

Oficio: UTAIPPJE/1462/2024

Xalapa, Equez., Ver., 13 de noviembre de 2024

PERSONA SOLICITANTE DE LA INFORMACIÓN PRESENTE

VISTO: El estado que guarda el procedimiento de acceso a la información derivado de la solicitud formulada a través de la Plataforma Nacional de Transparencia, identificada con el número de folio **301277624000440**, y;

RESULTANDO

1.- Con fecha 30 de octubre de 2024, se presentó la solicitud al tenor de los rubros siguientes:

"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;

Datos complementarios: 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. Informar 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)." [sic]

Por lo que en términos de los numerales 6 de la Constitución Política de los Estados Unidos Mexicanos, 6 de la Constitución Política del Estado de Veracruz de Ignacio de la Llave, 9 fracción II, 11 fracción XVI, 12, 132, 134 fracción II y 145 de la Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, este sujeto obligado es competente para dar respuesta de conformidad a los siguientes:

CONSIDERANDOS

PRIMERO.- El siete de febrero de dos mil catorce, se promulgó en el Diario Oficial de la Federación, el Decreto mediante el cual se reforman y adicionan diversas disposiciones de la Constitución Política los Estados Unidos Mexicanos, entre ellos el artículo 6 en materia de transparencia.

SEGUNDO.- El Decreto anteriormente citado, refería la obligación de la expedición de una Ley General de Transparencia y Acceso a la Información Pública, misma que fue publicada el cuatro de mayo del año dos mil quince en el Diario Oficial de la Federación, entrando en vigor al día siguiente de su publicación, acorde con lo dispuesto en el artículo Primero Transitorio de la referida Ley General.

TERCERO.- La Ley General estableció las bases, principios y procedimientos que deberán observar las autoridades, entidades, órganos y organismos de los Poderes Ejecutivos, Legislativos y Judicial, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral y demás sujetos obligados, en los tres niveles de gobierno, para la atención del derecho de acceso a la información, la transparencia y la rendición de cuentas.

CUARTO.- Con la expedición de la Ley General se dotó de nuevas atribuciones a los organismos garantes y a los sujetos obligados, estableciendo entre otros aspectos, las bases generales para homogeneizar el ejercicio del derecho de acceso a la información, la difusión proactiva de información de interés público, así como la promoción de la cultura de la transparencia, la rendición de cuentas y la participación ciudadana en la toma de decisiones públicas para contribuir a la consolidación de la vida democrática.

QUINTO.- La Ley General estableció la obligación a las entidades federativas de homologar sus respectivas leyes estatales conforme a los principios y bases del citado ordenamiento.

SEXTO.- El día jueves veintinueve de septiembre del año dos mil dieciséis, se promulgó en la Gaceta Oficial del Estado, la Ley Número 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, la cual contempla como sujeto obligado al Poder Judicial, que atiende en este acto con base a la seguridad jurídica tutelada por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, misma que se salvaguarda cuando las personas conocen cuáles serán las consecuencias de los actos que realizan las autoridades, y cuando el actuar de éstas se encuentra limitado y acotado, de tal manera que cualquier afectación a la esfera jurídica de las personas no resulte arbitraria.

Atendiendo a lo anterior se procede a formular la siguiente:

RESPUESTA

Se informa a la persona solicitante que esta Unidad de Transparencia, conforme a los numerales 6 de la Constitución Política de los Estados Unidos Mexicanos, 6 de la Constitución Política del Estado de Veracruz de Ignacio de la Llave, y lo dispuesto en los artículos, 45 fracciones II y IV y 134 de la Ley General de Transparencia y Acceso a la Información Pública y sus correlativos, 9 fracción II, 11 fracción XVI, 12, 132, 134 fracciones II y VII, y 145 de la Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, realizó todas las gestiones necesarias para cumplir con la entrega de la información solicitada ante la Subdirección de Tecnologías de la Información de la Dirección General de Administración del Consejo de la Judicatura del Poder Judicial. Se anexa oficio que da sustento a lo antes citado: **UTAIPPJE/1427/2024** de fecha cuatro de noviembre de dos mil veinticuatro.

