Xalapa, Ver., 08 de noviembre de 2024
Oficio: OPLEV/UTT/1872/2024
Asunto: Respuesta a solicitud de acceso a la información.

Estimada persona solicitante:
P r e s e n t e.

En atención a su solicitud de información recibida en la Plataforma Nacional de Transparencia con el número de folio 300564024000398, le comunico lo siguiente:

Del trámite interno:

De conformidad con los artículos 45 fracciones II, IV y XII, 131 de la Ley General de Transparencia y Acceso a la Información Pública; 134 fracciones II, IV, VII y XVIII de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave; 111 fracción XIII del Código número 577 Electoral para el Estado de Veracruz de Ignacio de la Llave; 34 numeral 1 incisos d), l), u) del Reglamento Interior del Organismo Público Local Electoral del estado de Veracruz; 33 numeral 1 incisos a), c), e) y q) del Reglamento en Materia de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Organización de Archivos del Organismo Público Local Electoral del Estado de Veracruz, la solicitud mencionada se turnó a:

Área	Número de oficio	Fecha
Dirección Ejecutiva de Administración	OPLEV/UTT/1791/2024	22/10/2024
Unidad técnica de Servicios Informáticos	OPLEV/UTT/1792/2024	22/10/2024

Respuesta a su solicitud:

En términos de los artículos 45 fracciones V y XII, 129 de la Ley General de Transparencia y Acceso a la Información Pública; 134 fracciones III y XII, 143, 145 y 148 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave; 34 numeral 1 inciso g), del Reglamento Interior del Organismo Público Local Electoral del estado de Veracruz; 16 y 17, 33 numeral 1 incisos f) y l) del Reglamento en Materia de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Organización de Archivos del Organismo Público Local Electoral del Estado de Veracruz, se acompañan al presente las siguientes documentales:

Número de oficio	Fecha	Emisor
OPLEV/DEA/1775/2024	08/11/2024	Director Ejecutivo de Administración
OPLEV/UTSI/562/2024	29/10/2024	Titular de la Unidad técnica de Servicios Informáticos

Ahora bien, con respecto de las preguntas 15, 17, 19, 21 22, 23 del Apartado 1; y las 32, 35, 39 y 42 del Apartado 2 de su solicitud de acceso a la información, en aras de garantizar el derecho humano de acceso a la información pública y de acuerdo a lo establecido en el artículo 45 de la Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, fue atendida también por la Unidad Técnica de Transparencia por lo que expreso lo siguiente:

APARTADO 2

PREGUNTA 32

Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente 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?;

> La respuesta es afirmativa
> El calendario de trabajo para la implementación del Sistema de Gestión de Protección de Datos Personales fue aprobado el 31 de enero de 2019, mediante acuerdo CT-ORD/OPLEV/07/2019, en el que participan todas las áreas administrativas de este sujeto obligado.

PREGUNTA 35

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;

> Conforme establece el artículo 28 de la Ley 316 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz, se realiza a través de la puesta a disposición de los avisos de privacidad disponibles por cada área administrativa para su consulta en https://www.oplever.org.mx/avisos-de-privacidad2/ lo cual se informa previo al tratamiento de datos personales.

PREGUNTA 39

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.

> De manera supletoria, con apego a lo establecido en el artículo 11, fracción III de la Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz, este sujeto obligado Proporciona capacitación continua y especializada al personal del Comité

de Transparencia, Unidades Técnica de Transparencia y áreas administrativas, en temas de transparencia, acceso a la información, rendición de cuentas, datos personales y archivos;
Capacitación anual en materia de datos personales, verificaciones físicas en materia de datos personales , políticas internas para la gestión y tratamiento de los datos personales https://www.oplever.org.mx/sitiotransparencia/art70/fracciones/39/A/2023/05.pdf

PREGUNTA 42

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

Conforme lo que señala el artículo 99 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz, este Sujeto Obligado ha adoptado diversas medidas administrativas, físicas y técnicas para el tratamiento de datos personales; realiza al menos de manera semestral, en cumplimiento al Programa Operativo Anual la revisión y actualización de los Sistemas de Datos Personales y notifica al Órgano Garante de manera anual, en apego al artículo 119, fracción VIII de la citada Ley, el cumplimiento de las obligaciones en materia de datos personales, disponible para su consulta en:

https://www.oplever.org.mx/sitiotransparencia/art70/fracciones/29/transparencia/2024/AnualDatos.pdf

Utilización de software test data como herramienta para la elaboración de versiones públicas, aprobado con el acuerdo CT-EXT/OPLEV/30/2021.

