



UNIDAD DE TRANSPARENCIA DEL SUPREMO TRIBUNAL DE JUSTICIA DEL ESTADO DE SINALOA

Culiacán Rosales, Sinaloa, a 04 de noviembre de 2024

Oficio: UT/268-002/2024

N° Control Interno: 268/2024

Folio: 251264400026824

Asunto: Respuesta a solicitud de información.

Apreciable solicitante,

En atención a su solicitud de información, registrada con número de folio 251264400026824, correspondiente al control interno 268/2024, efectuada de manera electrónica a través de Plataforma Nacional de Transparencia, presentada el día 30 de octubre de 2024, se le comunica que:

I. De los plazos de respuesta y forma de entrega:

Esta respuesta se notifica en tiempo y forma en términos de lo dispuesto por el artículo 128 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa, dentro del plazo natural de respuesta, considerando que el término para brindarla es de 10 días hábiles, conforme lo previsto en los artículos 130, 136 y 137 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa, visto que el plazo comenzó a partir del día hábil siguiente a su presentación, con fecha de inicio 31 de octubre de 2024 y fecha de expiración del 13 de noviembre de 2024.

Conforme obra en registros, su petición para la entrega de la información es por medio del sistema Plataforma Nacional de Transparencia.

II. De la respuesta que se otorga:

Vista la naturaleza de su solicitud de información que realiza en los siguientes términos:

“Solicito la siguiente información

- 1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o de ciberseguridad y cuáles áreas participan;***
- 2. Señalar si de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021, se han implementado las siguientes medidas: a) estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios de seguridad de la información o de tecnologías de la información y comunicación; b) 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); 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).

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 en la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información, de ha contado con el Dictamen Técnico favorable expedido por la CEDN, de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021

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

8. 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; 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.

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

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

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

12. 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;

13. 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 y cuántas horas de capacitación en ciberseguridad se realizan de forma anual.

14. 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?;

15. 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, lo anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO);

16. 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, o anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO);;

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

18. 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.

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

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

21. 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;

22. Informas si se cuenta con documento de seguridad en materia de protección de datos personales;

23. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;

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

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

26. 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. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización

27. Informar si se cuenta con un Centro de Operaciones de Ciberseguridad Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles)”

Mediante oficio número UT/268-001/2024 de fecha 31 de octubre de 2024, la Unidad de Transparencia turnó lo correspondiente a los *pedimentos con numerales 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23, 24, 25, 26 y 27*, a la Dirección de Tecnologías de la Información y Comunicaciones; área que cuenta con la información por así competer a sus atribuciones.

En respuesta a ese oficio, en fecha 01 de noviembre de 2024, el Lic. Juan Gabriel Ávila Osuna, proporcionó la información solicitada, tras una búsqueda exhaustiva de lo requerido en los términos textualmente invocados, efectuada en archivos y registros de esta institución, misma que se anexa a la presente respuesta.

Documentos los anteriores, que se adjuntan al final del presente oficio, a efecto de dar constancia de que se realizaron las gestiones necesarias para la búsqueda exhaustiva de la información, de conformidad con el artículo 135 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa.

Ahora bien, respecto de su *pedimento con numeral 22*, se le informa que no se cuenta con documento de seguridad en materia de protección de datos personales.

III. Del fundamento al procedimiento de atención de su solicitud:

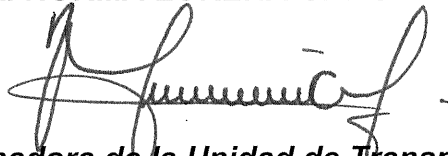
Lo anterior se realizó conforme lo señalado por los artículos 1, 3 fracciones II y XXV, 4, 16, 19, 20, 68 fracciones II, IV y V, 128, 130, 136 y demás relativos de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa, así como los artículos 87 y 89 fracciones II, IV y V del Reglamento Interior del Supremo Tribunal de Justicia del Estado de Sinaloa.

La actuación de las áreas fue conforme lo señalado por el artículo 3 fracción II de la Ley de Transparencia y Acceso a la Información Pública; 71, 72, 73 y 74 del Reglamento Interior del Supremo Tribunal de Justicia del Estado de Sinaloa.