Por lo anterior, estando dentro del plazo señalado por la Ley de la materia para dar respuesta a su solicitud, se hace entrega de la respuesta que fue remitida a esta Unidad mediante el oficio **STI-01322-2024**, signado por el Ing. Carlos Alberto Jiménez González, Subdirector de Tecnologías de la Información de la Dirección General de Administración, de fecha doce de noviembre de dos mil veinticuatro, recibido el mismo día, compuesto por cinco fojas, impresas por el lado anverso.

Para cualquier duda relacionada con la presente respuesta puede ponerse en contacto al teléfono 22 88 42 28 00 exts. 17204, 17205 y 17125, o al correo electrónico transparencia@pjeveracruz.gob.mx

Se le hace saber a la persona solicitante que, en caso de considerar que no se ha satisfecho su derecho de acceso a la información con la respuesta otorgada, podrá interponer el correspondiente recurso de revisión en términos del artículo 155 de la Ley 875 de Transparencia y Acceso a la Información Pública.

Sin otro particular por el momento, hago propicia la ocasión para enviarle un afectuoso saludo y me reitero a sus órdenes como Titular de la Unidad de Transparencia para atender cualquier situación inherente a la presente.

ATENTAMENTE



L.N.I. MARISELA GUADALUPE GONZÁLEZ MEZA RUEDA
TITULAR DE LA UNIDAD DE TRANSPARENCIA
Y ACCESO A LA INFORMACIÓN DEL PODER JUDICIAL

C.c.p. Archivo.

Folio UT: 1618/2024

4

"Comité de Ética: Noviembre, mes del Interés Público."



PODER JUDICIAL
DEL ESTADO DE VERACRUZ

"200 Años de Veracruz de Ignacio de la Llave como parte de la Federación 1824-2024"
SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

001618

STI-01322-2024

Asunto: Respuesta a solicitud de acceso a la información registrada bajo el
numero de folio 301277624000440

Xalapa-Enríquez, Veracruz, a 12 de Noviembre de 2024

UNIDAD DE TRANSPARENCIA
Y ACCESO A LA INFORMACIÓN PÚBLICA

LIC.(A) MARISELA GUADALUPE GONZALEZ MEZA RUEDA.

TITULAR, UNIDAD DE TRANSPARENCIA Y ACCESO A LA INFORMACION, XALAPA

P R E S E N T E

En atención al oficio número UTAIPPJE/1406/2024, recibido el día 04 de noviembre del año en curso, referente a la solicitud de acceso a la información registrada bajo el número de folio 301277624000440 de la Plataforma Nacional de Transparencia, al respecto y en lo que compete a esta Subdirección, me permito dar respuesta a los cuestionamientos planteados:

1.- Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o de ciberseguridad y cuales áreas participan.

Actualmente, la institución no cuenta con un gobierno de seguridad de la información o ciberseguridad. No obstante, se dispone de equipos dedicados a la seguridad que han logrado mantener la red interna sin contingencias relacionadas con accesos no autorizados. Esta red interna está habilitada en todos los sitios que forman parte de la institución, lo que asegura una cobertura integral. Además, se utiliza tecnología de certificados SSL en todos los portales institucionales, lo que refuerza la protección de los datos en tránsito y garantiza un acceso seguro a los sistemas en línea.

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;

No se han implementado los estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional del gobierno federal en la contratación de bienes y servicios de seguridad de la información o tecnologías de la información y comunicación. Cabe precisar que somos un ente estatal, y esta Subdirección no es responsable de llevar a cabo procesos de adquisición, arrendamiento de bienes o contratación de prestadores de servicios en el área de TIC.

