

RESOLUCIÓN QUE EMITE LA UNIDAD DE TRANSPARENCIA DEL INSTITUTO ESTATAL ELECTORAL DE AGUASCALIENTES, QUE DETERMINA COMO PROCEDENTE LA SOLICITUD 010055024000190, PRESENTADA EN FECHA 28 DE OCTUBRE DE DOS MIL VEINTICUATRO.

R E S U L T A N D O S

- I. En fecha cuatro de mayo del año dos mil quince, se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública (en adelante Ley General de Transparencia).
- II. En fecha siete de noviembre de dos mil dieciséis, se publicó en el Periódico Oficial del Estado de Aguascalientes la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes y sus Municipios (en adelante Ley de Transparencia Local).
- III. En fecha catorce de noviembre de dos mil dieciséis, se publicó en el Periódico Oficial del Estado de Aguascalientes el Reglamento de Transparencia del Instituto Estatal Electoral (en adelante Reglamento de Transparencia).
- IV. En fecha veinte de junio de dos mil diecisiete, en sesión extraordinaria el Consejo General del Instituto Estatal Electoral de Aguascalientes, aprobó el Acuerdo CG-A-18/17 mediante el cual se nombra a la Titular de la Unidad de Transparencia.
- V. En fecha veinticinco de septiembre de dos mil veintitrés, se publicó en el Periódico Oficial del Estado de Aguascalientes, el Acuerdo CG-A-31/2023 a través del cual el Consejo General del Instituto Estatal Electoral de Aguascalientes aprobó el Reglamento de Transparencia.

VI. En fecha 28 de octubre de dos mil veinticuatro, se recibió una solicitud de información en la Plataforma Nacional de Transparencia (en adelante PNT), bajo el número de folio **010055024000190**, en vía de la Ley General de Transparencia.

VII. En misma fecha del resultando que antecede, se asignó dicha solicitud a esta Unidad de Transparencia del Instituto Estatal Electoral de Aguascalientes, la cual tuvo por admitida, asignándole el número de expediente **IEE/UT/190/2024**.

VIII. Se notificó a la Coordinación de Informática el memorándum identificado con la clave **IEE/UT/M190/2024**, por medio del cual se le solicitó proporcionara a esta Unidad de Transparencia la información con que contara su área a efecto de dar contestación a la solicitud de información referida en el citado resultando VI.

IX. En fecha doce de noviembre de dos mil veinticuatro, la Coordinación de Informática, presentó a esta Unidad de Transparencia el oficio **IEE/CI/3039/2024** a través del cual otorga respuesta al memorando referido en el resultando previo; mismo que se anexa a la presente Resolución.

X. Se da contestación a la solicitud que nos atañe.

CONSIDERANDOS

COMPETENCIAS

1. SUJETOS OBLIGADOS EN EL ESTADO DE AGUASCALIENTES. Que de conformidad con los artículos 1 de la Ley General de Transparencia, 1 del Reglamento de Transparencia y 1° de la Ley de Transparencia Local, el Instituto Estatal Electoral de Aguascalientes es uno de los sujetos obligados a proporcionar la información pública requerida por cualquier persona física o moral, a efecto de garantizar el derecho de acceso a la información en poder del mismo, en términos de los ordenamientos legales referidos.

1.1 TITULAR DE UNIDAD DE TRANSPARENCIA. Que de acuerdo con lo establecido por los artículos 45 de la Ley General de Transparencia y 52 del Reglamento de Transparencia, la Lic. Shearley Ivett Álvarez Robles, es competente para realizar el trámite de la solicitud a la que se hace referencia en el resultando VI de la presente Resolución, al ostentar el carácter de titular de la Unidad de Transparencia del Instituto Estatal Electoral de Aguascalientes.

