

Aguascalientes, Ags., a 11 de noviembre de 2024

Asunto: Se atiende solicitud de transparencia 010055024000190.

LIC. SHEARLEY IVETT ÁLVAREZ ROBLES
TITULAR DE LA UNIDAD DE TRANSPARENCIA
PRESENTE.



En atención al oficio de fecha veintiocho de octubre del año en curso, identificado como memorándum IEE/UT/M190/2024, por medio del cual se requiere a la Coordinación de Informática, a efecto de que proporcione información correspondiente a la solicitud de transparencia, identificada con el número 010055024000190, recibida por la Plataforma Nacional de Transparencia (PNT). Al respecto de 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 si 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 si 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 si 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 si 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 si es que se cuenta con una estrategia de ciberseguridad dentro de la instituci3n, en caso de respuesta afirmativa, informar lo siguiente:*

- No se cuenta con estrategia alguna de ciberseguridad.

(i) referir la fecha de creaci3n;

- No aplica.

(ii) la fecha de implementaci3n,

- No aplica.

(iii) si es que se ha actualizado o modificado y en cu3ntas ocasiones;

- No aplica.

(iv) cu3les 3reas participaron en la creaci3n de dicha estrategia;

- No aplica.

4. *Informar si se emplea la firma electr3nica avanzada en la instituci3n;*

- Actualmente no se emplea la firma electr3nica avanzada.

5. *Informar si se realizan simulacros sobre el plan de recuperaci3n de desastres o en caso de incidentes cibern3ticos;*

- Durante el Proceso Electoral Concurrente 2023 - 2024 se realizaron simulacros cada semana respecto a incidentes cibern3ticos.

6. *Se3alar si se cuentan con lineamientos de programaci3n y desarrollo de sistemas inform3ticos seguros;*

- No se cuentan lineamientos, pero si se aplican buenas pr3cticas y constante an3lisis de vulnerabilidades dentro del desarrollo.

7. *Informar si los servicios de centros de datos son propios, de otra instituci3n 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/avisos-privacidad/>

b) certificados digitales vigentes;

- Si cuenta con certificados digitales vigentes.

12. Informar sí 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 sí 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 sí 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 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.

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 si 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 si 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 sí 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 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?;*

- 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 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.

40. *Informar si 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 si 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.

Sin más por el momento, quedo a sus órdenes para cualquier duda o aclaración y aprovecho la oportunidad para enviarle un cordial saludo.


ATENTAMENTE

L.I. JOSÉ DE JESÚS JAIME CARACHURE.
COORDINADOR DE INFORMÁTICA DEL INSTITUTO
ESTATAL ELECTORAL DE AGUASCALIENTES

C.c.p. Archivo.