

C. SOLICITANTE
Presente:

Por este medio le saludo cordialmente, y en atención a su solicitud de información pública recibida por la Plataforma Nacional de Transparencia (PNT), el día 31 treinta y uno de octubre de 2024 dos mil veinticuatro, a las 14:50:51 catorce horas con cincuenta minutos, en horario hábil, y registrada con el número de folio 140280224000945; le informo lo consecutivo:

I. Usted solicitó lo siguiente:

«...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 (LGPDPPO);
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 (LGPDPPO);
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) ...»

II. Por otro lado, y en virtud de que se trata de información pública conforme a lo que establece el artículo 3 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; esta Dirección de Transparencia de conformidad a lo establecido en el arábigo 32 fracciones III y VIII de la citada Ley, se da contestación a las preguntas señaladas con los números:

11.- Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.
R.- No se cuenta con esta capacitación.

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.
R.- a) No se cuenta con esos mecanismos.

b) No se cuenta con esos indicadores.

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.

R.- No se cuenta con ese programa.

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?

R.- En atención a lo solicitado, se le informa que este Consejo no lo rige la normativa señalada, tal y como se desprende del artículo 2 de dicho ordenamiento legal.

De igual forma, si se cuenta con un sistema de gestión de protección de datos personales, al cual podrá tener acceso, ingresando a la página del Consejo de la Judicatura del Estado de Jalisco, a la página: <https://cjj.gob.mx/> y trasladarse a la parte final de la página principal en comentario y darle click al: Documento de Seguridad o bien ingresar directamente al link:

https://cjj.gob.mx/assets/downloads/DOCUMENTO_SEGURIDAD_CONSEJO_JUDICATURA.pdf

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 (LGPDPPO);

R.- Se encuentra inserto en el documento de seguridad; al cual podrá tener acceso, ingresando a la página del Consejo de la Judicatura del Estado de Jalisco, a la página: <https://cjj.gob.mx/> y trasladarse a la parte final de la página principal en comentario y darle click al: Documento de Seguridad o bien ingresar directamente al link:

https://cjj.gob.mx/assets/downloads/DOCUMENTO_SEGURIDAD_CONSEJO_JUDICATURA.pdf

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 (LGPDPSSO):

R.- Se encuentra inserto en el documento de seguridad; al cual podrá tener acceso, ingresando a la página del Consejo de la Judicatura del Estado de Jalisco, a la página: <https://cej.jgb.mx/> y trasladarse a la parte final de la página principal en comentario y darle click al: Documento de Seguridad o bien ingresar directamente al link:

https://cjj.gob.mx/assets/downloads/DOCUMENTO_SEGURIDAD_CONSEJO_JUDICATURA.pdf

17. Informar si 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 con dispositivos móviles oficiales

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.

R.- Se le informa que el personal adscrito a la Unidad de Transparencia de este Consejo, que se encarga e brindar la información pública, cuenta con capacitación en materia de transparencia y protección de datos personales.

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

R.- Hasta el momento no se ha tenido.

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

R.- Para estar en aptitud de dar respuesta, se le hace de su conocimiento que podrá ingresar a la página del Consejo de la Judicatura del Estado de Jalisco, a la página: <https://cjj.gob.mx/> y trasladarse a la parte final de la página principal en comentario y darle click al: Documento de Seguridad o bien ingresar directamente al link:

https://cjj.gob.mx/assets/downloads/DOCUMENTO_SEGURIDAD_CONSEJO_JUDICATURA.pdf

Como parte de mejores prácticas en materia de datos personales, se informa que, mediante la Décima Tercera Sesión Extraordinaria del Comité de Transparencia de este Consejo, se aprobaron los mecanismos o controles para la debida acreditación de la identidad de las personas promoventes en los procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición. Asimismo, se actualizaron los formatos para las solicitudes de Derechos ARCO por comparecencia.

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:

R.- No se cuenta con esos mecanismos

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

R.- Sí, y está publicado en el siguiente link:

https://cjj.gob.mx/assets/downloads/DOCUMENTO_SEGURIDAD_CONSEJO_JUDICATURA.pdf

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

R.- No, no se cuenta con un plan específico de comunicación.

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

R.- No se cuenta con un período de tiempo establecido.

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

R.- No, no se cuentan con auditorías internas y/o externas.

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.

R.- No, no se cuenta con un help desk.

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)

R.- No, no se cuenta con un centro de ciberseguridad y no se han presentado incidentes que reportar...»