Verificaciones físicas en materia de datos personales http://www.oplever.org.mx/sitiotransparencia/art70/fracciones/39/2024/Res7.pdf

Capacitación anual en materia de datos personales , verificaciones físicas en materia de datos personales , políticas internas para la gestión y tratamiento de los datos personales https://www.oplever.org.mx/sitiotransparencia/art70/fracciones/39/A/2023/05.pdf

Políticas Internas para la gestión y el tratamiento de los datos personales

https://www.oplever.org.mx/wp-content/uploads/2023/Transparencia/Archivos/DatosPersonales/PoliticasInternas.pdf

Xalapa, Ver., 08 de noviembre de 2024

Oficio: OPLEV/UTT/1872/2024

Asunto: Respuesta a solicitud de acceso a la información.

Término para interposición del recurso de revisión:

En aras de promover, respetar, proteger y garantizar su derecho humano de acceso a la justicia se hace de su conocimiento que podrá interponer recurso de revisión ante Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales (IVAI) o ante esta Unidad Técnica de Transparencia, dentro del término de **15 días hábiles** siguientes a la fecha de notificación de la respuesta otorgada o del vencimiento del plazo para su notificación, conforme a lo previsto en los artículos 142 de la Ley General de Transparencia y Acceso a la Información Pública; 153, 155, 156 y 157 de la Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave.

Sin más por el momento, reciba un afectuoso saludo.

ATENTAMENTE

IXCHEL ALEJANDRA FLORES PÉREZ
TITULAR DE LA UNIDAD TÉCNICA DE TRANSPARENCIA

C.c.p. Archivo
IAFP/kpp/nnhu*

UNIDAD TÉCNICA DE TRANSPARENCIA
Xalapa–Equez., Ver., a 22 de octubre de 2024
Transmitimos valores para construir democracia
Oficio número: OPLEV/UTT/1791/2024
Asunto: Se envía solicitud de acceso a la información.

L.C. JOSÉ LAURO VILLA RIVAS
DIRECTOR EJECUTIVO DE ADMINISTRACIÓN
DEL ORGANISMO PÚBLICO LOCAL ELECTORAL DEL ESTADO DE VERACRUZ
P R E S E N T E.

Con fundamento en los artículos 132, 134 fracciones II y III y 145 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, por medio del presente me permito hacer de su conocimiento que se recibió la solicitud de acceso a la información que a continuación se detalla:

Folio de la solicitud	Solicitud
300564024000398	"… Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; …"

En caso que esa área a su cargo estime la actualización de los siguientes supuestos, se informa los plazos y términos para su comunicación a esta Unidad Técnica:

Supuesto	Plazo
Datos insuficientes o erróneos para atender la solicitud	Dos días hábiles[1]
Inexistencia de la información	Tres días hábiles
Ampliación del plazo para atender la solicitud	Seis días hábiles
Clasificación de la información	Seis días hábiles

Lo anterior, conforme al procedimiento establecido en el artículo 14 del Reglamento en Materia de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Organización de Archivos del Organismo Público Local Electoral del Estado de Veracruz, consultable a través de la siguiente dirección electrónica o el código QR:

https://goo.su/x7Zw

[1] Todos los plazos se computarán a partir de la recepción de la solicitud por parte del área.

Ahora bien, de contar con la información requerida deberá enviarse en un plazo no mayor a cinco días hábiles a fin de que ésta sea comunicada a la persona solicitante, por lo que agradeceré su colaboración institucional para el debido cumplimiento del término señalado.

En espera de su pronta respuesta, sirva el presente para saludarle cordialmente.

