CONSEJO DE LA JUDICATURA
PODER JUDICIAL DEL ESTADO DE JALISCO

OF. 2102/2024 EXP. 1066/2024 DIRECCIÓN DE TRANSPARENCIA E INFORMACIÓN PÚBLICA DEL CONSEJO DE LA JUDICATURA DEL ESTADO DE JALISCO

C. SOLICITANTE
P r e s e n t e:

Se le brinda un cordial saludo y a la vez hacerle de su conocimiento que se recibió la solicitud de acceso a la información a través de Plataforma Nacional de Transparencia, generándose, bajo el número de folio **140280224000944**, de la cual se desprende la siguiente información:
Usted solicitó lo siguiente:

«…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 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); 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). 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 sí 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 sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero; 8. 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; 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 sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos; 10. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes; …» (sic).

SALVADOR CANTERO PACHECO
706A6620274653200000000000000000000011E1
2026-05-15 18:00:00

SCP/cve/dara

OF. 2102/2024 EXP. 1066/2024 DIRECCIÓN DE TRANSPARENCIA E INFORMACIÓN PÚBLICA DEL CONSEJO DE LA JUDICATURA DEL ESTADO DE JALISCO

I. Con fundamento los artículos 32 treinta y dos, párrafo 1 primero, fracciones III y VIII de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios (LTAIPEJM), se determinó a la Unidad Departamental de Informática del Consejo de la Judicatura, con el oficio número **2016/2024 EXP. 1066/2024** para que hiciera las búsquedas inherentes a efecto de que entregaran la información solicitada, por lo que se recibe el oficio número **UDI/101/2024** signado por el Lic. Francisco Javier de León González, en su carácter de Jefe de la Unidad Departamental de Informática del Consejo de la Judicatura del Estado de Jalisco, en el cual informa:

«… Por medio del presente y en contestación al Oficio 2016/2024 Exp. 1066/2024 recibido el día 05 de Noviembre del año en curso por medio del correo electrónico oficial de esta Unidad Departamental de Informática, en donde se solicita lo siguiente:
<<...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;
No se cuenta con ese sistema de mecanismos, ni protocolos en esta dependencia.

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;
No se han implementado esas medidas.

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 una Inventario Institucional de bienes y servicios de TIC;
Solo se cuenta con el inventario de bienes y servicios de TI.

c) un plan de continuidad de operaciones, y señalar la fecha de implementación;
No se cuenta con esos planes

d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;
No se ha desarrollado.

e) desarrollado e implementado un programa de gestión de vulnerabilidades;
No se ha implementado.

f) Marco de Gestión de Seguridad de la Información (MGSI);
No se cuenta con 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;
No se cuenta con una política general de seguridad de la información estipulada, sin embargo, los servicios informáticos con los que cuenta la dependencia mantienen las políticas de seguridad de las empresas que brindan el servicio, tales como, AWS, FORTINET, Cisco Webex, entre otros.

h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos

SALVADOR CANTERO PACHECO
706A6620274653200000000000000000000011E1
2026-05-15 18:00:00

SCP/cve/dara

esenciales de la Institución;
No se cuenta con esa información.

i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC).
No se cuenta con un ERISC, sin embargo, en caso de que suceda un tema de seguridad informática, la Unidad Departamental de Informática, se apoyaría de sus proveedores de AWS, FORTINET, etc.

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;
No se cuenta con un estrategia de ciberseguridad integral.

4. Informar sí se emplea la firma electrónica avanzada en la institución;
Si, el uso de Firel y de e.firma del SAT.

5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;
No se realizan.

6. Señalar sí 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.
No se cuenta con ese contrato ni el dictamen.

7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;
Algunos servicios son propios y también existen servicios en la nube de AWS.

8. 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;
Si se cuenta con correo electrónico institucional y solo ciertas cuentas de correo tienen la inserción de la leyenda de confidencialidad.
c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;
Se cuenta con la administración y consola de Google Workspace
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;
Se cuenta con las herramientas propias de la consola de Google Workspace para dicho fin
e) cuenta con cifrado en el envío de información.
Si se cuenta con cifrado.

