



OFICIO No. UT-CJF/060/2024

ASUNTO: Atención a Solicitud de
Información 180368124000018

Tepic, Nayarit; Noviembre 14 de 2024

C.

nacidoel1deenero@gmail.com

P R E S E N T E.

De conformidad con lo establecido en los Artículos 134, 141 y demás relativos de la Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit (LTAIPEN), así como el artículo 124 de su Reglamento, en atención a su solicitud de información recibida a través de la *Plataforma Nacional de Transparencia*, con número de folio 180368124000018 dirigida a este sujeto obligado, en la cual 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**





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.

Por lo anterior, me permito hacer de su conocimiento la respuesta generada por la Unidad Administrativa correspondiente, anexando a la presente, copia digitalizada del Oficio: DGCJF/1980/2024, formulado y firmado por la Licenciada Carmen Eleny Martínez Vázquez, Directora General del Centro de Justicia Familiar del Estado de Nayarit.

Gracias por ejercer su derecho a la información.

ATENTAMENTE:

TITULAR DE LA UNIDAD DE TRANSPARENCIA

ING. JOSE AVIGAEEL JACOBO MEZA





Oficio: DGCJF/1980/2024

Tepic, Nayarit, a 14 de noviembre del año 2024

Asunto: Se rinde informe

ING. JOSÉ AVIGUEL JACOBO MEZA
TITULAR DE LA UNIDAD DE TRANSPARENCIA
DEL CENTRO DE JUSTICIA FAMILIAR
PRESENTE

*Recibido
14/Noviembre/2024
13:05 HS.*

Sirva la presente para que con fundamento en lo establecido en el artículo 141 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit, y en atención a la solicitud de información con número de folio 180368124000018, hacer de su conocimiento lo siguiente:

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

Actualmente no se cuenta con dicha figura al interior del este Centro de Justicia Familiar.

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.

- A) No se cuenta con ello
 - B) No se cuenta con ello
 - C) No se cuenta con ello
 - D) No se cuenta con ello
 - E) Continuamente se advierten vulnerabilidades y mejoras en el SIPCIE de este Centro de Justicia Familiar, lo que permite la mejora constante del mismo.
 - F) No se cuenta con ello
 - G) No se cuenta con ello
 - H) No se cuenta con ello
 - I) No se cuenta con ello
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 se cuenta con estrategia definida de ciberseguridad al interior de la institución.
4. Informar si se emplea la firma electrónica avanzada en la institución;
- No se emplea la firma electrónica avanzada
5. Informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;
- Existen planes de recuperación aplicados al SIPCIE de este Centro de Justicia Familiar, no obstante, no hay aplicación de simulacros.





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

Se emplean los protocolos de seguridad requeridos para el desarrollo de sistemas seguros.

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

En relación al SIPCIE son propios.

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

Las propias de las plataformas de uso libre (en el caso de requerirlas).

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.

Se cuenta con un correo institucional, pero en relación a los incisos A, B, C, D Y E, es preciso mencionar que el dominio no pertenece al Centro de Justicia Familiar, toda vez que este es suministrado por el Gobierno del Estado de Nayarit, y que en virtud de ello no se cuenta con la información complementaria.

10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;





Nayarit

CENTRO DE
JUSTICIA FAMILIAR

Los establecidos en el Reglamento Interno del Centro de Justicia Familiar y el Decreto Administrativo que tiene por objeto crear el Centro de Justicia Familiar como Organismo Público Descentralizado.

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

La página es administrada por un órgano distinto al Centro de Justicia Familiar.

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

El personal no ha recibido la capacitación en comentario

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;

No se cuenta con los mecanismos e indicadores a los que se hace referencia.

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 implemento.

No se cuenta con el programa al que se hace referencia.

Sin más por el momento, y en la espera de que dicha información sea de su completa utilidad, le envío un cordial saludo.

**ATENTAMENTE:
LA DIRECTORA GENERAL DEL CENTRO DE JUSTICIA FAMILIAR
DEL ESTADO DE NAYARIT.**

LICENCIADA CARMEN ELENY MARTÍNEZ VÁZQUEZ



C.c.p. Archivo.