IV. De la aclaración a la respuesta proporcionada:

Deseando que la información proporcionada le sea de utilidad, en caso de cualquier duda, problemas al visualizar el contenido o enlace electrónico, estamos a sus órdenes en la Unidad de Transparencia del Poder Judicial del Estado de Sinaloa ubicadas en Palacio de Justicia, con domicilio en Segundo Nivel, Lázaro Cárdenas 891, Colonia Centro Sinaloa, Culiacán, Sinaloa, C.P. 80000; número telefónico 6677611723, así como en la cuenta de correo electrónico utstj@stj-sin.gob.mx

ATENTAMENTE
MTRA. NORMA LORENA GARCÍA LÓPEZ



**Coordinadora de la Unidad de Transparencia
del Poder Judicial del Estado de Sinaloa.**

SUPREMO TRIBUNAL DE JUSTICIA DEL
ESTADO DE SINALOA



PODER JUDICIAL
UNIDAD DE TRANSPARENCIA



UNIDAD DE TRANSPARENCIA DEL SUPREMO TRIBUNAL DE JUSTICIA DEL ESTADO DE SINALOA

Culiacán, Sinaloa, 31 de octubre de 2024

Oficio: UT/268-001/2024

Control Interno: 268/2024

Folio: 251264400026824

Lic. Juan Gabriel Ávila Osuna

Director de Tecnologías de la Información y Comunicaciones
del Supremo Tribunal de Justicia del Estado de Sinaloa.

P r e s e n t e.-

Por este conducto y atento a lo establecido en los artículos 71, 72, 73, 74, 87 y 89 fracciones I, II y IV del Reglamento Interior del Supremo Tribunal de Justicia del Estado de Sinaloa; atendiendo a la información requerida electrónicamente a través de la PLATAFORMA NACIONAL DE TRANSPARENCIA, con folio número 251264400026824, se solicita la siguiente información que a continuación se transcribe:

“Solicito la siguiente información

- 1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o de ciberseguridad y cuáles áreas participan;***
- 2. Señalar sí de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021, se han implementado las siguientes medidas:***
 - a) estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios de seguridad de la información o de tecnologías de la información y comunicación;***
 - b) 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 un 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);***
 - 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 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).

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 en la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información, de ha contado con el Dictamen Técnico favorable expedido por la CEDN, de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021

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

8. 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; 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.

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

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

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

12. 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;

13. 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 y cuántas horas de capacitación en ciberseguridad se realizan de forma anual.

14. 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?;
15. 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, lo anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPSSO);
16. 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, o anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPSSO);;
17. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
18. 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.
19. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
20. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
21. 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;
22. ...
23. Informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;
24. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
25. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
26. 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. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización
27. Informar sí se cuenta con un Centro de Operaciones de Ciberseguridad

Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles)”

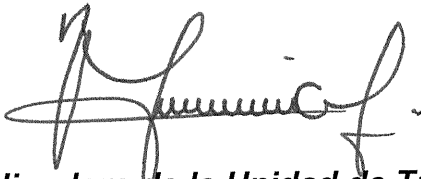
Se pide su valiosa colaboración a fin de verificar la disponibilidad y existencia de lo señalado, y comunicar a esta Unidad la modalidad en la que se encuentra la información requerida, esto es, si se encuentra en soporte físico o electrónico, en el entendido que, en el primer supuesto deberá informar el número de copias que hayan de realizarse para su obtención y, en el segundo, deberá proporcionar el archivo o archivos correspondientes a la dirección electrónica institucional *norma.garcia@stj-sin.gob.mx*

Para el oportuno y eficaz cumplimiento en la atención de la solicitud de mérito, la respuesta al presente oficio deberá ser remitida a esta Unidad de Transparencia a más tardar el día *06 de noviembre de 2024*.

En el supuesto de necesitar alguna aclaración sobre la misma deberá comunicarla a más tardar al día hábil siguiente al de su recepción.

Sin otro particular, reciba un cordial saludo.

ATENTAMENTE
MTRA. NORMA LORENA GARCÍA LÓPEZ



**Coordinadora de la Unidad de Transparencia
del Poder Judicial del Estado de Sinaloa.**



10:04 am



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Culiacán, Sinaloa, a 01 de noviembre de 2024.
OFICIO DTIC-0676/2024.