Sin embargo, esta Subdirección sí realiza los requerimientos en materia de tecnologías de la información, para lo cual se efectúan estudios de costo-beneficio y análisis de mercado a fin de asegurar que las propuestas estén alineadas con las necesidades institucionales y con los principios de la Ley de Austeridad para el Estado de Veracruz de Ignacio de la Llave.

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;

En cuanto a las mejores prácticas en la gestión de las TIC aplicables a los procesos de contratación para la adquisición, arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información, esta Subdirección realiza propuestas y requerimientos con base en estudios de costo-beneficio y análisis de mercado que permiten optimizar la relación costo-calidad. Esto se realiza bajo los lineamientos de la Ley de Austeridad para el Estado de Veracruz de Ignacio de la Llave, buscando siempre satisfacer las necesidades tecnológicas de la Institución de forma eficiente y responsable.



PODER JUDICIAL
DEL ESTADO DE VERACRUZ

STI-01322-2024

**Asunto: Respuesta a solicitud de acceso a la información registrada bajo el
numero de folio 301277624000440
Xalapa-Enríquez, Veracruz, a 12 de Noviembre de 2024**

Asimismo, respecto al inventario institucional de bienes y servicios de TIC, sí se cuenta con un inventario en el cual se registran los bienes y servicios de TIC que se encuentran en operación dentro de la Institución, permitiendo así una gestión ordenada y eficiente de los recursos tecnológicos.

c) Un plan de continuidad de operaciones, y señalar la fecha de implementación;

Esta subdirección cuenta con un Manual Específico de Organización y un Manual Específico de Procedimientos, ambos aprobados por el Consejo de la Judicatura. El cual contiene procedimientos para garantizar que las funciones mínimas esenciales operen ante la ocurrencia de un fenómeno.

d) Informar si se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;

Esta Subdirección continúa con el desarrollo del Plan de Recuperación de Desastres, en espera de su aprobación próximo a implementarse una vez aprobado.

e) Desarrollado e implementado un programa de gestión de vulnerabilidades;

Esta subdirección ha desarrollado un Programa de Gestión de Riesgos, mismo que incluye actividades para responder ante y prevenir vulnerabilidades, descritas por la Certificación ISO 27001.

f) Marco de Gestión de Seguridad de la Información (MGSI);

Esta Subdirección aún no cuenta con un Marco de Gestión de Seguridad de la Información.

g) Informar si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuando se implementó;

Existe una Política Tecnológica, uno de sus apartados es: "Sobre la seguridad de la información", dicha política fue propuesta en febrero de 2024, en espera de aprobación; a la fecha se cuenta con medidas estandarizadas de ciberseguridad mediante la adquisición de hardware dedicado para esta labor.

h) Informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;

Esta subdirección cuenta con un Manual Específico de Organización y un Manual Específico de Procedimientos, ambos aprobados por el Consejo de la Judicatura.

i) Informar si se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC).

Esta Subdirección aún no cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información.

STI-01322-2024

**Asunto: Respuesta a solicitud de acceso a la información registrada bajo el
numero de folio 301277624000440**

Xalapa-Enríquez, Veracruz, a 12 de Noviembre de 2024

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 cuantas ocasiones;
- iv. Cuales áreas participaron en la creación de dicha estrategia.

El Programa de Gestión de Riesgos creado en noviembre de 2022 incluye estrategias en materia de ciberseguridad, donde se miden las amenazas y vulnerabilidades, y se proponen acciones de prevención y respuesta ante ellas; el catálogo de vulnerabilidades y amenazas está descrito por la Certificación ISO 27001.

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

Actualmente se utiliza la Firma Electrónica (FIREL) para firmar las actuaciones que realizan los Juzgados en Línea de este Poder Judicial.

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

Actualmente, no se realizan simulacros específicos del plan de recuperación de desastres ni en caso de incidentes cibernéticos. Sin embargo, llevamos a cabo monitoreo frecuente del tráfico de la red que accede a los servicios institucionales, lo que nos permite detectar y responder a posibles incidentes de manera proactiva.

