INSTRUCTIVO DE NOTIFICACIÓN

CEEPAC/UIP/004/INF/304/2024
San Luis Potosí, S.L.P, 06 de noviembre de 2024

C.
P R E S E N T E.-

En atención a su solicitud de información recibida vía **PLATAFORMA NACIONAL DE TRANSPARENCIA,** con número de folio **240477424000202,** quedando registrada en esta Unidad de Transparencia con número de expediente **CEEPAC/UIP/004/INF/304/2024** donde el Consejo Estatal Electoral y de Participación Ciudadana figura como ente obligado, recibida en esta Unidad de Transparencia con fecha 22 de octubre de 2024 relativa a:

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.*
49.

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?.

Una vez que se ha revisado y analizado el contenido de su solicitud y turnado a la Dirección de Sistemas de este organismo electoral, área competente para dar respuesta, se hace de su conocimiento el cuestionario respondido que remite a esta Unidad de Transparencia y que se anexa al presente instructivo de notificación.

De igual manera a continuación se proporciona respuesta a las preguntas que la Dirección de Sistemas no fue competente para responder al tratarse de información relativa a esta Unidad de Transparencia:

11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes.

Respuesta: Si se cuenta con avisos de privacidad integral y simplificado

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?

Respuesta: Este Organismo Electoral atiende los deberes establecidos en la normatividad citada en cuanto a seguridad y confidencial de datos personales, por lo que para su fortalecimiento se mantiene capacitación continua al funcionariado electoral.

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;

Respuesta: La Unidad de Transparencia de este Organismo Electoral participa en la comunicación con las personas titulares de datos personales para el caso que exista una vulneración de datos personales.

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.

Respuesta: Si cuentan con capacitación en los temas señalados por la persona peticionaria.

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

Respuesta: Si, capacitaciones, jornadas de elaboración de avisos de privacidad para sensibilizar a las personas servidoras públicas sobre el manejo de datos personales.

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;

Respuesta: Si se tienen sistemas con manejo de datos personales, y la intitucion se está conforme a lo establecido en la Ley de Protección de Datos Personales en Posesión de los Subetos Obligados en el Estado de San Luis Potosí

23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales;

Respuesta: No se cuenta con documento de seguridad. No se cuenta con documento de seguridad, pero se atienden todos los requerimientos necesarios para salvaguardar los datos personales en posesión 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?;

Respuesta: Este Organismo Electoral es una institución de carácter público, por lo que la citada Ley no tiene aplicación sobre esta entidad.

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;

Respuesta: Si se tiene y es a través de la Unidad de Transparencia.

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.

Respuesta: Si se cuenta y es a través de la Unidad de Transparencia.

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.

Respuesta: Si cuenta con conocimientos en las materias señaladas por la parte peticionaria.

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

Respuesta: Si, a través de capacitación al funcionariado.

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.

Respuesta: Si se manejan datos personales en la institución y no se han tenido evaluaciones de datos personales.

En caso de inconformidad con la respuesta por este medio otorgada, cuenta con un plazo de quince días siguientes a la fecha de la notificación de la respuesta, o del vencimiento del plazo para su notificación para presentar el recurso de Revisión ante la Comisión Estatal de Garantía de Acceso a la Información Pública, o ante la Unidad de Transparencia que haya conocido de la Solicitud de conformidad con lo establecido en los artículos 166,167 y demás relativos de la Ley de Transparencia y Acceso a la Información Pública del Estado.

Atentamente P.P.

Lcda. Iris Adriana Rivera Nava
Directora de la Unidad de Transparencia
Consejo Estatal Electoral y de Participación Ciudadana

CONSEJO ESTATAL ELECTORAL Y DE PARTICIPACIÓN CIUDADANA
CEEPAC 11:32 m

CEEPAC
Consejo Estatal Electoral y de Participación Ciudadana de S.L.P.

Memorando

05 NOV. 2024
RECIBIDO
UNIDAD DE TRANSPARENCIA

Para: Lic. Iris Adriana Rivera Nava. Directora de la Unidad de Transparencia.

C.C.: Mtro. Mauro Eugenio blanco Martínez. Secretario Ejecutiva

De: Edgar Gerardo Sánchez Salazar. Director de Sistemas

Asunto: Respuesta Solicitud CEEPAC/UT/004/INF/304/2024.

