicioso.

XVII. **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.

XVIII. **Medio físico.** Conjunto de elementos materiales que constituyen un sistema.

XIX. **Monitoreo.** Determinación del estado de un sistema, proceso o actividad.

XX. **Personas externas.** Todas aquellas personas a las que se les proporciona información del Instituto por motivos laborales, tales como proveedores o consultores.

XXI. **Política.** Documento de alto nivel que define las disposiciones generales sobre una actividad, proceso o sistema para guiar y asegurar su adecuado funcionamiento.

XXII. **Proceso.** Conjunto de actividades interrelacionadas o interactuantes que transforman entradas en salidas.

XXIII. **Seguridad de la información.** Preservación de la confidencialidad, integridad y disponibilidad de la información.

XXIV. **Unidades responsables (UR).** 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.

XXV. **Vulnerabilidad.** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

B. Siglas y acrónimos

XXVI. **GISI.** Grupo Interno de Seguridad de la Información.

XXVII. **UR.** Unidades Responsables.

XXVIII. **UTSIT.** Unidad Técnica de Sistemas de Información y Telecomunicaciones.

Objetivos específicos

Artículo 5. Esta Política de Seguridad de la Información tiene por objetivos específicos:

I. Garantizar la confidencialidad, integridad y disponibilidad de la información;

II. Dar cumplimiento a las disposiciones contenidas en las leyes generales y locales en materia de Seguridad de la Información, con el fin de evitar el mal uso de ella y dar certeza sobre el actuar del Instituto;

III. Atender lo necesario para dar solución y seguimiento a todo asunto relacionado con la seguridad de información, a través del GISI, y

IV. Fomentar una cultura de Seguridad de la Información al interior del Instituto, procurando que todo el personal se sensibilice, participe y contribuya de forma permanente y proactiva en los temas afines a ello.

Capítulo II
Del GISI en materia de Seguridad de la información

Atribuciones del GISI en materia de Seguridad de la información

Artículo 6. El Instituto a través del GISI, deberá:

I. Evaluar la aplicación de las acciones conforme a la Matriz de riesgos de TI del Instituto, orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información.
II. Actualizar las políticas en materia de Seguridad de la Información conforme a las disposiciones previstas por las leyes generales y locales en materia de Seguridad de la Información, 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 esta Política en todos los niveles de la estructura orgánica del Instituto;
IV. Concientizar a todo el personal del Instituto, en cuanto a la responsabilidad de la protección y buen uso de la información;
V. Definir mecanismos para la protección de la información; y
VI. Aplicar auditorías periódicas que aseguren que los equipos propiedad del Instituto cuenten con un mínimo de mecanismos de Seguridad de la Información.

Normativa en materia de Seguridad de la Información

Artículo 7. Lo no previsto en esta Política será resuelto conforme a los Lineamientos , los cuales contemplan las disposiciones previstas por leyes internacionales, nacionales y estatales vigentes que, en materia de Seguridad de la Información, sean aplicables para este Instituto.

Capítulo III
Del inventario de activos

Inventario de activos tecnológicos

Artículo 8. El inventario de activos de toda la infraestructura tecnológica (hardware y software) deberá mantenerse actualizado, con la finalidad de controlar la integridad de los equipos que están bajo responsabilidad de las personas usuarias de este Instituto. La integración y actualización del inventario estará a cargo de la UTSIT.

Uso aceptable de activos tecnológicos

Artículo 9. El uso aceptable de los activos tecnológicos con los que cuente este Instituto consistirá en asegurar su apropiada operación y administración mediante el cumplimiento de las premisas establecidas en los Lineamientos.

Gestión de capacidad de activos tecnológicos

Artículo 10. Toda solicitud de activos o servicios tecnológicos que se turnen a la UTSIT, deberán atender el protocolo dispuesto en los Lineamientos a fin de contar con los requerimientos específicos que permitan brindar el soporte en tiempo y forma.

Capítulo IV
De la protección y clasificación de la información

Clasificación de la información

Artículo 11. La información se clasificará en pública, reservada y confidencial de acuerdo con la Ley General de Transparencia y Acceso a la Información Pública y Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato y la demás normativa aplicable en la materia.

Protección de la información y datos personales

Artículo 12. El personal del Instituto deberá atender las disposiciones referidas en los Lineamientos respecto a la protección de la información y datos personales.

Capítulo V
De la gestión de incidentes de seguridad de la información

Gestión de incidentes

Artículo 13. Todo incidente en cuanto a Seguridad de la Información será reportado a la UTSIT para ser tratado de acuerdo con el protocolo previsto en los Lineamientos.