LIC. NORMA LORENA GARCÍA LÓPEZ

Coordinadora de la Unidad de Transparencia.
Presente.

En atención a oficio número UT/268-001/2024, recibido el día 31 de octubre del año en curso, mediante el cual solicita información requerida electrónicamente a través de la PLATAFORMA NACIONAL DE TRANSPARENCIA con folio número 251264400026824, que a la letra dice:

"Solicito la siguiente información

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

En el tema de ciberseguridad, actualmente en esta institución si se cuenta con esquemas de seguridad de la información, los cuales se encuentran implementados bajo la protección de nuestros equipos firewall, en cada uno de nuestros centros de datos distribuidos por todo el Estado, además de que en cada equipo de cómputo conectado a nuestra red de dominio cuenta con seguridad antivirus.

Las áreas que participan son:

- Dirección de tecnologías de la información y comunicaciones.
- Administración de tecnologías de la información y comunicaciones.
- Departamento de redes y telecomunicaciones.
- Departamentos de tecnologías de la información y comunicaciones regionales norte, centro y sur.
- Unidades de tecnologías de la información de cada una de nuestras Sedes de Justicia Penal Acusatoria y Oral de las regiones norte, centro, sur y centro-norte.

- 2. Señalar sí de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en***



PODER JUDICIAL

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

el DOF el 6 de septiembre de 2021, se han implementado las siguientes medidas:

a) estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios de seguridad de la información o tecnologías de la información y comunicación; b) 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); 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).

- a) No se cuenta con ello.
- b) Actualmente no se cuenta con 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; Por otro lado, si se cuenta con un inventario institucional de bienes de TIC, el cual es administrado y controlado por la Administradora de Bienes Informáticos de esta Dirección de Tecnologías a través de un aplicativo informático. En cuanto a servicios de TIC, se cuenta con un portafolio de proyectos dentro del cual se incluyen los servicios que presta esta Dirección a los usuarios.
- c) No se cuenta con ello.
- d) No se cuenta con ello.
- e) No se cuenta con ello.
- f) No se cuenta con ello.
- g) Si se cuenta con una política general de seguridad de la información, el cual está contenido en el Manual de Políticas y Estándares de Seguridad Informática, implementado en el año 2017 y su última revisión es abril del 2018.
- h) No se cuenta con ello.
- i) Si, personal adscrito al Departamento de Redes y Telecomunicaciones en coordinación con el Administrador de Tecnologías de la Información, pertenecientes a esta Dirección de Tecnologías, además de tres empresas externas que nos apoyan mediante una póliza de servicios, para responder a eventuales incidentes de seguridad o cibernéticos.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

- 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;**

La estrategia de ciberseguridad que se sigue dentro de la institución, es la implementación de esquemas de seguridad mediante dispositivos firewall para la protección de la información contenida en nuestros centros de datos, seguridad antivirus en cada equipo de cómputo conectado a nuestra red de dominio, así como una plataforma de respaldos en tres capas como medida de seguridad ante una eventual falla de servidores o eliminación de información.

- i. La fecha de creación de esta estrategia fue en el año 2010.
- ii. La fecha de implementación fue en el transcurso del 2010.
- iii. El esquema de seguridad perimetral para la protección de los centros de datos se ha redimensionado en una sola ocasión por renovación de equipo obsoleto y nuestro esquema de respaldos se modificó a un esquema de 3 capas para incrementar la seguridad de la información.
- iv. Dirección de Tecnologías, Administración de Tecnologías y Departamento de Redes y Telecomunicaciones.

- 4. Informar si se emplea la firma electrónica avanzada en la institución;**

Si, actualmente se emplean dos firmas electrónicas avanzadas la "FIREL" y "FIEL", las cuales se utilizan para realizar trámites a través de nuestro portal Tribunal Electrónico y en algunos aplicativos informáticos implementados en esta Institución.

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

Periódicamente y de manera aleatoria se llevan a cabo acciones de restauración de servidores virtuales desde nuestras plataformas de respaldos, con la finalidad de verificar la integridad de la información ante una eventual falla de nuestros servidores.

