INSTITUTO ESTATAL ELECTORAL CHIHUAHUA

31 OCT 2024
14:58 Hrs.
RECIBIDO
UNIDAD DE TRANSPARENCIA

INSTITUTO ESTATAL ELECTORAL
CHIHUAHUA

Chihuahua, Chih. A 31 de octubre de 2024
**Interoficio: I-IEE-DS-388/2024**
**ASUNTO:** Respuesta de transparencia

**Lic. Nancy Ivonne Ruelas Nevárez**
**Titular de la Unidad de Transparencia Acceso a la Información y Protección de Datos Personales.**
**Presente:**

Saludos cordiales, por medio del presente, me permito dar respuesta a la información solicitada por medio del interoficio I-IEE-UTAIPDP-223/2024 con número de folio 080159324000206, donde se solicita lo siguiente y se da respuesta a cada una de las preguntas:

## APARTADO 1

1- Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuales áreas participan;

R. No se cuenta.

2- Señalar si se cuenta con lo siguiente:

a) Un marco de mejores practicas 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 las TIC y de seguridad de la información;

R. No se cuenta

b) informar si se cuenta con un inventario institucional de bienes y servicios en materia de las TIC

R.Si se tiene un inventario.

c) Un plan de continuidad de operaciones, y señalar la fecha de implementación.

R. Solo PREP

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

R. No se cuenta con un plan de recuperación.

e) Desarrollo e implementado un programa de gestión de vulnerabilidades.

R. No se cuenta con un desarrollo.

f) Marco de gestión de Seguridad de la información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI).

R. No se cuenta

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

R. No se cuenta

h) Informar si se cuenta con un diagnóstico de identificación de los procesos y los activos esenciales de la institución.

R. Si, se cuenta con la implementación del ISO 9000:2015

i) Informar si se cuenta con un Equipo de Respuesta de Incidentes de Seguridad de la información (ERISC) o Equipo de Respuesta de Incidentes Cibernéticos o en su caso SOC.

R. No se cuenta

3- Informar si se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente:

R. No se cuenta

i) referir la fecha de creación; ii) La fecha de implementación; iii) si es que se a actualizado o modificado y en cuantas ocasiones; iv) cuales áreas participaron en la creación de dicha estrategia.

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

R. No se emplea la firma electrónica.

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

R. No se realizan simulacros.

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

R. No se cuenta con lineamientos de programación y desarrollo de sistemas.

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

R. Son propio y esta alojada en AWS y Azure

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

R. No se cuentan.

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;

R. No se cuenta.

b) Control institucional de la totalidad de los correos contenidos en las carpetas de usuarios;

R. Si se cuenta con el control institucional en su totalidad.

c) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos de software malicioso;

R. Si se cuenta

d) Cuenta con cifrado en el envió de la información

R. No se cuenta

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

R. No se cuenta

11- Informar si la página web de la institución cuenta con:

a) Aviso de privacidad

R. Si se cuenta.

b) Certificados digitales vigentes

R. Si se tienen certificados vigentes.

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

R. No se han capacitado.

13-Informar si se cuenta con:

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

R. No se cuentan

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

R. No se cuentan

14-Informar sí dentro de la institución se cuenta con un programa de formación en la cultura de la seguridad de la información o ciberseguridad; y en caso afirmativo señalar: cuando se implementó.

R. No se cuenta,

Otros datos para facilitar su localización:

15-Informar si de conformidad con la Ley General de Protección de Datos Personal en Posesión de Sujetos Obligados se cuenta con un sistema de gestión de protección datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuando se adoptó y cuales áreas participaron en su desarrollo e implementación?

R. No se cuenta.

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 cuando se implementó

R. No se cuenta.

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 cuales áreas de la organización participan en su implementación y desde cuando se implementó.

R. No se cuenta

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

R.No se cuenta.

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

j) transparencia; ii) protección de datos personales; iii) archivos públicos; o, iv) seguridad de la información.

R. No se cuenta.

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

R.solo una vez en el 2023

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

R. No se cuenta

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 se se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuales han sido las recomendaciones vertidas por el INAI, en su caso;

R.No se cuenta

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

R.No se cuenta

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

R.No se cuenta

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

R.Cada año

26-Informar si se llevan auditorias de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad.

R. Por año

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.

R. Si y es interno.

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

R.No se tiene este tipo de páginas web

**APARTADO 2**

29-Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuales áreas participan.

R.No se cuenta

30-Informar si 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)si es que se ha actualizado o modificado y en cuantas ocasiones; iv) cuales áreas participaron en la creación de dicha estrategia;

R.No se cuenta

31-Informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución.

R.No se cuenta

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 cuando se adoptó y cuáles áreas participaron en su desarrollo e implementación?

R.No se cuenta

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 cuando se implementó.

R.No se cuenta

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 cuando se implementó.

R.No se cuenta

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 cuando se implementó.

R.No se cuenta

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

R.Si cada año

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.

R.No se tiene documentado y es el área de Soporte Técnico la que atiende los casos.

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

R.No se cuenta

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, ii) protección de datos personales, iii) archivos públicos; o, iv) seguridad de la información.

R.No se cuenta

40-Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuantas.

R.Uno en el 2013 a la página institucional

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 cuando se implementa.

R.No se cuenta

42-Informar si se han adoptado esquemas de mejores practicas en materia de protección de datos personales y señalar cuales son.

R.No se cuenta

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 cuales han sido las recomendaciones vertidas por el INAI, en su caso;

R.No se cuenta

44-Informar cada cuanto tiempo se actualizan las medidas de ciberseguridad dentro de la institución.

R.Cada año

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

R.Uno por año externamente

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

R. No se cuenta

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.

R.Si es interno

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

R.El Departamento de Soporté Técnico.

**APARTADO 3**

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

R.No e cuenta

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.

R.No se cuenta

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 que 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:

    R.No se tiene conocimiento

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

    R.No aplica

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

R. No aplica

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?

R.No aplica

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

R.No aplica

Atentamente:

Ing. Héctor Enrique Martínez Dorador
Director de Sistemas