Concientización y sensibilización

Artículo 14. Se deberá contar con los recursos (asesoría, materiales, tiempo, instalaciones) necesarios, así como un plan de concientización y sensibilización aprobado por el GISI, con el propósito de concientizar y sensibilizar al personal del Instituto en materia de Seguridad de la Información.

Accesos físicos

Artículo 15. El personal del Instituto deberá contar con una identificación vigente proporcionada por el Instituto para su acceso a este, así mismo, en caso de que un tercero requiera acceso deberá realizar un registro conforme a lo dispuesto por la Coordinación Administrativa.

Para el caso de las áreas restringidas de acceso, se llevará a cabo el protocolo dispuesto en los Lineamientos.

Responsabilidad del equipo asignado

Artículo 16. Todo el personal que tenga asignada una estación de trabajo asumirá la responsabilidad del equipo asignado, durante y cuando se ausente de esta, debiendo observar para ello las disposiciones contenidas en los Lineamientos.

Escritorio lógico limpio

Artículo 17. Todo el personal que tenga asignada una computadora, de escritorio o portátil, tendrá únicamente en el escritorio lógico los accesos directos; en caso de contar con información sensible o crítica imprescindible para sus actividades laborales, esta deberá quedar resguardada toda vez que se ausente de su estación de trabajo.

Disposición o reutilización segura del equipo

Artículo 18. La disposición o reutilización segura de un equipo tendrá por objetivo garantizar que cualquier medio físico o intangible que contenga información y se desee reutilizar o rescindir de su uso, pase por un proceso de borrado o, en su caso, de destrucción seguro, mismo que se describe en los Lineamientos, así como el resguardo de la información necesaria para la atención de posibles Auditorías.

Capítulo VI
De los respaldos de la información

Respaldos de información

Artículo 19. El Instituto garantizará los recursos necesarios y suficientes para la administración de respaldos de seguridad o, en su caso, determinará la necesidad de contratar a un tercero, así como vigilar su correcto funcionamiento de acuerdo con lo establecido en los Lineamientos.

Capítulo VII
De la gestión de medios removibles

Uso de medios de almacenamiento removibles

Artículo 20. El uso de medios electrónicos de almacenamiento removibles solo aplicará para personal autorizado de acuerdo con el cumplimiento de sus funciones, manteniendo su obligación de buen uso y su compromiso de velar por su contenido conforme a lo dispuesto en los Lineamientos.

Seguridad en el uso de medios de almacenamiento removibles

Artículo 21. El Instituto deberá aplicar los mecanismos de seguridad que a nivel tecnológico se definen en los Lineamientos**.**

Capítulo VIII
Del correo electrónico

Servicios de correo electrónico

Artículo 22. Los servicios institucionales de correo electrónico deberán considerar:

I. La inserción de una leyenda de confidencialidad de la información en los correos institucionales emitidos;
II. El control institucional de la totalidad de los correos contenidos en las carpetas de las personas usuarias;
III. Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso;
IV. Técnicas de autenticación de correo electrónico que permita a la persona receptora comprobar que un correo electrónico fue enviado y autorizado por la Institución poseedora del dominio;
V. Que el envío por internet se realice con mecanismos de cifrado de la información, y
VI. Contar con los mecanismos necesarios para evitar la divulgación no autorizada de datos o información institucional por parte del personal.

Adicionalmente, cuando los servicios de correo electrónico sean contratados a una persona proveedora, este deberá garantizar, al menos:

I. Que el Instituto podrá acceder y tener a su disposición la totalidad de los correos contenidos en las carpetas de las personas usuarias, durante la vigencia de la contratación y al término de esta, en el formato establecido en los estándares técnicos aplicables, y entregar un respaldo de estos en medio no editable;
II. La suscripción de un Acuerdo de confidencialidad y no divulgación respecto de la información y datos personales relacionados con los correos electrónicos y personas usuarias del servicio prestado, el cual deberá prevenir efectos legales durante y después de la vigencia del contrato;
III. Que concluida la vigencia de los servicios contratados y una vez entregado el respaldo al Instituto, se elimine toda información y contenido de los correos electrónicos institucionales en la infraestructura de la persona proveedora, y
IV. Que los procedimientos de borrado seguro se efectúen ante la supervisión de personal designado por el GISI y se genere evidencia de su realización.

Uso de correo electrónico

Artículo 23. El personal que labore en este Instituto deberá atender a lo dispuesto en los Lineamientos con respecto al uso del correo electrónico institucional.

Capítulo IX
De los dispositivos móviles

Uso de dispositivos móviles

Artículo 24. Todo el personal que opere dispositivos móviles del Instituto asumirá la responsabilidad con la que se cuenta en cuanto a la protección y buen uso de la información contenida en estos.