ESTUDIO DE FONDO

2. ANÁLISIS. Que de conformidad con los artículos 121, 122 y 124 de la Ley General de Transparencia, 71 y 72 de la Ley de Transparencia Local, y 22, 23, 24 y 29 del Reglamento de Transparencia, esta Unidad de Transparencia procedió a sustanciar la solicitud que nos ocupa, en razón de que la información creada, administrada y en posesión de este Instituto Estatal Electoral de Aguascalientes es considerada como un bien público accesible a cualquier persona en los términos de la ley de la materia, salvo las excepciones en ella señaladas; por lo tanto, con el objeto de proveer lo necesario para que la persona peticionaria pueda tener acceso a la información requerida, resultó conducente integrar el expediente administrativo correspondiente, procediendo a su análisis respectivo.

3. INFORMACIÓN PÚBLICA. Que el artículo 3° fracción VII de la Ley de Transparencia Local, establece que: *“Para los efectos de esta Ley se entiende por: VII. Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos y que se encuentre en posesión de los mismos con motivo del desempeño de sus funciones legales, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico...”*

4. FORMA DE CUMPLIMIENTO DE OBLIGACIÓN. El artículo 133 de la Ley General de Transparencia señala que el acceso se dará en la modalidad de entrega y, en su caso, de envío elegidos por la persona solicitante. Asimismo,

indica que en el caso de que la información no pueda entregarse o enviarse en la modalidad elegida, el sujeto obligado deberá ofrecer otra u otras modalidades de entrega. En cualquier caso, se deberá fundar y motivar la necesidad de ofrecer otras modalidades.

5. FECHA DE EMISIÓN DE RESOLUCIÓN. En atención al escrito de la solicitud **010550024000190** presentada a través de la PNT, resulta pertinente observar el término establecido en el artículo 71 de la Ley Local, mismo que otorga el plazo de diez días hábiles contados a partir del día siguiente al de su presentación para emitir una respuesta a la solicitud, en virtud de lo cual, el plazo de respuesta precluye el día doce de noviembre de dos mil veinticuatro, por lo que se establece que la presente Resolución se encuentra pronunciada en tiempo y forma legales.

6. SOLICITUD. Asimismo, de la solicitud **010550024000190** que nos ocupa, se desprende que se requiere de este sujeto obligado, lo siguiente:

“PREGUNTAS

APARTADO 1

1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
2. Señalar sí se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar sí se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.

3. Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institucion, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creacion; (ii) la fecha de implementacion, (iii) si es que se ha actualizado o modificado y en cuantas ocasiones; (iv) cuales areas participaron en la creacion de dicha estrategia ;
4. Informar si se emplea la firma electronica avanzada en la institucion;
5. Informar si se realizan simulacros sobre el plan de recuperacion de desastres o en caso de incidentes ciberneticos;
6. Señalar si se cuentan con lineamientos de programacion y desarrollo de sistemas informaticos seguros;
7. Informar si los servicios de centros de datos son propios, de otra institucion gubernamental o de un tercero;
8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;
9. Informar si se cuenta con un correo electronico institucional; e Informar si el correo electronico que se emplea en la institucion cuenta con lo siguiente: a) insercion de leyenda de confidencialidad de la informacion o en su caso de transparencia y acceso a la informacion; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, asi como programas informaticos que protejan del envio y recepcion de correos electronicos con software malicioso; e) cuenta con cifrado en el envio de informacion.
10. Informar si se cuentan con mecanismos para evitar la divulgacion no autorizada de datos o informacion Institucional por parte de los servidores publicos;
11. Informar si la pagina web de la institucion cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;
12. Informar si el personal responsable se ha capacitado en la implementacion del Protocolo Nacional Homologado para la Gestion de Incidentes Ciberneticos;
13. Informar si se cuentan con: a) Los mecanismos de supervision y evaluacion que permitan medir la efectividad de los controles de seguridad de la informacion; b) Indicadores que permitan medir el madurez institucional en la gestion de seguridad de la informacion;
14. Informar si dentro de la institucion se cuenta con un Programa de formacion en la cultura de la seguridad de la informacion o de ciberseguridad; y en caso afirmativo señalar: cuando se implementó.
15. Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados se cuenta con un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuando se adoptó y cuáles áreas participaron en su desarrollo e implementación?;
16. Informar si se cuenta con un modelo o sistema de comunicacion, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institucion, y en caso de ser

- afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;
17. Informar sobre si se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;
 18. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
 19. Informar si las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.
 20. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
 21. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
 22. Informar si algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar si se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;
 23. Informas si se cuenta con documento de seguridad en materia de protección de datos personales;
 24. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;
 25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
 26. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
 27. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.
 28. Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.

APARTADO 2

Solicito la siguiente información.

29. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
30. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;
31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;
32. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente Un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;
33. Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;
34. Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;
35. Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;
36. Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;
37. Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;
38. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
39. Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.
40. Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;
41. Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;

42. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
43. Informar si algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la ley en la materia; en caso afirmativo señalar si se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el INAI, en su caso;
44. Informar cada cuanto tiempo se actualizan las medidas de ciberseguridad dentro de la institución;
45. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;
47. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.
48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.

APARTADO 3

49. Indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial.

50. En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia.

51. En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad, favor de indicar el sujeto obligado que pudiera contener dicha información. Me gustaría saber de qué manera aplican medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al momento de brindar servicios a la ciudadanía. En caso de que no, saber si se tienen proyectos para aplicar dicho tipo de tecnología. A su vez se pide conocer lo siguiente:

52. Qué programas, algoritmos, sistemas de inteligencia artificial, sistemas de decisiones judiciales asistidas, algoritmos o programas de selección aleatoria de casos a jueces, tiene y opera.

53. El número de registros existentes de lo solicitado en el punto anterior.

- a. Las fechas de operación.
- b. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.
- c. Los contratos de su uso o adquisición.

54. ¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas de selección y asignación aleatoria de casos?

55. ¿Qué datos se utilizan para la selección y asignación aleatoria de casos?"(sic.)

7. PROCEDENCIA. Una vez establecida la naturaleza de la información requerida en el escrito de la solicitud materia de la presente Resolución, esta Unidad de Transparencia determina como **PROCEDENTE** la misma, con base a la respuesta otorgada por la Coordinación de Informática, la cual señala lo siguiente:

“Al respecto se da respuesta en los términos siguientes:

SECCIÓN 1

1. *Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;*

- Actualmente están por aprobarse políticas de seguridad informática que tendrá el Instituto Estatal Electoral de Aguascalientes.
- Así mismo se cuenta con el *REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO ESTATAL ELECTORAL DE AGUASCALIENTES.*

2. *Señalar sí se cuenta con lo siguiente:*

a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC;

- El Instituto cuenta actualmente con un *MANUAL DE INTEGRACIÓN Y FUNCIONAMIENTO DEL COMITÉ DE ADQUISICIONES, ARRENDAMIENTOS, Y SERVICIOS, DESINCORPORACIÓN Y ENAJENACIÓN DEL INSTITUTO ESTATAL ELECTORAL.*

c) un plan de continuidad de operaciones, y señalar la fecha de implementación;

- El Plan de Continuidad y Seguridad se implementó durante el Proceso Electoral Concurrente 2023 – 2024, en las actividades de diseño, implementación y operación del Sistema del Programa de Resultados Electorales Preliminares y el Sistema de Cómputos.

d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;

- De igual manera el Plan de Continuidad y Seguridad implementado durante el Proceso Electoral Concurrente 2023 - 2024 cuenta con un plan de recuperación ante desastres.

e) desarrollado e implementado un programa de gestión de vulnerabilidades;

- Actualmente el Instituto gestiona análisis de vulnerabilidades.

f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI);

- Actualmente se ha implementado el NIST como marco de ciberseguridad.

g) Informar sí se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó;

- Actualmente no se cuenta con una Política General de Seguridad de la Información.

h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;

- En cuestión informática se tienen identificados los equipos y/o activos que son de alta relevancia para su protección.

i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.