ATENTAMENTE

IXCHEL ALEJANDRA FLORES PÉREZ
TITULAR DE LA UNIDAD TÉCNICA DE TRANSPARENCIA

C.c.p. Archivo
IAFP/kpp/nnhu*

Gmail

Transparencia OPLEVER <oplevertransparencia@gmail.com>

TURNO SAI 300564024000398

1 mensaje

Transparencia OPLEVER <oplevertransparencia@gmail.com>
Para: DEA - 1 <deaoplev@gmail.com>

22 de octubre de 2024, 16:09

L.C. JOSÉ LAURO VILLA RIVAS

DIRECTOR EJECUTIVO DE ADMINISTRACIÓN

DEL ORGANISMO PÚBLICO LOCAL ELECTORAL DEL ESTADO DE VERACRUZ

P R E S E N T E.

Con fundamento en los artículos 132, 134 fracciones II y III y 145 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, por medio del presente me permito hacer de su conocimiento que se recibió la solicitud de acceso a la información que a continuación se detalla:

Folio de la solicitud	Solicitud
300564024000398	"... Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; ..."

En caso que esa área a su cargo estime la actualización de los siguientes supuestos, se informa los plazos y términos para su comunicación a esta Unidad Técnica:

Supuesto	Plazo
Datos insuficientes o erróneos para atender la solicitud	Dos días hábiles[1]
Inexistencia de la información	Tres días hábiles
Ampliación del plazo para atender la solicitud	Seis días hábiles
Clasificación de la información	Seis días hábiles

Lo anterior, conforme al procedimiento establecido en el artículo 14 del Reglamento en Materia de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Organización de Archivos del Organismo Público Local Electoral del Estado de Veracruz, consultable a través de la siguiente dirección electrónica o el código QR:

https://goo.su/x7Zw

Ahora bien, de contar con la información requerida deberá enviarse en un plazo no mayor a cinco días hábiles a fin de que ésta sea comunicada a la persona solicitante, por lo que agradeceré su colaboración institucional para el debido cumplimiento del término señalado.

En espera de su pronta respuesta, sirva el presente para saludarle cordialmente.

ATENTAMENTE

IXCHEL ALEJANDRA FLORES PÉREZ

TITULAR DE LA UNIDAD TÉCNICA DE TRANSPARENCIA

C.c.p. Archivo

IAFP/kpp/nnhu*

---

[1] Todos los plazos se computarán a partir de la recepción de la solicitud por parte del área.

Para tal efecto, me permito informarle a usted lo correspondiente, remitiendo el siguiente oficio adjunto al presente debidamente firmado de manera electrónica mediante Código de Integridad tipo HASH.

NOM. DE ARCHIVO	CÓDIGO DE INTEGRIDAD
TURNADOS\TURNO- DEA-SAI-398.pdf	5BFA6C03C8B436529003254F353DE2 EDEC1437C09A4525484829303E7C3D1883

TURNO- DEA-SAI-398.pdf
510K

UNIDAD TÉCNICA DE TRANSPARENCIA
Xalapa–Equez., Ver., a 22 de octubre de 2024
Transmitimos valores para construir democracia
Oficio número: OPLEV/UTT/1792/2024
Asunto: Se envía solicitud de acceso a la información.

ING. RAFAEL GONZÁLEZ ORTIZ
TITULAR DE LA UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS
DEL ORGANISMO PÚBLICO LOCAL ELECTORAL DEL ESTADO DE VERACRUZ
P R E S E N T E.

Con fundamento en los artículos 132, 134 fracciones II y III y 145 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, por medio del presente me permito hacer de su conocimiento que se recibió la solicitud de acceso a la información que a continuación se detalla:

Folio de la solicitud	Solicitud
300564024000398	"APARTADO 1 1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan; 2. Señalar sí se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar sí se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC. 3. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en

	cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ; 4. Informar sí se emplea la firma electrónica avanzada en la institución; 5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos; 6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros; 7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero; 8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas; 9. Informar sí se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información. 10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos; 11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes; 12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos; 13. Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información; 14. Informar sí dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó. 15. 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?; 16. 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; 17. 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; 18. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos; 19. 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. 20. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas; 21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son; 22. 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; 23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales; 24. Informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información; 25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;

	26. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad; 27. 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. 28. Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes. APARTADO 2 Solicito la siguiente información. 29. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan; 30. 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 ; 31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución; 32. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente 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?; 33. Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó; 34. 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; 35. 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; 36. Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan; 37. Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes; 38. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos; 39. 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. 40. Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas; 41. Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa; 42. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son; 43. 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 ey 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; 44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución; 45. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad; 46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este; 47. 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.