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, se 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 ha contado con un Dictamen Técnico favorable expedido por la Coordinación de Estrategia Digital Nacional (CEDN) en los procesos de contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación. Esto se debe a que nuestra institución es un ente estatal y, por lo tanto, no forma parte de la Administración Pública Federal, por lo que no estamos sujetos a las disposiciones específicas de dicho Acuerdo en materia de contratación.

Cabe señalar que esta Subdirección no es la responsable de realizar los procesos de adquisición, arrendamiento o contratación de servicios en materia de TIC; su función se limita a la formulación de requerimientos que posteriormente son gestionados por el área correspondiente.

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

Un servicio está alojado en un centro de datos de otra institución gubernamental, todos los demás son propios de este Poder Judicial del Estado de Veracruz.



STI-01322-2024

**Asunto: Respuesta a solicitud de acceso a la información registrada bajo el
numero de folio 301277624000440**

Xalapa-Enríquez, Veracruz, a 12 de Noviembre de 2024

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:

Este Poder Judicial del Estado de Veracruz cuenta con un servicio de correo electrónico institucional.

a) Inserción de leyenda de confidencialidad de la información;

En este Poder Judicial, la inclusión de leyendas sobre confidencialidad o transparencia en los correos electrónicos es una responsabilidad asignada a cada usuario. De este modo, cada remitente es responsable de asegurar que sus comunicaciones incluyan cualquier advertencia necesaria sobre la privacidad de la información.

b) Control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;

La Subdirección de Tecnologías de la Información tiene bajo su gestión la operación y administración del servicio de correo electrónico, lo que incluye la supervisión y el control de los buzones de todos los usuarios de la institución. Esto garantiza un control centralizado de la totalidad de los correos institucionales.

c) Soluciones de filtrado para correo no deseado o no solicitado, así como programas informáticos que protejan del envío y recepción de correos con software malicioso;

El sistema de correo institucional incorpora herramientas de filtrado avanzadas que permiten la identificación y el bloqueo de correos no deseados, además de contar con protección contra correos que puedan contener software malicioso o de riesgo, tanto en el envío como en la recepción.

d) Cuenta con cifrado en el envío de información.

Para garantizar la seguridad y confidencialidad de los datos transmitidos, el servicio de correo institucional emplea cifrado en el envío de la información, asegurando la integridad y privacidad de los mensajes.

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

Actualmente en lo que compete a esta Subdirección de Tecnologías de la Información, cuenta con bitácoras de acceso y actividad en sistemas de información, así como al correo electrónico institucional, además otorga credenciales de acceso a estos solo a personal autorizado por los responsables de área.

10.- Informar si la página web de la institución cuenta con:

a) Aviso de privacidad;

La página web del Poder Judicial del Estado de Veracruz, no recaba en ningún momento datos personales de los usuarios que acceden a dicha página, razón por la cual no cuenta con aviso de privacidad específico, sin embargo, se precisa que sí se cuenta con un micrositio, en el que se pueden consultar todos los avisos de privacidad integrales y simplificados que han generado las diversas áreas administrativas del Poder Judicial del Estado de Veracruz, que recaban y dan algún tratamiento a datos personales respecto a algún determinado tramite y/o servicio, disponible en la siguiente dirección url: <https://www.pjeveracruz.gob.mx/avisos-de-privacidad/>.





PODER JUDICIAL
DEL ESTADO DE VERACRUZ

"200 Años de Veracruz de Ignacio de la Llave como parte de la Federación 1824-2024"
SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

STI-01322-2024

**Asunto: Respuesta a solicitud de acceso a la información registrada bajo el
numero de folio 301277624000440
Xalapa-Enríquez, Veracruz, a 12 de Noviembre de 2024**

b) Certificados digitales vigentes.

Todos los sitios web de este Poder Judicial cuentan con certificados de seguridad (SSL) vigentes.

Sin más por el momento, aprovecho la ocasión para enviarle un cordial saludo.