Fecha: 05 de noviembre de 2024

En respuesta a la ***Solicitud de Información Pública CEEPAC/UT/004/INF/304/2024***, le comento 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;

Respuesta:
De la definición "***El gobierno de seguridad de la información consiste en el liderazgo, estructura organizacional y proceso para proteger la información***", se establece que se cuentan con procedimientos de respaldo de información y protección de esta a través de procedimientos que se aplican en respaldos de información, así como controles de sistema operativo para acceso controlado a recurso compartidos. Estas actividades son implementadas y ejecutadas por la Dirección de Sistemas.

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;

      Respuesta:
      No se cuenta.

      Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC;

      Respuesta:
      Si se cuenta

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

      Respuesta

No se cuenta

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

Respuesta:
Si se cuenta, a partir del mes de abril del año 2011

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

Respuesta:
No se cuenta

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

Respuesta:
Respuesta:
No se cuenta

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

Respuesta:
Si se cuenta, no se ha implementado

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

Respuesta:
No se cuenta

h) 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.

Respuesta:
No se cuenta

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 ;

Respuesta:
No se cuenta

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

Respuesta:
No

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

Respuesta:
No

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

Respuesta:

No

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

Respuesta:
Se tienen ambos servicios, centro de datos propios y con un tercero no gubernamental.

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

Respuesta:
Se cuenta con aplicaciones de trabaja remoto y videollamadas, sin lineamientos

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:

   Si se cuentan con correos electrónicos institucionales.

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

   Respuesta:
   Sí, depende del usuario

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

   Respuesta:
   Control sobre las cuentas, adición y eliminación sí, no se cuenta con permisos para entrar a los buzones de los usuarios.

   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 con software malicioso;

   Respuesta:
   Sí, con las herramientas de GMAIL.

   d) cuenta con cifrado en el envío de información.

   Respuesta:
   Sí, por parte de GMAIL.

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

Respuesta:
No se cuenta

~~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;

Respuesta:
No

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;

Respuesta:
No

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

Respuesta:
No

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.

Respuesta:
No se cuenta

~~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;

Respuesta:
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 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;

Respuesta:
No se cuenta

~~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;

Respuesta:
Si, específicamente en la página Web institucional.

~~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;

Respuesta:
No se cuenta

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

Respuesta:
No se ha implementado

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

Respuesta:
Se han hecho auditorias al servidor de aplicaciones del organismo en el año 2022 y 2024 por parte de la Universidad Autónoma de San Luis Potosí.

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.

Respuesta:
Se incorpora solamente para los Procesos Electorales para dar soporte a las oficinas descentralizadas y es interno.

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

Respuesta:
En este caso, el Tribunal deberá responder esta pregunta.

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;

Respuesta:
Misma que en el Apartado 1, pregunta 1.

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 ;

Respuesta:
Misma que en el Apartado 1, pregunta 2.

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;

Respuesta:
Misma que en el Apartado 1, pregunta 2.

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;

Respuesta:
Misma que en el Apartado 1, pregunta 16.

~~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;

Respuesta:
No se cuenta

~~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;

Respuesta:
Misma que en el Apartado 1, pregunta 18.

~~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;

Respuesta:
Misma que en el Apartado 1, pregunta 20.

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;

Respuesta:
Misma que en el Apartado 1, pregunta 13, inciso b.

~~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;

Respuesta:
Misma que en el Apartado 1, pregunta 25.

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

Respuesta:
Misma que en el Apartado 1, pregunta 26.

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

Respuesta:
Misma que en el Apartado 1, pregunta 16.

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.

Respuesta:
Misma que en el Apartado 1, pregunta 27.

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

Respuesta:
Misma que en el Apartado 1, pregunta 12.

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.

Respuesta:

No se 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.

Respuesta:
No aplica

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:

Respuesta:
No se tiene conocimiento de ninguna entidad.

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.

Respuesta:

Good Tape Transcription

53. El número de registros existentes de lo solicitado en el punto anterior.
    a. Las fechas de operación.

Respuesta:
A partir del año 2023

    b. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.

Respuesta:
Transcripción de audios a texto.

    c. Los contratos de su uso o adquisición.

Respuesta:
Pago de licencia anual. (https://goodtape.io/)

53. ¿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?

Respuesta:
No aplica

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

Respuesta:
No aplica

Sin más por el momento, quedo de Usted para cualquier duda o aclaración.

Atentamente

Edgar Gerardo Sánchez Salazar
Director de Sistemas