"2024, Año del XXV Aniversario de la Inscripción de la Ciudad Histórica Fortificada de Campeche en la Lista de Patrimonio Mundial de la Unesco"

UNIDAD DE TRANSPARENCIA

Asunto:	**Se emite Respuesta.**
Folio:	**040081700004424.**
Fecha de Respuesta:	**12 de noviembre 2024.**

nacidoel1deenero@gmail.com
Solicitante de Información Pública

Con fecha 22 de octubre de 2024 fue registrada en esta Unidad de Transparencia su solicitud de información con **folio 040081700004424**, referente a **"SECCION 1 1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan; 2. Señalar sí se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar sí se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC. 3. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;4. Informar sí se emplea la firma electrónica avanzada en la institución; 5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos; 6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros; 7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero; 8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas; 9. Informar sí se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información. 10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos; 11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes; 12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos; 13. Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información; 14. Informar sí dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó. 15. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados se cuenta con un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?; 16. Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó; 17. Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su**

implementación y desde cuándo se implementó; 18. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos; 19. Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información. 20. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas; 21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son; 22. Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso; 23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales; 24. Informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información; 25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución; 26. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad; 27. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo. 28. Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes. SECCION 2 Solicito la siguiente información. 29. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan; 30. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ; 31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución; 32. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente Un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;.". *[sic]*----------

En términos de los Artículos 44 párrafo primero, 51, fracciones II, V y XII, 124, 125, 130 y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche, se emite la siguiente:

RESPUESTA

En atención a su solicitud, se informa lo siguiente:

APARTADO 1

1.- Respecto a la información si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan, le hago de su conocimiento que este organismo no cuenta con un gobierno de seguridad de la información.

2.- Respecto a señalar sí se cuenta con : 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., le informo esta información no ha sido generada por este organismo.

3.- Respecto a informar sí se cuenta con una estrategia de ciberseguridad dentro de la institución, le informo que no se cuenta.

4.- Respecto a informar sí se emplea la firma electrónica avanzada en la institución, le informo que no se emplea.

5.- Respecto a informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos, le informo que no se han realizado simulacros de este tipo.

"2024, Año del XXV Aniversario de la Inscripción de la Ciudad Histórica Fortificada de Campeche en la Lista de Patrimonio Mundial de la Unesco"

6.- Respecto a señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros, le informo que este organismo no cuenta con lineamientos.

7.- Respecto a informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero, le informo que esta Institución no cuenta con un centro de datos.

8.- Respecto a informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas, le informo que este organismo no cuenta con lineamientos de seguridad.

9.- Respecto a informar sí se cuenta con un correo electrónico institucional, le informo que si se cuenta con el correo electrónico institucional, ahora bien respecto a Informar si el correo electrónico que se emplea en la institución cuenta con: 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, le informo que el correo institucional no cuenta con estas características.

10.- Respecto a informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos, le informo que este Instituto, brinda su servicio, no sin antes hacerles de su conocimiento a los usuarios de los avisos de privacidad con los que cuenta, para hacerles saber de su conocimiento cual es la finalidad de la obtención de sus datos, asimismo todos los servidores públicos de este organismo, están sujetos a un Código de Conducta y Código de Ética aprobados, que establecen los principios que todo servidor público sin excepción alguna debe observar en el desempeño de su empleo, cargo, función o comisión. Entre los que se encuentra el principio de CONFIDENCIALIDAD, que es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

11.- Respecto a informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes, respecto al inciso a) la Institución si cuenta con avisos de privacidad, con relación al inciso b) la página institucional no cuenta con certificado digital.

12.- Respecto a informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos, le informo que no se ha tenido este tipo de capacitación.

13.- Respecto a 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 la madurez institucional en la gestión de seguridad de la información, le informo que este organismo no tiene generada esta información.

14.- Respecto a 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, le informo que no se tiene implementado este tipo de programa.

15.- Respecto a 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, le informo que actualmente no se tiene implementado un sistema.

16.-. Respecto a 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, se informa que no se cuenta con modelo o sistema de comunicación.

17.- Respecto a 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, le informo que no se tiene implementado modelo o sistema de comunicación.

18.- Respecto a informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos, le informo que actualmente no se cuenta con este tipo de lineamientos.

19.- Respecto a 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, le informo que la Institución cuenta con personal que tiene conocimiento y recibe capacitación en materia de transparencia, protección de datos personales y en materia de archivos.

20.- Respecto a informar sí se han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas, le informo que no se han tenido brechas de ciberseguridad.

21.- Respecto a informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son, le informo que no se tienen hasta el momento esquemas implementados.