- Actualmente el proveedor de servicios de cómputo en la nube da acompañamiento y seguimiento junto con el equipo de Desarrollo, Seguridad y Operaciones para dar respuesta a los incidentes.

3. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente:

- No se cuenta con estrategia alguna de ciberseguridad.

(i) referir la fecha de creación;

- No aplica.

(ii) la fecha de implementación,

- No aplica.

(iii) sí es que se ha actualizado o modificado y en cuántas ocasiones;

- No aplica.

(iv) cuáles áreas participaron en la creación de dicha estrategia;

- No aplica.

4. *Informar si se emplea la firma electrónica avanzada en la institución;*

- Actualmente no se emplea la firma electrónica avanzada.

5. *Informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;*

- Durante el Proceso Electoral Concurrente 2023 - 2024 se realizaron simulacros cada semana respecto a incidentes cibernéticos.

6. *Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;*

- No se cuentan lineamientos, pero si se aplican buenas prácticas y constante análisis de vulnerabilidades dentro del desarrollo.

7. *Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;*

- Los centros de datos son de un proveedor tercero.

8. *Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;*

- Actualmente no se cuentan con lineamientos, la seguridad de las videollamadas corresponde a un administrador en su mayoría operado por la Coordinación de Informática.

9. *Informar si se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente:*

- Si se cuenta con correo electrónico institucional.

a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información;

- Si se cuenta con la inserción de la leyenda de confidencialidad de la información.

c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;

- Si se cuenta con el control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios.

d) 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;

- Si se cuenta con soluciones para evitar correo malicioso, detección de SPAM y malware.

e) cuenta con cifrado en el envío de información.

- Si se cuenta con un cifrado en el envío de la información

10. *Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;*

- Se cuentan con mecanismos, sin embargo, dicha información es de carácter sensible.

11. *Informar si la página web de la institución cuenta con:*

a) aviso de privacidad;

- Si cuenta con aviso de privacidad, consultable en la liga: <https://ieeags.mx/aviso-privacidad/>

b) certificados digitales vigentes;

- Si cuenta con certificados digitales vigentes.

12. *Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;*

- No se encuentra capacitado.

13. *Informar si se cuentan con:*

a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información;

- No se cuenta con ello.

b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;

- No se cuenta con ello.

- • •
 - 14. *Informar si dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó.*
 - Actualmente no se cuenta con un programa de formación en la cultura de seguridad de la información.

- 15. *Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados se cuenta con un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;*
- Se cuenta con el REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO ESTATAL ELECTORAL DE AGUASCALIENTES.

- 16. *Informar si se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;*
- La Coordinación de Presidencia y la Coordinación de Comunicación Social determinan los mecanismos y planes de acción en temas de comunicación e información hacia la ciudadanía.

- 17. *Informar sobre si se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;*
- Todos los datos que actualmente se tienen son de carácter público, por lo tanto, no habría brechas de seguridad.

18. *Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;*

- El Instituto si cuenta con procedimiento interno que regula el traslado de activos fuera y dentro de las instalaciones, a cargo de la Dirección Administrativa del Instituto.

19. *Informar si las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias*

(i) *transparencia;*

- Si se cuenta.

(ii) *protección de datos personales;*

- Si se cuenta.

(iii) *archivos públicos; o,*

- Si se cuenta.

(iv) *seguridad de la información.*

- Si se cuenta.

20. *Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;*

- Si se han presentado brechas, sin embargo, la información relativa a ello se trata de datos sensibles y confidenciales que por cuestiones de protección y seguridad informática no se pueden revelar.

21. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;

- Al ser una institución pública, los datos que se publican en nuestros sitios son de total acceso a la ciudadanía.

