ACUERDO DE RESPUESTA
FOLIO PNT: 070124224000206
EXPEDIENTE: TSJCJ/UT/12C06/206/2024

Con fecha 21 de octubre del año dos mil veinticuatro, se recibió la solicitud de acceso a la información pública realizada por **Solicitante No Identificado,** presentada a través del Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia (PNT) bajo el número de folio citado al rubro y en la que solicita la siguiente información: **"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."(sic). Asi mismo, se tiene por recibido el archivo adjunto a la solicitud, el cual contiene las 55 preguntas a las que se le dará respuesta. ----------

UNIDAD DE TRANSPARENCIA DEL TRIBUNAL SUPERIOR DE JUSTICIA - CONSEJO DE LA JUDICATURA. - Tuxtla Gutiérrez, Chiapas; a 13 de noviembre de 2024. ----------

--- **Vista** la información enviada por la **Dirección de Desarrollo e Infraestructura Tecnológica,** relativa a la respuesta recaída a la solicitud de acceso a la información de mérito de las preguntas de su competencia, ahora bien con respecto a las preguntas 16, 17, 22, 23, 32, 34, 35, 43, esta **Dirección de Transparencia y Acceso a la Información Pública** informa lo siguiente:

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;
R= 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;
R= No

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;
R= No

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

R= Si, puede consultarlo en el Portal de Transparencia con la siguiente liga electrónica: https://transparencia.poderjudicialchiapas.gob.mx/archivos/pd/sesedap/DOCUMENTO%20DE%20SEGURIDAD%20(ver.%2029112022).pdf.

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?;

R= Si, a finales del año 2023 la Direccción de Desarrollo e Infraestructura Tecnlogica diseñó el Sistema Electrónico de Seguridad de Protección de Datos Personales la Direccción de Desarrollo e Infraestructura Tecnlogica, mismo que fue solicitado por la Dirección de Transparencia y Acceso a la Información Publica y aprobado por el Comite de Transparencia. Cabe mencionar que dicho sistema se encuentra en periodo de implementación, toda vez que fué sometido a un periodo de prueba el cual generó algunos ajustes y una vez realizados los cambios pertinenetes, se comenzó a capacitar a los órganos jurisdiccionales para la carga de la información correspondiente.

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;
R= 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;
R= No

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;
R= No

- - - En consecuencia, **NOTIFÍQUESE** y hágase entrega de la información solicitada en los medios y formas señalados por el solicitante, esto es por el Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia (PNT); archívese en el expediente correspondiente y téngase como asunto totalmente concluido. Lo anterior, con fundamento en los artículos 151, 152 y 157 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.------------------

- - - Así lo acuerda y firma la **C. MTRA. GUADALUPE DEL ROCÍO SANTOS ACOSTA**, Titular de la Unidad de Transparencia del Tribunal Superior de Justicia - Consejo de la Judicatura. ---------

19 NOV 2024

C. MTRA. GUADALUPE DEL ROCÍO SANTOS ACOSTA
TITULAR DE LA UNIDAD DE TRANSPARENCIA

Elabora: RAMM/YVD

Tuxtla Gutiérrez, Chiapas; a 05 de noviembre de 2024.
Oficio No. DDIT/2003/2024.

11 NOV 2024
9:55
anexo ocho hojas

Mtra. Guadalupe del Rocío Santos Acosta.
Directora Interina de la Unidad de Transparencia del Consejo de la Judicatura.
P r e s e n t e

En atención a su memorándum número DTAIP/693/2024, le envío la información por solicitante no identificado, en las hojas que se anexa (8 fojas), donde se anexa respuesta a las preguntas que son competencia de esta Dirección.

Agradeciendo anticipadamente la atención brindada. Saludos cordiales.

A t e n t a m e n t e.

Dr. Bernardo López Maldonado.
Director.