- 6. Señalar si en la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información, de ha contado con el Dictamen Técnico favorable expedido por la CEDN, de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la**



PODER JUDICIAL

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021;

Actualmente no se cuenta con algún Dictamen Técnico favorable expedido por la CEDN, en la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información, en esta Dirección de Tecnologías.

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

La infraestructura tecnológica de los centros de datos para la prestación de servicios es propia en su totalidad, adicionalmente contamos con el servicio de hosting de nuestro portal y la prestación de algunos servicios en tribunal electrónico con una empresa externa.

8. Informar si se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con los siguiente: a) inserción de leyenda de confidencialidad de 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 se cuenta con correo electrónico institucional bajo el dominio @stj-sin.gob.mx

- a) Cada correo electrónico enviado desde nuestro correo electrónico institucional cuenta con una leyenda de confidencialidad de la información que a la letra dice: "Este correo electrónico (y cualquier anexo al mismo) podría contener información que es confidencial, privilegiada y reservada bajo la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados o que por alguna otra razón no debe ser revelada. Si usted no es el destinatario de este correo electrónico, por favor no lo revise, copie o distribuya por ningún medio. Por favor informe al remitente que lo ha recibido por error y bórrelo junto con cualquier anexo del mismo. Si usted no es el destinatario de este correo electrónico, tiene prohibido llevar a cabo cualquier acto derivado o relacionado con la información que este correo contiene. Revelar información confidencial o privada es fuente de sanciones civiles y penales."
- b) Personal adscrito al Departamento de Redes y Telecomunicaciones en coordinación con el Administrador de Tecnologías de la Información y Comunicaciones de esta Dirección, administran todo el correo entrante y saliente.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

- c) El correo electrónico institucional cuenta con una solución Virtual de AntiSpam para el filtrado de correo entrante y saliente, así como el Antivirus institucional que a través de reglas de seguridad verifica la integridad de la información.
- d) Nuestro correo institucional si cuenta con cifrado en el envío de información.

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

Se cuenta con un Código de Ética del Poder Judicial del Estado de Sinaloa, en el cual se estipulan una serie de artículos y donde se exhorta a las y los servidores judiciales a cumplir con ciertos mecanismos para evitar la divulgación no autorizada de información ya sea en papel o digital. Este código de ética se encuentra disponible para todos los usuarios a través de nuestro portal:

www.stj-sin.gob.mx/assets/files/leyes/codeticapjsin.pdf

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

- a) Si se cuenta con aviso de privacidad accesible a través de nuestro portal en la siguiente liga:

www.stj-sin.gob.mx/assets/files/transparencia/aviso_privacidad_integral.pdf

Así como también contamos con un aviso de privacidad simplificado

accesible a través de la siguiente liga:

tribunal.stj-sin.gob.mx/build/data/aviso_privacidad_simplificado.pdf

- b) Si contamos con certificado digital vigente, este es renovado anualmente y fue emitido para nuestro dominio "stj-sin.gob.mx" por parte de "Sectigo RSA Domain Validation Secure Server CA".

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

No se cuenta con capacitación en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

12. 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;

- a) Dentro de esta Dirección no contamos con mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información, sin embargo, una de las empresas externas que nos apoya con una póliza de servicios, si lleva a cabo periódicamente evaluaciones para



PODER JUDICIAL

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

medir la seguridad de la información, y en su caso nos indica las acciones a seguir para adecuar los controles de seguridad.

- b) Esta Dirección no cuenta con indicadores para medir la madurez institucional en la gestión de seguridad de la información.

13. 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 y cuántas horas de capacitación en ciberseguridad se realizan de forma anual.

Esta Dirección no cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad, sin embargo, eventualmente se llevan a cabo campañas en las que se publican carteles y banners en los equipos de las y los servidores judiciales, con el propósito de concientizar al usuario en el tema de la seguridad de la información.

14. 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?;

Por el momento no se cuenta con un sistema o herramienta informática de gestión de protección de datos personales de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

15. 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, lo anterior en términos de lo establecido por los artículos 40, 41 y 42 de la Ley General de protección de datos personales en posesión de sujetos obligados (LGPDPPO);

Actualmente esta Dirección no 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.

