



Culiacán Rosales, Sinaloa, 28 de octubre de 2024

**Estimado solicitante**  
**Presente. -**

En atención a su solicitud con folio número 251159400006524, realizada a través de la Comisión Estatal para el Acceso a la Información Pública del Estado de Sinaloa, me permito dar respuesta en tiempo y forma con base a la información proporcionada a esta unidad por el área correspondiente en los siguientes términos:

Con respecto a la información solicitada, en la cual requiere:

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 un 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 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 sí 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 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)''.





**TRIBUNAL DE JUSTICIA  
ADMINISTRATIVA DEL  
ESTADO DE SINALOA**

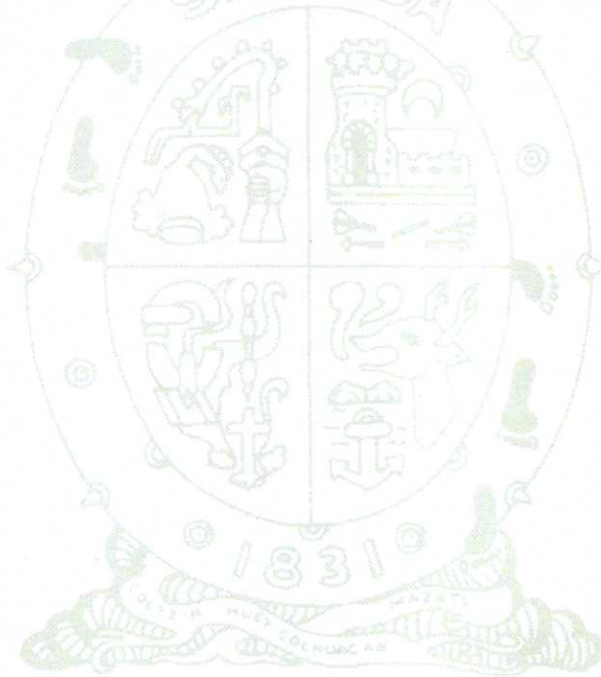
En relación a lo anterior, se informa que la respuesta proporcionada por la Unidad de Informática de este Tribunal, área competente de acuerdo al objeto y naturaleza de su solicitud para su debida atención, se encuentra en el archivo anexo, mismo que pongo a su disposición a través de la Plataforma Nacional de Transparencia.

Sin otro particular, me despido con un cordial saludo.

**ATENTAMENTE**

---

**Lic. Dianet Pérez Castro**  
**Titular de la Unidad de Transparencia**





**UNIDAD DE INFORMATICA**

OFICIO: TJA/UI/0119-2024

ASUNTO: *Contestación de Oficio de Acceso  
a la Información Pública*

*Culiacán, Sinaloa, 28 de octubre de 2024*

**Lic. Dianet Pérez Castro**

**Titular de la Unidad de Transparencia**

*Dando cumplimiento la solicitud de información número de folio 251159400006524 presentada ante la Comisión Estatal de Acceso a la Información Pública de Sinaloa, mediante oficio 65/UT-TJA/2024 de fecha de recibido 22 de octubre de 2024 el cual solicita lo siguiente:*

**APARTADO 1**

PREGUNTA	RESPUESTA
1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;	No se cuenta
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.	a) No c) No d) No e) No f) No g) No h) No 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;	No
4. Informar si se emplea la firma electrónica avanzada en la institución;	No
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;	No
7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;	Propios y contratados a terceros.
8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;	No se cuenta por el momento con trabajo remoto.
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.	Si contamos con un correo institucional. a) No c) Si. d) Si. e) Si.
10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;	No
11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;	a) Si b) No
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?;	Si, Unidad de Transparencia, Sala Superior, no cuento con la información desde cuando se adoptó.
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 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;	Si





18. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;	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 (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información	(i) Si (ii) Si (iii) Si (iv) Si
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;	No
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;	No se cuenta
23. Informas si se cuenta con documento de seguridad en materia de protección de datos personales;	Si cuenta
24. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;	No cuenta
25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;	No contamos
26. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;	No se llevan
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.	Si se cuenta y es Interno
28. Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.	No

**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 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 cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;	No se cuenta
31. Informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;	Si
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?;	Si





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
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;	Si, Unidad de Transparencia, Unidad de Informática, Sala Superior.
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;	No
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;	Si se cuenta, Unidad de Informática.
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
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 (i) Si (ii) Si (iii) Si (iv) 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;	Si, se recopila, se procesa y se resguarda, y se respeta La Ley LGPDPPSO. Identificar y vigilar los riesgos de seguridad, bajo la política de privacidad clara y consentimiento informado. Control de Accesos. Auditoria y Trazabilidad.
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;	No





44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;	Una vez por semana
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;	Si, todas las áreas.
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.	Si, Interno.
48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.	Si, 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
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
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:	No
52. <i>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.</i>	Ninguno
53. <i>El número de registros existentes de lo solicitado en el punto anterior.</i> a. <i>Las fechas de operación.</i> b. <i>El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.</i> c. <i>Los contratos de su uso o adquisición.</i>	Sin información
54. <i>¿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?</i>	Sin información
55. <i>¿Qué datos se utilizan para la selección y asignación aleatoria de casos? (sic)</i>	No se cuenta

Sin otro particular quedo a la espera de cualquier, duda o aclaración, Saludos.

Atentamente

Lic. Elda Yesenia Moreno Pulido  
Titular de la Unidad de Informática del TJA