CONSEJO DE LA JUDICATURA DEL PODER JUDICIAL ESTADO DE CHIAPAS
OFICIALÍA MAYOR
DIRECCIÓN DE DESARROLLO E INFRAESTRUCTURA TECNOLÓGICA

C.c.p. Archivo
Revisó: gabp / Elaboró: scra

PREGUNTAS

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;

   R=Si, Dirección de Desarrollo e Infraestructura tecnológica, Dirección de Asuntos Jurídicos, y en su caso Contraloría Interna.

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.

   R= Si, se hace un estudio de las necesidades del equipo de acuerdo a eso se hace la adquisición, Si contamos con inventario institucional, se lleva la continuidad de operaciones de acuerdo al incidente, así como del sistema electrónico de seguridad de protección de datos personales.

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 ;

   R=Si, principios de agosto del 2024, Dirección de Desarrollo e Infraestructura Tecnológica.

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

   R= si

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

   R=No

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

   R=Si

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

   R= Infraestructura propia

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

   R=Si

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.

   R=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;

    R=Si

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

    R=Si, cuenta con avisos de privacidad y la información recabada está bajo el tratamiento de las áreas correspondientes, y si contamos con los certificados vigentes.

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

    R=No

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;

    R=Si

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.

    R=Si, 15 de junio de 2023.

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?;

    R=Si , desde finales del 2023, Dirección de desarrollo e infraestructura tecnológica, Dirección de Transparencia y Acceso a la Información Pública y avalado por el Comité de Transparencia de este sujeto obligado

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;

    R= No se cuenta sin embargo se cuenta con carta responsiva de confidencialidad

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.

    R=Si

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

    R=Si, dos

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

    R=Si, con la implementación del SESEDAP, y la medidas de seguridad en plataformas

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;

    R=Si

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

    R=En cuanto antivirus diariamente, en cuanto a sistemas operativos e implementaciones en cuanto se publica

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

    R=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.

R=No

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

R=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;

R= Si, Dirección de Desarrollo e Infraestructura Tecnológica, Dirección de Asuntos Jurídicos, y en su caso Contraloría Interna.

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 ;

R= Si, principios de agosto del 2024, Dirección de Desarrollo e Infraestructura Tecnológica.

31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;

R=Si

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;

R=SI

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;

R= 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;

R= SI

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

R= No se cuenta sin embargo se cuenta con carta responsiva de confidencialidad

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. .

R=SI

40. Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;

R=Si, DOS

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;

R=SI

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

R= SI, con la implementación del SESEDAP, y la medidas de seguridad en plataformas

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;

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

R= En cuanto antivirus diariamente, en cuanto a sistemas operativos e implementaciones en cuanto se publica

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

R=No

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

R=SI, Dirección de Desarrollo e Infraestructura Tecnológica y el área del incidente

47. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.

R=No

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

R= SI, interno

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.

R=Si

50.En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia.

R=Se llevan a cabo algunas audiencias por videoconferencias (en linea) para efectos de solucionar brechas de distancia u otra que se pueda generar, fue de mayor auge desde la pandemia.

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:

R=Se desconoce la infraestructura de los diversos sujetos obligados de la 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.

R=Este sujeto obligado por medio de la dirección de desarrollo e infraestructura tecnológica desarrollo un sistema el cual es un programa de oficialía de partes que se encarga de hacer una designación aleatoria.

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.

R=A) El sistema inicio en 2018,b) la asignación de asuntos se realiza de acuerdo a la cantidad de órganos del mismo ramo en el distrito, no se basa en inteligencia artificial, el balanceo de cargas es aleatorio, c) el sistema fue realizado por personal de la institución.

54.¿Cómo procede y op1era 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?

R=Este sistema se basa de acuerdo a los inicios presentados, en cuantos juzgados y de cada ramo del derecho existentes en la sede judicial y si es para primera o segunda instancia.

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

R=El tipo de materia, cantidad de órganos de la misma materia y mismo distrito, y la cantidad máxima de asignaciones.