Gestión de dispositivos móviles

Artículo 25. El Instituto respecto a los dispositivos móviles, deberá:

I. Contar con un control de comodatos e inventario del equipo asignado;
II. Especificar a las personas usuarias que el dispositivo móvil es para uso exclusivo en el desempeño de las funciones que tienen asignadas, y
III. Aplicar los mecanismos de seguridad, a nivel tecnológico, que sean definidos por los Lineamientos.

Capítulo X
Del control de red

Uso de red institucional

Artículo 26. El personal que utilice la red del Instituto es responsable de la protección y buen uso de la información que se transmita por dicho medio, asumiendo que el uso de la red institucional es exclusivamente para las actividades relacionadas con las necesidades del puesto, rol y función que desempeñen.

Acceso a internet

Artículo 27. El acceso a Internet previsto para el personal es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. Considerando que al ser personas usuarias con acceso a la red institucional deberán considerar que:

I. Serán sujetos de monitoreo en cuanto al tráfico de datos en la red institucional;
II. Está prohibida la transmisión de archivos que contengan información sensible o confidencial;
III. Toda actividad realizada con el servicio de navegación en Internet es de única responsabilidad de la persona usuaria;
IV. Se monitoreará el consumo de ancho de banda en sus navegaciones por Internet;

V. Está prohibido acceder a páginas electrónicas y servicios no autorizados por el Instituto o la descarga de software sin la autorización de la UTSIT;

VI. La utilización del servicio de Internet será únicamente para el desempeño de su función y puesto en el Instituto y no para propósitos personales, y

VII. Cualquier uso no adecuado del servicio de Internet será revisado por el GISI conforme a la Matriz de riesgos de TI vigente.

Capítulo XI
Del control de acceso lógico

Acceso lógico

Artículo 28. Respecto a los mecanismos de acceso y reserva a los activos informáticos generados y administrados por el Instituto, las personas usuarias deberán mantener la confidencialidad y el uso responsable de la información, así como el cumplimiento de lo dispuesto en los Lineamientos.

Seguridad contra malware

Artículo 29. Se deberá conocer y aplicar las medidas dispuestas en los Lineamientos para la prevención de "malware" como pueden ser virus, caballos de Troya, phishing, spyware, ransomware, gusanos de red o cualquier otro código diseñado para auto replicarse, dañar o afectar el desempeño o acceso al equipo de cómputo.

Capítulo XII
Del desarrollo seguro

Seguridad del desarrollo de software

Artículo 30. El desarrollo de software realizado por el Instituto o por algún tercero con el que colabore deberá contar con un proceso formal de seguridad, que aplique durante el ciclo de vida (SDLC) por sus siglas en inglés.

Derechos de propiedad intelectual

Artículo 31. Toda la información que se utilice o genere en el Instituto para el desempeño de funciones, incluyendo los datos creados en los sistemas de información, programas y código fuente, son propiedad de este.

Capítulo XIII
De las personas proveedoras

Relación con las personas proveedoras

Artículo 32. Las personas proveedoras con los que se tenga una relación de suministro deberán contar con un contrato vigente donde se establezcan cláusulas que los comprometan a proteger la seguridad de la información a la que se tenga acceso. Las UR solicitantes de la contratación deberán asegurarse de lo anterior, así como de contar con un Acuerdo de no divulgación y de confidencialidad.

Acuerdo de confidencialidad y no divulgación

Artículo 33. El Instituto respecto al Acuerdo de confidencialidad y no divulgación, contemplará las siguientes premisas:

I. Garantizar la confidencialidad, integridad y disponibilidad de la información;
II. Dar el cumplimiento legal y regulatorio que disponen las leyes generales y locales en materia de Seguridad de la Información, con el fin de evitar el mal uso de ella y dar certeza sobre el actuar del Instituto, y
III. Asegurar que la vigencia de los acuerdos esté alineada a los requerimientos legales aplicables.

Capítulo XIV
De la Auditoría en Seguridad de la Información

Deberes relacionados con Auditorías en Seguridad de la Información

Artículo 34. El Instituto, a través del GISI, deberá:

I. Garantizar que las Políticas de Seguridad de la Información sean auditadas de forma independiente en intervalos regulares;
II. Asegurar que los responsables de las UR revisen regularmente el cumplimiento del procesamiento de la información y procedimientos dentro de su área;
III. Supervisar que los sistemas de información sean revisados regularmente para el cumplimiento de las políticas y Lineamientos (pruebas de penetración, endurecimiento y análisis de vulnerabilidades), y
IV. Dar seguimiento a los resultados de las auditorías realizadas en materia de TI.

TRANSITORIOS

ÚNICO. La presente Política entrará en vigor quince días hábiles posteriores a su aprobación por la Junta Estatal Ejecutiva.