ATENTAMENTE

ING. CARLOS ALBERTO JIMÉNEZ GONZÁLEZ.
SUBDIRECTOR



Ccp.- MTRO.(A) DIANA ADIVEDH CRUZ VILLEGAS, DIRECTORA, DIRECCION GENERAL DE ADMINISTRACIÓN, XALAPA.-PRESENTE.- Para su conocimiento.
Ccp.- Archivo / DAG / lma

Oficio: UTAIPPJE/1427/2024
Xalapa, Equez., Ver., 04 de noviembre de 2024

MTRA. DIANA ADIVEDH CRUZ VILLEGAS
DIRECTORA GENERAL DE ADMINISTRACIÓN
DEL CONSEJO DE LA JUDICATURA
DEL PODER JUDICIAL DEL ESTADO DE VERACRUZ.

ING. CARLOS ALBERTO JIMÉNEZ GONZÁLEZ
SUBDIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN
DE LA DIRECCIÓN GENERAL DE ADMINISTRACIÓN
P R E S E N T E S



VISTO: El estado que guarda el procedimiento de Acceso a la Información derivado de la solicitud formulada a través de la Plataforma Nacional de Transparencia, identificada con el número de folio **301277624000440**, y

RESULTANDO

1-Con fecha 30 de octubre del año 2024, se presentó la solicitud al tenor de los rubros siguientes:

"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 la 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; "...[sic]

Por lo que en términos de los numerales 6 de la Constitución Política de los Estados Unidos Mexicanos, 6 de la Constitución Política del Estado de Veracruz de Ignacio de la Llave, 9 fracción II, 11 fracción XVI, 12, 132, 134 fracción II, 143 y 145 de la Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, 1, 2, 3, 124 y 125 de la Ley Orgánica del Poder Judicial del Estado de Veracruz de Ignacio de la Llave; 7 fracción IV, 68 y 69 del Reglamento Interior del Consejo de la Judicatura, artículo 4, 11, 36, 37 y 38 del Reglamento Interior de la Dirección General de Administración, en lo que respecta a la solicitud existen facultades legales para dar respuesta de conformidad a los siguientes:

TÉRMINOS EN MATERIA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PARA DAR RESPUESTA

PRIMERO.- Datos insuficientes o erróneos: De considerar que los datos contenidos en la solicitud son insuficientes o erróneos para otorgar el acceso a la información, debe remitir su prevención escrita a esta Unidad, dentro de los **03 días hábiles** siguientes a aquel en que haya recibido la solicitud, es decir, a más tardar el **07 de noviembre de 2024**. Con fundamento en el artículo 140 de la Ley número 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz.

SEGUNDO.- Información disponible: Si la información requerida por el solicitante ya está disponible al público en medios impresos, tales como libros, compendios, trípticos, registros públicos, en formatos electrónicos disponibles en Internet o en cualquier otro medio, la entrega de información y envío de respuesta a esta Unidad, debe realizarse dentro de los **03 días hábiles** siguientes a aquel en que se haya recibido la solicitud, por lo tanto, debe remitir su respuesta a más tardar el día **07 de noviembre de 2024**. Con fundamento en el artículo 130 de la Ley General de la materia.



TERCERO.- Clasificación de información: Si su área determina que la información solicitada es reservada o confidencial, debe remitir su solicitud de clasificación a esta Unidad, con la debida prueba de daño fundada y motivada, agregando carátula, para consideración del Comité de Transparencia y remitir la versión pública del documento a entregar, dentro de los **05** días hábiles siguientes a aquel en que haya recibido la solicitud, es decir, a más tardar el **11 de noviembre de 2024**. Con fundamento en el artículo 149 de la Ley número 875 de Transparencia.

