Saltillo, Coahuila de Zaragoza, a 08 de noviembre de 2024
Oficio TCA/PJ/UT/037/2024
Número de Folio 051785900002224

A quien corresponda

Presente.

En fecha 21 de octubre de 2024 se recibe por la Unidad de Transparencia del Tribunal de Conciliación y Arbitraje, mediante la Plataforma Nacional de Transparencia (PNT), una solicitud de información con número de folio **051785900002224**, y, de conformidad con el artículo 99 de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza, y una ez recibida la información relativa a su solicitud por el área correspondiente, anexo la respuesta proporcionada.

"**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;
   No
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; b) 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.

a) Sí
b) Sí
c) No
d) No
e) No
f) No
g) No
h) Sí
i) No

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;
   Sí i) 01/06/2024 ii) 15/06/2024 iii) No se ha modificado desde su creación iv) Dirección de Innovación y Dirección de Informática
4. Informar sí se emplea la firma electrónica avanzada en la institución;

c.c.p Archivo.

Saltillo, Coahuila de Zaragoza, a 08 de noviembre de 2024
Oficio TCA/PJ/UT/037/2024
Número de Folio 051785900002224

Si

5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;
   No
6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;
   Sí
7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;
   Hay centros de datos propios de la institución así como de terceros.
8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;
   No
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.
   Sí. a) No, c), Sí d), Sí, e) Sí
10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;
    Sí
11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;
    a) Si
    b) Si
12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
    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; b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;
    a) No, b) 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.
    No
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?;
    No

c.c.p Archivo.

Saltillo, Coahuila de Zaragoza, a 08 de noviembre de 2024
Oficio TCA/PJ/UT/037/2024
Número de Folio 051785900002224

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;
    No
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;
    No
18. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
    No, los usuarios de los sistemas de gestión de información no usan dispositivos móviles
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.
    Si
20. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
    No
21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
    Sí, los esquemas de mejores prácticas en materia de protección de datos personales adoptados son la capacitación frecuente, monitoreo periódico de los servidores y de las redes, respaldos frecuentes, aplicación de actualizaciones y uso de antivirus.
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;
    Sí, no se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales ni se han emitido recomendaciones por el del INAI
23. Informar sí se cuenta con documento de seguridad en materia de protección de datos personales;
    Si
24. Informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;
    Sí
25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
    Dependiendo de las características técnicas se hace la revisión y actualización inmediata. Además, cada seis meses se hace una revisión exhaustiva.
26. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
    No

c.c.p Archivo.

Saltillo, Coahuila de Zaragoza, a 08 de noviembre de 2024
Oficio TCA/PJ/UT/037/2024
Número de Folio 051785900002224

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.
    Se tiene un sistema de Tickets de Soporte Técnico. Es para uso interno solamente.
28. Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.
    Si.

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;
    No.
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;
    Sí i) 01/06/2024 ii) 15/06/2024 iii) No se ha modificado desde su creación iv) Dirección de Innovación y Dirección de Informática
31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;
    No
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?;
    No
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;
    No se cuenta con un plan de continuidad del negocio.
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;
    No
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;
    No
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;
    Sí, la capacitación se lleva a cabo de acuerdo a las necesidades requeridas.
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;

c.c.p Archivo.

Saltillo, Coahuila de Zaragoza, a 08 de noviembre de 2024
Oficio TCA/PJ/UT/037/2024
Número de Folio 051785900002224

Sí, las Direcciones de Innovación e Informática son las responsables de ello.

38. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
    No, los usuarios de los sistemas de gestión de información no usan dispositivos móviles
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.
    Si
40. Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;
    No
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
42. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
    Sí, los esquemas de mejores prácticas en materia de protección de datos personales adoptados son la capacitación frecuente, monitoreo periódico de los servidores y de las redes, respaldos frecuentes, aplicación de actualizaciones y uso de antivirus.
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 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;
    Sí, no se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales ni se han emitido recomendaciones por el del INAI
44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
    Las medidas de seguridad se actualizan cada vez que los responsables tienen el conocimiento de dicha actualización. Dependiendo de las características técnicas se hace la revisión y actualización inmediata. Además, cada seis meses se hace una revisión exhaustiva.
45. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
    No
46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;
    Sí, la Dirección de Informática es la responsable.
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.
    Se tiene un sistema de Tickets de Soporte Técnico. Es para uso interno solamente.
48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.
    Sí, es interno.

c.c.p Archivo.

Saltillo, Coahuila de Zaragoza, a 08 de noviembre de 2024
Oficio TCA/PJ/UT/037/2024
Número de Folio 051785900002224

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.
No aplica
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.
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:
En el presente, no usamos tecnologías de inteligencia artificial.
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.
Los sistemas de gestión de información tienen algoritmos para balancear la carga de trabajo.
53. El número de registros existentes de lo solicitado en el punto anterior. Las fechas de operación. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta. Los contratos de su uso o adquisición.
Los algoritmos para la selección aleatoria de jueces de los sistemas de gestión de información son desarrollados por el equipo de desarrollo de la institución desde el año 2000.
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?
Los algoritmos para la selección aleatoria de jueces de los sistemas de gestión de información deben mantenerse en secreto por su vital importancia, sin dejar a un lado el balanceo de carga de trabajo.
55. ¿Qué datos se utilizan para la selección y asignación aleatoria de casos? (sic)
Los algoritmos para la selección aleatoria de jueces de los sistemas de gestión de información deben mantenerse en secreto por su vital importancia, además de vigilar el balance de carga de trabajo hacia los jueces."

De esta forma se da respuesta a su solicitud de información como lo disponen los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos; 7° y 8° de la Constitución Política del Estado de Coahuila de Zaragoza y, artículo 99, 102 y 103 de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza.

c.c.p Archivo.

Saltillo, Coahuila de Zaragoza, a 08 de noviembre de 2024
Oficio TCA/PJ/UT/037/2024
Número de Folio 051785900002224

Igualmente, informo que puede hacer valer el recurso de revisión ante el Instituto Coahuilense de Acceso a la Información Pública en caso de considerar que la presente respuesta no es acorde a su solicitud, como lo determinan los artículos 110 y 111 de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza o, en su caso, a través de la Plataforma Nacional de Transparencia, cuya liga electrónica es: https://www.plataformadetransparencia.org.mx/ en el apartado Quejas de respuestas.

Sin otro particular, quedo de Usted.

Atentamente
Titular de la Unidad de Acceso a la Información Pública
del Tribunal de Conciliación y Arbitraje

Liliana Ortiz Herrera

PODER JUDICIA
DEL ESTADO DE COAHUILA DE ZARAGOZA
Tribunal de Conciliación y Arbitraje
Unidad de Transparencia

c.c.p Archivo.