III. En consecuencia, el sentido de respuesta a su solicitud de acceso a la información es **AFIRMATIVO PARCIALMENTE**, y ha sido atendida de conformidad con lo dispuesto por los artículos 3º tercero, 32 treinta y dos, párrafo 1 primero, fracciones III y IV, 79 setenta y nueve, 84 ochenta y cuatro, 86 ochenta y seis, fracción II, 87 ochenta y siete, y demás relativos y aplicables de la LTAIPEJM.

En caso de que usted requiera asesoría adicional, o bien, si tiene alguna duda sobre su solicitud, le invitamos a que acuda a la sede de esta Dirección de Transparencia e Información Pública de este Consejo de la Judicatura del Estado de Jalisco, ubicada en la calle Paseo del Rincón del Diablo, número 38 treinta y ocho, primer piso, Colonia Centro, plaza tapatía, en la ciudad de Guadalajara, Jalisco, o bien vía telefónica a través del número 33 30012345, extensiones 2517 y 2332, en horario de 09:00 nueve horas a 15:00 quince horas, de lunes a viernes, para que establezca contacto con personal de esta Dirección, en los términos que dispone el artículo 32.1 fracción III de la LTAIPEJM.

ATTENTAMENTE:

GUADALAJARA, JALISCO, A 08 DE NOVIEMBRE DE 2024.

(FIRMADO ELECTRÓNICAMENTE)

LIC. SALVADOR CANTERO PACHECO

COORDINADOR GENERAL DE LA DIRECCIÓN DE

TRANSPARENCIA E INFORMACIÓN PÚBLICA

DEL CONSEJO DE LA JUDICATURA DEL ESTADO DE JALISCO.

| Firmante | Nombre: | SALVADOR CANTERO PACHECO | Validez: | OK | Vigente |
|----------|---------------------------------|---|------------|----|-------------|
| Firma | # Serie: | 706a662020746532000000000000000000000011e1 | Revocación | OK | No Revocado |
| | Fecha: (UTC / Ciudad de México) | 08/11/2024T19:28:20Z / 08/11/2024T13:28:20-06:00 | Status: | OK | Valida |
| | Algoritmo: | Sha256withRSA | | | |
| | Cadena de Firma: | <div>59 e2 4c e6 e5 ab c1 f1 fe c1 6a 26 30 ec 21 2f</div> <div>07 0c 00 11 2d 40 99 17 5c bb 45 7e ad 85 a9 22</div> <div>2d 4f f1 48 4f d5 3e e4 8d 54 2c 8f 7f 3e 3f 6e</div> <div>d0 01 dd b2 2f 06 01 1c bd e2 10 8b 17 1e ac d4</div> <div>94 51 85 27 af 28 21 18 94 48 4a 1f 06 df 2d fb</div> <div>6e ec de 53 e9 16 5d 93 98 9c ae 75 41 b6 ed 56</div> <div>73 26 80 0f 32 f3 a0 72 61 90 71 8a de 3a 5c 9d</div> <div>e9 0f 9a 54 92 55 7f fd 3d 44 e3 05 a8 77 02 36</div> <div>cf 21 ed 64 01 f2 38 04 da 16 ad f8 ac 8f 92 2a</div> <div>47 75 fa 19 ab 01 52 41 e0 a7 77 f7 c3 be 20 cc</div> <div>6c 04 0c 7d 2d b4 c1 49 29 a4 0a 2a 53 5d 6d f6</div> <div>26 68 ce 2a 23 82 54 1a 2a b7 08 ad e8 a0 46 ed</div> <div>ff 8b 0b 34 8e 3a 22 30 b3 f1 36 a5 f0 fc 38 a6</div> <div>7a c8 13 63 55 4f 3c 3b 4c 3f 91 74 bb bf b9 da</div> <div>d0 de f4 e7 ed 0c 3b a3 3d d0 06 91 ed e4 c0 e7</div> <div>2b b7 33 d2 fa f8 33 df 95 62 21 16 30 6c 3c 62</div> | | | |
| OCSP | Fecha: (UTC / Ciudad de México) | 08/11/2024T07:28:34Z / 08/11/2024T13:28:34-06:00 | | | |
| | Nombre del respondedor: | OCSP de la Unidad de Certificacion Electronica del TEPJF - PJF | | | |
| | Emisor del respondedor: | Unidad de Certificación Electrónica del TEPJF - PJF | | | |
| | Número de serie: | 303030323330 | | | |