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

SCP/cve/dara

SALVADOR CANTERO PACHECO
706A6620274653200000000000000000000011E1
2026-05-15 18:00:00

10. Informar sí la página web de la institución cuenta con:
a) aviso de privacidad;
Si, dentro de la sección de transparencia.

b) certificados digitales vigentes;...» (Sic)
Si, **Certificado**
cjj-gob.mx - ESET SSL Filter CA
Nombre del interesado - cjj.gob.mx

Nombre del emisor
ESET SSL Filter CA, ESET, spol. s r. o.
País SK

Validez
No antes Mon, 18 Dec 2023 00:00:00 GMT
No después Wed, 15 Jan 2025 23:59:59 GMT …»

II. 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 3° 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 Paseo Rincón del Diablo #38, Colonia Centro, 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.

A T E N T A M E N T E:
GUADALAJARA, JALISCO, A 11 DE NOVIEMBRE DE 2024

(Firmado electrónicamente)
LICDO. SALVADOR CANTERO PACHECO
COORDINADOR GENERAL DE LA DIRECCIÓN
DE TRANSPARENCIA E INFORMACIÓN PÚBLICA
DEL CONSEJO DE LA JUDICATURA DEL ESTADO DE JALISCO

CONSEJO DE LA JUDICATURA
PODER JUDICIAL DEL ESTADO DE JALISCO
Dirección de Transparencia e Información Pública

SALVADOR CANTERO PACHECO
706A6620274653200000000000000000000011E1
2026-05-15 18:00:00

SCP/cve/dara

Evidencia Criptográfica – Transacción

Archivo Firmado: pkcs7_1731356676732.doc

Autoridad Certificadora: Autoridad Certificadora Intermedia del Consejo de la Judicatura Federal

Firmante(s):

Firmante	**Nombre:**	SALVADOR CANTERO PACHECO	**Validez:**	OK	Vigente
Firma	**# Serie:**	706a66202074653200000000000000000000011e1	**Revocación**	OK	No Revocado
	Fecha: (UTC / Ciudad de México)	11/11/2024T20:24:24Z / 11/11/2024T14:24:24-06:00	**Status:**	OK	Valida
	Algoritmo:	Sha256withRSA			
	Cadena de Firma:	c4 6a b0 a4 34 8f 1c 21 53 28 51 a9 3b 3c 5e 1e 7d 90 78 61 3f 46 7d b8 d3 7a 19 5b b7 62 ac 62 18 f9 00 a1 fb 39 1e c5 1d b3 63 e4 40 29 89 0e 33 d6 36 5d 4d cb 03 1e bb 6f 7b f4 dd 17 70 ed f0 cb 61 13 7f 6d 97 4b 5f 1f 35 d0 f3 da 7d 4d 0c c0 c0 1e c3 bd e3 07 c2 01 ec fa 96 3b ca 0f cf 0a 5c d5 24 3a 8a ee 05 6d 01 42 6b 3f ba 6d d6 43 71 ef 5a dd 43 82 86 35 dc f0 37 ba 66 f5 e4 bb e2 d0 1f 66 34 a7 da ab 4a 5c 31 c8 d6 98 d6 f0 f5 80 e1 e4 60 9f 2b e8 2c bc a3 ca de 84 0d 98 74 f3 f1 d4 6e 2c e7 7f 73 94 0c 5a 10 d6 cc 6b 39 94 c2 ff 08 f9 2a e9 c4 d2 9c 3b b5 66 cf f7 c6 73 de 41 f5 7a 05 01 2e b4 d6 ed f2 4f 33 e3 7a 45 56 7d e8 14 08 36 72 b5 af c7 26 78 ba e0 1a 6c fd a7 b0 49 88 22 cf f7 11 76 b9 bf 58 42 7d 70 d5 d6 7c 03 af 4d ad b1 7e 05 7e 5c			
OCSP	**Fecha: (UTC / Ciudad de México)**	11/11/2024T08:24:38Z / 11/11/2024T14:24:38-06:00			
	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			