



Saltillo, Coahuila de Zaragoza a 08 de noviembre de 2024

Oficio n° STT/506/2024

Número de Folio 051259000026724

**Solicitante
Presente.**

Por este conducto le comunico que fue recibida por vía electrónica su petición con el número de folio 051259000026724, donde mediante archivo adjunto a su vez solicita:

“PREGUNTAS

APARTADO 1

1. *Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;*
2. *Señalar si 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 si 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 si 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 si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; 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.*
3. *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 cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;*
4. *Informar si se emplea la firma electrónica avanzada en la institución;*
5. *Informar si 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 si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;*
8. *Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;*
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: 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 si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;*
11. *Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;*
12. *Informar si 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 si 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 si 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 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;*



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;
18. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
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; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.
20. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
21. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
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;
23. Informar si se cuenta con documento de seguridad en materia de protección de datos personales;
24. Informar si 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 si 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 si 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 si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
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 cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;
31. Informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;
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 cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;
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;
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;
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;
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;
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;
38. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
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.
40. Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;
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;



42. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
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;
44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
45. Informar si 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 de selección y asignación aleatoria de casos?
55. ¿Qué datos se utilizan para la selección y asignación aleatoria de casos? (sic) ” (sic)

En mérito de lo anterior, de conformidad con los artículos 97, 99, 102 y 103 de la Ley de Acceso a la Información Pública para el Estado de Coahuila y para dar atención y respuesta a la misma, fue turnada por la Unidad de Atención a las Solicitudes de Acceso a la Información de la Secretaría Técnica y de Transparencia a la Dirección de Informática de la Oficialía Mayor del Poder Judicial.

En virtud de lo anterior, se le informa por conducto de esta Unidad, después de una búsqueda exhaustiva de la información, lo siguiente:

APARTADO 1

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

No.
2. Señalar si 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 si 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 si 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 si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; 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.

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

3. 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 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 si se emplea la firma electrónica avanzada en la institución;

Sí

5. Informar si 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 si 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 si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;

No.

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: 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) Sí.

b) Sí.

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.

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 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.

Sí.



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

No.

21. Informar si 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 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;

Sí, no se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales, ni emitido recomendación por el INAI.

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

Sí.

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

No.

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

Sí.

APARTADO 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;

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.
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;
- Sí, las Direcciones de Innovación e Informática 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 utilizan 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.
- Sí.
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 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.

42. Informar si 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 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;

Sí, no se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales, ni emitido recomendación por el INAI.

44. 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.

45. Informar si 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.

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. 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.

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.

Se informa lo anterior, con fundamento en lo establecido por el artículo 102 y 103 de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza, disposiciones que establecen:

Artículo 102.-La obligación de dar acceso a la información se tendrá por cumplida cuando la información se entregue al solicitante en medios electrónicos, ésta se ponga a su disposición para consulta en el sitio en que se encuentra, o bien mediante la expedición de copias simples o certificadas. El acceso a la información se dará solamente en la forma en que lo permita el documento de que se trate.

En el caso de que la información ya esté disponible en medios electrónicos, la Unidad de Transparencia se lo indicará al solicitante, precisando la dirección electrónica completa del sitio donde se encuentra, y en la medida de sus posibilidades, podrá adjuntar a la respuesta la imagen digital que compruebe que ahí se encuentran los datos o documentos solicitados y proporcionar una impresión de la misma.

En el caso de que la información solicitada ya esté disponible al público en medios impresos, tales como libros, compendios, informes, trípticos o en cualquier otro medio, se le hará saber al solicitante por escrito la fuente, el lugar y la forma en que puede consultar, reproducir o adquirir dicha información en un plazo no mayor a cinco días.

Artículo 103.- Los sujetos obligados entregarán documentos que se encuentren en sus archivos. La obligación de proporcionar información no comprende el procesamiento de la misma, ni el presentarla conforme al interés particular del solicitante. Sin perjuicio de lo anterior, los sujetos obligados deberán sistematizar la información.



PODER JUDICIAL

DEL ESTADO DE COAHUILA DE ZARAGOZA

“2024, Año de la justicia al servicio de las niñas y los niños”
“2024 Bicentenario de Coahuila; 200 años de grandeza”

Ello encuentra su refuerzo en el criterio SO/03/2017 emitido por el INAI y que señala:

No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información. Los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública, señalan que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las características físicas de la información o del lugar donde se encuentre. Por lo anterior, los sujetos obligados deben garantizar el derecho de acceso a la información del particular, proporcionando la información con la que cuentan en el formato en que la misma obre en sus archivos; sin necesidad de elaborar documentos ad hoc para atender las solicitudes de información.

Con lo anterior se responde a su solicitud de información de conformidad con lo dispuesto en los artículos 6o de la Constitución Política de los Estados Unidos Mexicanos; 7o, párrafo séptimo y 8o, párrafo sexto, de la Constitución Política del Estado de Coahuila de Zaragoza y, 97 de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza.

Por otro lado, y en cumplimiento de lo previsto por los artículos 110 y 111 de la Ley de Acceso de Información Pública para el Estado de Coahuila de Zaragoza, le comunico que si Usted no está conforme con esta respuesta podrá presentar recurso de revisión e interponerlo de manera directa o por medios electrónicos, a través de la Plataforma Nacional de Transparencia, ante el Instituto Coahuilense de Acceso a la Información Pública.

Sin otro particular, le reitero las seguridades de mi atenta y distinguida consideración.

Atentamente



PODER JUDICIAL
DEL ESTADO DE COAHUILA DE ZARAGOZA
**Unidad de Atención a las Solicitudes
de Acceso a la Información de la
Secretaría Técnica y de Transparencia**

Yesenia Yazmín Perales Ortega
Unidad de Atención a Solicitudes de Acceso a la Información de la
Secretaría Técnica y de Transparencia de la Presidencia del
Tribunal Superior de Justicia del Estado.

c.c.p. Mtro. Miguel Felipe Mery Ayup. Magistrado Presidente del Tribunal Superior de Justicia del Estado de Coahuila de Zaragoza.
c.c.p. Mtro. Rodrigo González Morales. Secretario Técnico y de Transparencia de la Presidencia del Tribunal Superior de Justicia del Estado.
c.c.p. Archivo.