22. Informar si algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar si se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;

- Para el tratamiento de datos el Instituto cuenta con un REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO ESTATAL ELECTORAL DE AGUASCALIENTES.

23. Informar si se cuenta con documento de seguridad en materia de protección de datos personales;

- Actualmente se cuenta con un apartado extenso para los avisos de Protección de Datos Personales: <https://ieeags.mx/avisos-privacidad/>

24. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;

- La Coordinación de Presidencia y la Coordinación de Comunicación Social determinan los mecanismos y planes de acción en temas de comunicación e información hacia la ciudadanía.

25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;

- Se actualizan una vez al año.

26. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;

- Durante el Proceso Electoral Concurrente 2023 – 2024, se llevaron a cabo auditorías por parte del ente Auditor de la Centro de Física Aplicada y Tecnología Avanzada de la Universidad Nacional Autónoma de México, Campus Juriquilla.

27. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.

- No se cuenta actualmente con un help desk.

28. Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.

- Esta pregunta hace referencia a otra institución pública, de la cual este Instituto no cuenta con información.

SECCIÓN 2

Solicito la siguiente información.

29. *Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;*

- Actualmente no se cuenta con un gobierno de seguridad de la información.

30. *Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente.*

- No se cuenta con estrategia alguna de ciberseguridad.

(i) referir la fecha de creación;

- No aplica.

(ii) la fecha de implementación,

- No aplica.

(iii) sí es que se ha actualizado o modificado y en cuántas ocasiones;

- No aplica.

(iv) cuáles áreas participaron en la creación de dicha estrategia;

- No aplica.

- 31. *Informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;*
 - Actualmente no se cuenta con sistema alguno de gestión de seguridad.

32. *Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente: Un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;*

- Actualmente están por aprobarse políticas de seguridad informática que tendrá el Instituto Estatal Electoral.
- Así mismo se cuenta con el REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO ESTATAL ELECTORAL DE AGUASCALIENTES.

33. *Informar si es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;*

- Existe el Plan de Continuidad Institucional, se implementó desde que se dio inicio a los trabajos del Programa de Resultados Electorales Preliminares durante el Proceso Electoral Concurrente 2023 – 2024.

34. *Informar si se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;*

- En caso de que se presente algún incidente, la Coordinación de Presidencia y la Coordinación de Comunicación Social determinan los mecanismos y planes de acción en temas de comunicación e información hacia la ciudadanía.

35. *Informar sobre si se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;*

- El tratamiento de datos personales se realiza de conformidad con el REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO ESTATAL ELECTORAL DE AGUASCALIENTES.

36. *Informar si se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;*

- Actualmente no se llevan capacitaciones a los servidores públicos sobre temas de ciberseguridad.

37. *Informar si se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;*

- Si se cuenta con un procedimiento interno para la mitigación de amenazas o vulnerabilidades, el área encargada de resolverlo es la Coordinación de informática y la Dirección Jurídica del instituto.

38. *Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;*

- El Instituto si cuenta con procedimiento interno que regula el traslado de activos fuera y dentro de las instalaciones, a cargo de la Dirección Administrativa del Instituto.

39. *Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias*
(i) transparencia;

- Si se cuenta.

(ii) protección de datos personales;

- Si se cuenta.

(iii) archivos públicos; o,

- Si se cuenta.

(iv) seguridad de la información.

- Si se cuenta.

40. *Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;*

- Si se han presentado brechas, sin embargo, la información relativa a ello se trata de datos sensibles y confidenciales que por cuestiones de protección y seguridad informática no se pueden revelar.

41. *Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;*

- No se cuenta con ello.

42. *Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;*

- El tratamiento de datos personales se realiza de conformidad con el REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO ESTATAL ELECTORAL DE AGUASCALIENTES. Los datos son de carácter público.

