Folio No.199/2024

Oficio IEEZ-01/UT/530/2024
Guadalupe, Zac. 11 de noviembre de 2024

A quien corresponda
Presente

Por este medio, y por instrucciones del Mtro. Juan Manuel Frausto Ruedas, Consejero Presidente del Instituto Electoral del Estado de Zacatecas, y en atención a su solicitud de información que presentó ante la Autoridad Administrativa Electoral Local a través de la Plataforma Nacional de Transparencia, el día veintiuno de octubre del año en curso, en la cual, textualmente solicita lo siguiente:

"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 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 ;*
4. *Informar sí se emplea la firma electrónica avanzada en la institución;*
5. *Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;*
6. *Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;*
7. *Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;*
8. *Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;*

9. *Informar sí se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; 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, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información.*
10. *Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;*
11. *Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) 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;*
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; b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;*
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.*
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?;*
16. *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;*
17. *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;*
18. *Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;*
19. *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.*
20. *Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;*
21. *Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;*
22. *Informar sí 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 sí 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 sí se cuenta con documento de seguridad en materia de protección de datos personales;*
24. *Informar sí 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 sí 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 sí 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 sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;*
43. *Informar sí 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 ey en la materia; en caso afirmativo señalar sí 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;*
44. *Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;*
45. *Informar sí 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 se selección y asignación aleatoria de casos?

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

Al respecto, con base en la información proporcionada por las Direcciones Ejecutivas de Sistemas Informáticos, y la de Jurídicos, se comunica lo siguiente:

En relación a la información requerida en los **puntos 1, 4, 8, 13, 16, 22, 24, 28, 29, 30, 33, 34, 41, 43, 46, 49, 50, 51, 52, 53, 54 y 55** se comunica que la Autoridad Administrativa Electoral Local, no ha generado, por lo tanto, no cuenta en su archivo institucional con información al respecto.

En cuanto a lo solicitado en el **punto 2**, se informa que se cuenta únicamente con: Un Inventario Institucional de bienes y servicios de TIC, y en el Programa de Resultados Electorales Preliminares (PREP) se cuenta con un plan de continuidad de operaciones y su implementación fue a partir del año 2016. Así como, una política general de seguridad de la información implementada desde el 2021 y un Equipo de Respuesta a Incidentes Cibernéticos.

Por lo que hace a lo solicitado en el **punto 3,** se informa que la estrategia de ciberseguridad dentro de la institución se basa en:

- El uso de las buenas prácticas.
- El uso de Políticas de Seguridad Informática.
- La Dirección Ejecutiva de Sistemas Informáticos es el área que participa en el desarrollo de la estrategia.

En relación a lo formulado en el **punto 5,** se comunica que sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos en el Programa de Resultados Electorales Preliminares (PREP).

Respecto de lo solicitado en los **puntos 6 y 7,** se informa que se sigue el uso de buenas prácticas para la programación y desarrollo de sistemas informáticos seguros, y los servicios de centros de datos son propios y de la nube.

En lo que atañe a lo requerido en el **punto 9**, se informa que sí se cuenta con un correo electrónico institucional, el cual cuenta con lo siguiente:

a) La inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información, depende directamente del usuario;
c) NO hay un control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;
d) SÍ hay 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;
e) SÍ se cuenta con cifrado en el envío de información, la proporciona la plataforma del correo electrónico.

En cuanto a lo solicitado en el **punto 10**, se comunica que la Autoridad Administrativa Electoral Local, cuenta con un Reglamento de Transparencia y Acceso a la Información Pública del Instituto Electoral del Estado de Zacatecas, y los Lineamientos que reglamentan las condiciones generales, los derechos, las obligaciones y las prohibiciones de trabajo del Personal del Instituto Electoral del Estado de Zacatecas, en los cuales se contempla la obligación del personal de guardar reserva de los asuntos de los que tenga conocimiento con motivo de su trabajo, marco normativo disponible para su consulta en las siguientes ligas:
https://ieez.org.mx/MJ/2023/Reglamento_de_Transparencia_y_Acceso_a_la_Informacion_Publica_del_IEEZ_15_Dic_2022.docx
https://ieez.org.mx/Tr/ieez/DEAJ/DEAJ_39/Anexos/Lineamientos_Condiciones.pdf

En lo concerniente a la información solicitada en el **punto 11,** se comunica que la Autoridad Administrativa Electoral Local, cuenta con sus respectivos Avisos de Privacidad, en términos de los datos personales que se recopilan en el ejercicio de sus atribuciones, los cuales están disponibles para su consulta directa, a través de la liga: https://ieez.org.mx/Tr/ieez/Avisos_de_Privacidad_2024.html.