16. 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, lo anterior en términos de lo establecido por los artículos 40, 41 y 42 de la Ley General de protección de datos personales en posesión de sujetos obligados (LGPDPPO);

Esta Dirección por el momento no cuenta con un modelo o sistema de



PODER JUDICIAL

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de información.

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

Esta Dirección cuenta con un control interno para el traslado de activos físicos de la institución, mediante la firma de resguardos administrados por la Administradora de Bienes Informáticos, sin embargo, no tiene conocimiento si alguna otra dependencia lleve a cabo lineamientos para el mismo traslado.

18. Informar si las personas encargadas de sistemas de información, donde se brindé 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.

La Dirección de Tecnologías toda vez que culmina el desarrollo de los sistemas de información, proporciona capacitación técnica de estas herramientas informáticas a las y los servidores judiciales para su implementación, sin embargo, no tiene conocimiento si los usuarios de los sistemas tienen previamente los conocimientos comprobables para brindar información de carácter público.

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

Se han tenido dos ataques confirmados de virus tipo Ransomware, el primero de ellos fue en diciembre de 2019 y el segundo a principios del año 2023.

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

En materia de protección de datos personales esta Dirección coadyuva mediante la implementación de las siguientes acciones:

1. Bloqueo de dispositivos de almacenamiento extraíble.
2. Cifrado de discos mediante seguridad en cada estación de trabajo.
3. Contamos con software Anti-Malware en cada estación de trabajo.
4. Contamos con Firewall para la seguridad perimetral, además de detector de intrusos por medio de software.
5. Nuestro correo electrónico institucional no puede ni debe responderse de manera automática.
6. Contamos con mecanismos de autenticación (usuario y contraseña) para cada funcionario judicial esto por medio de Microsoft Active Directory, además de un servicio de autenticación para nuestras aplicaciones y sistemas de gestión institucionales.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

7. Tenemos reglas y políticas para el manejo de la información electrónica plana. Manejadas a través de nuestro directorio activo y consola de seguridad antivirus.
8. Contamos con filtrado web a través de nuestro Firewall.

21. 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;

Actualmente no se cuenta con un sistema o plataforma informática, aplicación electrónica que se emplee para el tratamiento intensivo de datos personales de conformidad de la Ley en la materia.

22. ...

23. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;

Ante un eventual caso de incidente de ciberseguridad o seguridad de la información, esta Dirección solo comunica a la Presidencia de este Supremo Tribunal, quien es la encargada de dictar los lineamientos a seguir y de las formas para comunicar a los titulares de cada dependencia u órgano jurisdiccional.

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

Para nuestra infraestructura tecnológica las medidas de ciberseguridad se actualizan diariamente por medio de Políticas de Antivirus, Actualizaciones de DAT o base de datos de malware para detección, Políticas de Firewall, Actualizaciones del motor de Firewall.

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

Solo se han llevado a cabo auditorías externas en dos ocasiones a solicitud de la propia Dirección y se aplicaron de manera eventual, en cuanto a las auditorías internas no se ha llevado a cabo ninguna.

26. 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. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Si se cuenta un sistema de mesa de ayuda que registra las incidencias en materia de TI reportadas por los servidores judiciales y es operado por el personal de recepción de esta Dirección, este sistema es de tipo interno.

27. Informar si se cuenta con un Centro de Operaciones de Ciberseguridad. Además informar si se han tenido incidentes de ciberseguridad (sin importar ni decir cuáles).

Actualmente esta Dirección no cuenta con un Centro de Operaciones de Ciberseguridad, sin embargo, todos los incidentes de ciberseguridad son atendidos por personal adscrito al Departamento de Redes y Telecomunicaciones en conjunto con el Administrador de Tecnologías de la Información, pertenecientes a esta Dirección de Tecnologías. A la fecha se han tenido dos ataques confirmados de virus tipo Ransomware.

Sin otro particular aprovecho la ocasión para enviarle un cordial saludo.

SUPREMO TRIBUNAL DE JUSTICIA DEL
ESTADO DE SINALOA



PODER JUDICIAL
DIRECCIÓN DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Atentamente

LIC. JUAN GABRIEL AVILA OSUNA

Director de Tecnologías de la Información y Comunicaciones