43. *Informar si algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la ley en la materia; en caso afirmativo señalar si se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;*

- El tratamiento de datos personales se realiza de conformidad con el REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO ESTATAL ELECTORAL DE AGUASCALIENTES. Los datos son de carácter público.

44. *Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;*

- Se actualizan una vez al año.

45. *Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;*

- Durante el Proceso Electoral Concurrente 2023 – 2024, se llevaron a cabo auditorías por parte del ente Auditor de la Centro de Física Aplicada y Tecnología Avanzada de la Universidad Nacional Autónoma de México, Campus Juriquilla.

46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;

- La metodología con la cual se gestionan los incidentes es trabajada bajo el marco NIST y MAGERIT.

47. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.

- No se cuenta actualmente con un help desk.

48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.

- El proveedor de servicios de cómputo en la nube da acompañamiento y seguimiento junto con el equipo de Desarrollo, Seguridad y Operaciones para dar respuesta a los incidentes.

SECCIÓN 3

49. Indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial.

50. En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia.

51. En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad, favor de indicar el sujeto obligado que pudiera contener dicha información. Me gustaría saber de qué manera aplican medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al momento de brindar servicios a la ciudadanía. En caso de que no, saber si se tienen proyectos para aplicar dicho tipo de tecnología. A su vez se pide conocer lo siguiente:

52. Qué programas, algoritmos, sistemas de inteligencia artificial, sistemas de decisiones judiciales asistidas, algoritmos o programas de selección aleatoria de casos a jueces, tiene y opera.

53. El número de registros existentes de lo solicitado en el punto anterior.

- a. Las fechas de operación.
- b. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.
- c. Los contratos de su uso o adquisición.

54. ¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas de selección y asignación aleatoria de casos?

55. ¿Qué datos se utilizan para la selección y asignación aleatoria de casos? (sic)

Al respecto informo que el Instituto no sustancia procedimientos en línea relacionados con juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial. Por lo anterior, la SECCIÓN 3, que contemplan la preguntas 49 a 54, se contesta en su conjunto de forma negativa. “(sic.)”

Por lo anterior, conforme a los resultandos y considerandos anteriores y con fundamento en los artículos 1, 45, 121, 122, 124 y 130 de la Ley General de Transparencia, 1°, 3° fracción VII y 71 de la Ley de Transparencia Local, y 1, 22, 23, 24, 29 y 42 del Reglamento de Transparencia, esta Unidad de Transparencia, **RESUELVE:**

PRIMERO. Esta Unidad de Transparencia es competente para resolver la solicitud bajo el número de folio **010550024000190**, lo anterior de conformidad con lo establecido por los considerandos de la presente Resolución.

SEGUNDO. Esta Unidad de Transparencia determina como **PROCEDENTE** la presente solicitud de información en términos de lo establecido en el considerando 7 de la actual Resolución.

TERCERO. La presente Resolución surtirá efectos a partir de su emisión.

CUARTO. Notifíquese la presente Resolución a la persona solicitante por correo electrónico conforme con lo establecido en el tercer párrafo del artículo 71 de la Ley de Transparencia Local.

QUINTO. Se le hace saber a la persona solicitante, que cuenta con el término de quince días hábiles siguientes contados a partir de la notificación de la presente determinación, para presentar Recurso de Revisión en contra de la presente Resolución ante el Instituto de Transparencia del Estado de Aguascalientes o la Unidad de Transparencia del Instituto Estatal Electoral de Aguascalientes, en términos de lo dispuesto por el Capítulo I, Título Octavo de la Ley General de Transparencia, así como el 75 de la Ley de Transparencia Local.

La presente Resolución fue emitida por la Unidad de Transparencia del Instituto Estatal Electoral de Aguascalientes, en fecha doce de noviembre de dos mil veinticuatro. **CONSTE.** -----

LA TITULAR DE TRANSPARENCIA

LIC. SHEARLEY IVETT ALVAREZ ROBLES