En lo que atañe a lo requerido en el **punto 12**, se informa que el personal responsable, tiene conocimiento del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

En relación con lo solicitado en el **punto 14,** se informa que sí se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y se implementó desde el año 2022.

Respecto de lo solicitado en los **puntos 15, 17**, **22, 23, 31, 32, 35 y 42** se comunica que actualmente se está trabajando el documento de Medidas de Seguridad de los Sistemas de Datos Personales del Instituto Electoral del Estado de Zacatecas, en el cual se contempla entre otros rubros un apartado de análisis de brecha.

En relación a lo requerido en el **punto 18,** se informa que el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos se atienden las Políticas de Seguridad Informática.

Por lo que hace a lo requerido en los **puntos 19 y 39,** se informa que el personal adscrito a la Unidad de Transparencia, ha participado en diversos cursos, seminarios y o capacitaciones en materia de Acceso a la información, transparencia, archivo, protección de datos personales, y seguridad de la información.

En cuanto a lo solicitado en los **puntos 20 y 40**, se comunica que a la fecha no se han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud.

Por lo que hace a lo solicitado en los **puntos 25 y 44** se comunica que, ante un problema de ciberseguridad dentro de la institución, se reacciona al tener conocimiento del evento.

En relación a lo solicitado en los **puntos 26 y 45** se informa que con la implementación del Programa de Resultados Electorales Preliminares (PREP) se llevan auditorías de seguridad en materia de ciberseguridad cada 3 años.

En cuanto a lo solicitado en los **puntos 27, 47 y 48**, se informa que sí se cuenta con un help desk que recoge las incidencias reportadas por los servidores públicos y es interno.

En relación a lo requerido en el **punto 36,** se informa que sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad:

- Manejo de información.
- Resguardo de bienes informáticos.
- Uso de la red Institucional.
- Uso de bienes informáticos.
- Mantenimiento de los bienes informáticos.
- Uso del correo electrónico.
- Controles contra códigos maliciosos.
- Uso de sistemas institucionales.
- Uso del servicio de internet.

Respecto de lo solicitado en el **punto 37,** se comunica que sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y el área encargada de atender la incidencia es la Dirección Ejecutiva de Sistemas Informáticos.

Oficio IEEZ-01/UT/530/2024
Guadalupe, Zac. 11 de noviembre de 2024

De igual manera, se informa que en caso de inconformidad con la respuesta que se le proporciona, podrá interponer el Recurso de Revisión, por sí o a través de su representante, de manera directa o por medio electrónico ante el Instituto Zacatecano de Transparencia, Acceso a la Información y Protección de Datos Personales, ante la Unidad de Transparencia del Instituto Electoral del Estado de Zacatecas, o bien, a través de la Plataforma Nacional de Transparencia en el apartado de Quejas, en la liga https://www.plataformadetransparencia.org.mx/web/guest/inicio, dentro de los 15 días hábiles siguientes a la fecha de la notificación de la presente.

Sin otro particular por el momento, reitero a usted mi consideración respetuosa.

A t e n t a m e n t e

Mtro. Jorge Chiquito Díaz de León
Secretario Ejecutivo

C.c.p.- Mtro. Juan Manuel Frausto Ruedas. Consejero Presidente del Instituto Electoral del Estado de Zacatecas. - Para su conocimiento. - Presente.
Mtra. Sandra Valdez Rodríguez. Consejera Electoral y Presidenta del Comité de Transparencia. - Mismo fin.
Lic. Martha Valdez López. Titular de la Unidad de Transparencia. - Mismo fin.
Archivo