22.- Respecto a informar sí se tiene algún sistema o plataforma informática, aplicación electrónica o cualquier otra

tecnología que se emplee que implique el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia, le informo que no se tiene empleado algún tipo de sistema.

23.- Respecto a informar sí se cuenta con documento de seguridad en materia de protección de datos personales, le informo que actualmente este sujeto obligado se encuentra en el proceso de integración y creación de su marco normativo, por lo que no se tiene generada esta información.

24.- Respecto a informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información, le informo que no se cuenta con un plan de comunicación.

25.- Respecto a informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución, le informo que esta información no se ha generado dentro del organismo.

26.- Respecto a informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad, le informo que no se han llevado auditorías de este tipo en la Institución.

27.- Respecto a 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., le informo que no se tiene este tipo de equipo que brinde soporte técnico.

28.- Respecto a señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes, le informo que relativo a la información de este organismo, este no cuenta con certificados digitales.

APARTADO 2

29.- Respecto a informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan, le informo que no se cuenta con un gobierno de seguridad.

30.- Respecto a informar sí se cuenta con una estrategia de ciberseguridad dentro de la institución, le informo que no se cuenta con una estrategia implementada.

31.- Respecto a informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución, le informo que no se cuenta con un sistema de gestión de seguridad.

32.- Respecto a informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con un sistema de gestión de protección de datos personales, le informo que no se tiene implementado un sistema de gestión.

33.- Respecto a 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, le comunico que no se tiene implementado un plan de continuidad.

34.- Respecto a 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 le informo que no se tiene implementado modelo o sistema de comunicación.

35.- Respecto a 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, le informo que no cuenta con un modelo o sistema de comunicación.

36.- Respecto a 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, le informo que actualmente no se ha tenido capacitación en esta temática.

37.- Respecto a 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, le informo que no se cuenta con un procedimiento en la actualidad.

38.- Respecto a informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos, le informo que no se cuenta con lineamientos para el traslado de activos físico de la Institución.

39.- Respecto a 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, le informo que la Institución cuenta con personal que tiene conocimiento y recibe capacitación en materia de transparencia, protección de datos personales y en materia de archivos.

40.- Respecto a informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas, le informo que no se ha generado información de brechas de ciberseguridad.

41.- Respecto a informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro

de la institución, le informo que no se tiene implementado modelo alguno.

42.- Respecto a informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son, le informo que no se ha adoptado esquemas de mejores prácticas.

43.- Respecto a 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, le informo que no se tiene implementado este tipo de tecnología.

44.- Respecto a informar cada cuanto tiempo se actualizan las medidas de ciberseguridad dentro de la institución, le informo que no se tienen implementado medidas de seguridad.

45.- Respecto a informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad, le informo que no se han realizado auditorías de seguridad externa.

46.- Respecto a señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este, le informo que no se cuenta con un sistema de gestión de incidentes.

47.- Respecto a 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, le informo que no se tiene este tipo de equipo que brinde soporte técnico.

48.- Respecto a señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo, le informo que no se cuenta con este tipo de equipo de respuesta.

APARTADO 3

49.- Respecto a indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial, le informo que no se tiene generada información, ya que no se cuenta con una solución tecnológica.

50.- Respecto a contar con alguna solución para el propósito antes señalado e 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, le informo que no se tiene generada esta información.

51. Se desconoce cuál es el sujeto obligado en la entidad, que cuente con una solución tecnológica para los propósitos señalados líneas arriba, en consecuencia, este sujeto no tiene generada esta información; asimismo se desconoce la aplicación de la forma en que se apliquen medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de otra institución, al momento de brindar servicios a la ciudadanía.

52. En relación a 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, le informo que esta información no ha sido generada por este sujeto obligado.

53. Respecto al número de registros existentes de lo solicitado en el punto anterior, como son las fechas de operación, el funcionamiento y operación de cada sistema o algoritmo con el que cuenta y los contratos de su uso o adquisición, le informo que esta información no ha sido generada por este sujeto obligado.

54. Con respecto a 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, le hago de su conocimiento que este sujeto obligado de acuerdo a sus facultades y atribuciones, no genera esta información.

55. Respecto a qué datos se utilizan para la selección y asignación aleatoria de casos, le informo que no se tiene generada esta información en este sujeto obligado

CÚMPLASE. Así lo acordó y firma la **Lic. Estela del Carmen Tun Encalada**, Analista de la Unidad de Transparencia del Instituto de Acceso a la Justicia del Estado de Campeche. Se le notifica que podrá actuar conforme lo previsto en el artículo 147 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.