CUARTO.- Inexistencia de información: Si la información solicitada no se encuentra en su archivos, debe enviar a esta Unidad dentro de los **05** días hábiles siguientes a aquel en que se haya recibido la solicitud, un informe en el que exponga de manera fundada y motivada las razones que motivan la inexistencia, para análisis del Comité de Transparencia, quien resolverá la declaración formal de inexistencia en términos de los artículos 150 y 151 de la Ley antes citada, por lo que deber remitir su inexistencia a más tardar el **11 de noviembre de 2024**.

QUINTO.- Solicitud de prórroga: Si requiere solicitar prórroga para responder la solicitud, debe enviar su solicitud fundada y motivada a esta Unidad dentro de los **05** días hábiles siguientes a aquel en que se haya recibido la solicitud, pidiendo que dicha prórroga sea sometida a la consideración de Comité de Transparencia, por lo que deberá solicitar prórroga a más tardar el día **11 de noviembre de 2024**. Con fundamento en el artículo 147 de la Ley de Transparencia Local.

SEXTO.- Respuesta y entrega de información: La entrega normal de información y envío de respuesta a esta Unidad, debe realizarse dentro de los **05** días hábiles siguientes a aquel en que se haya recibido la solicitud, por lo tanto, debe remitir su respuesta a más tardar el día **11 de noviembre de 2024**. Con fundamento en el artículo 145 de la Ley de la materia.

SÉPTIMO: Vista al inmediato superior: En caso de que algún servidor público se niegue a colaborar con ésta Unidad de Transparencia, para dar trámite al presente Procedimiento de Acceso a la Información, sin causa justificada, debe hacerlo del conocimiento de esta área, para los avisos que resulten de conformidad con el artículo 135 de la multicitada Ley de Transparencia para el Estado de Veracruz.

Sin otro particular, le reitero mi consideración y estima.

ATENTAMENTE

L.N.I. MARISELA GUADALUPE GONZÁLEZ MEZA RUEDA
TITULAR DE LA UNIDAD DE TRANSPARENCIA
Y ACCESO A LA INFORMACIÓN DEL PODER JUDICIAL

C.c.p. Archivo.

Acuse de Recibo de Solicitud de Información

Hemos recibido exitosamente su solicitud de información, con los siguientes datos:

Nº de folio: 301277624-109-4
Fecha de presentación: 30/10/2024 15:26:18 PM
Nombre del solicitante: Qt
Usuario: cybertichu@protonmail.com
E-mail:

Denominación Social:

Nombre del representante:

Entidad pública a quien se solicita
la información:

Poder Judicial del Estado de Veracruz

INFORMACIÓN SOLICITADA:

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

Acuse de Recibo de Solicitud de Información

INFORMACIÓN SOLICITADA:

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;

Forma de entrega de la
información:

Sistema de Solicitudes de Información de la Plataforma Nacional de Transparencia

Documentación Anexa

Fecha de inicio de trámite:

De conformidad en lo dispuesto por el artículo 145 de la Ley de Transparencia y Acceso a la Información Pública, para el Estado de Veracruz de Ignacio de la Llave, su solicitud de acceso a información pública será atendida a partir del día 04/11/2024.

La solicitud recibida después de las 18:00 horas de un día hábil o en cualquier hora de un día inhábil, se tendrá por recibida el día hábil siguiente.

Plazos de respuesta y posibles notificaciones a su solicitud.

1) Respuesta a su solicitud:	0 días hábiles	19/11/2024
2) En caso de que se requiera más información:	5 días hábiles	11/11/2024
3) Respuesta si se requiere más tiempo para localizar la información:	20 días hábiles	03/12/2024

OBSERVACIONES:

Las notificaciones se le comunicarán a través del medio que usted haya seleccionado, independientemente de lo anterior; las notificaciones oficiales se realizarán vía Plataforma Nacional de Transparencia.

Si usted recibe una notificación de que se requieren más datos para atender su solicitud y no la responde en el tiempo establecido, su solicitud será desechada por el sistema.

Para darle seguimiento a su solicitud de información, puede consultar la Plataforma Nacional de Transparencia, ingresando su número de folio o acudir a las oficinas del sujeto obligado correspondiente.