	48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo. APARTADO 3 49.Indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial. 50.En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia. 51.En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad , favor de indicar el sujeto obligado que pudiera contener dicha información. Me gustaría saber de qué manera aplican medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al momento de brindar servicios a la ciudadanía. En caso de que no, saber si se tienen proyectos para aplicar dicho tipo de tecnología. A su vez se pide conocer lo siguiente: 52.Qué programas, algoritmos, sistemas de inteligencia artificial, sistemas de decisiones judiciales asistidas, algoritmos o programas de selección aleatoria de casos a jueces, tiene y opera. 53.El número de registros existentes de lo solicitado en el punto anterior. a. Las fechas de operación. b. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta. c. Los contratos de su uso o adquisición. 54.¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas se selección y asignación aleatoria de casos? 55.¿Qué datos se utilizan para la selección y asignación aleatoria de casos? (sic)”

UNIDAD TÉCNICA DE TRANSPARENCIA
Xalapa–Equez., Ver., a 22 de octubre de 2024
Transmitimos valores para construir democracia
Oficio número: OPLEV/UTT/1792/2024
Asunto: Se envía solicitud de acceso a la información.

En caso que esa área a su cargo estime la actualización de los siguientes supuestos, se informa los plazos y términos para su comunicación a esta Unidad Técnica:

Supuesto	Plazo
Datos insuficientes o erróneos para atender la solicitud	Dos días hábiles[1]
Inexistencia de la información	Tres días hábiles
Ampliación del plazo para atender la solicitud	Seis días hábiles
Clasificación de la información	Seis días hábiles

Lo anterior, conforme al procedimiento establecido en el artículo 14 del Reglamento en Materia de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Organización de Archivos del Organismo Público Local Electoral del Estado de Veracruz, consultable a través de la siguiente dirección electrónica o el código QR:

https://goo.su/x7Zw

Ahora bien, de contar con la información requerida deberá enviarse en un plazo no mayor a cinco días hábiles a fin de que ésta sea comunicada a la persona solicitante, por lo que agradeceré su colaboración institucional para el debido cumplimiento del término señalado.

En espera de su pronta respuesta, sirva el presente para saludarle cordialmente.

ATENTAMENTE

IXCHEL ALEJANDRA FLORES PÉREZ
TITULAR DE LA UNIDAD TÉCNICA DE TRANSPARENCIA

C.c.p. Archivo
IAFP/kpp/nnhu*

[1] Todos los plazos se computarán a partir de la recepción de la solicitud por parte del área.

Gmail

Transparencia OPLEVER <oplevertransparencia@gmail.com>

TURNO SAI 300564024000398

1 mensaje

Transparencia OPLEVER <oplevertransparencia@gmail.com> 22 de octubre de 2024, 13:58
Para: UNIDAD TÉCNICA DE SERVICIOS INFORMATICOS <informatica@oplever.org.mx>

ING. RAFAEL GONZÁLEZ ORTIZ

TITULAR DE LA UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

DEL ORGANISMO PÚBLICO LOCAL ELECTORAL DEL ESTADO DE VERACRUZ

P R E S E N T E.

Con fundamento en los artículos 132, 134 fracciones II y III y 145 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, por medio del presente me permito hacer de su conocimiento que se recibió la solicitud de acceso a la información que a continuación se detalla:

Folio de la solicitud	Solicitud
300564024000398	"APARTADO 1 1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan; 2. Señalar sí se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar sí se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC. 3. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta

afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;

4. Informar sí se emplea la firma electrónica avanzada en la institución;

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

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

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

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

9. Informar sí se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información.

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

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

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

13. Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;

14. Informar sí dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó.

15. 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?;

16. 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;

17. 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;

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

19. 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.

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

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

22. 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;

23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales;

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

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

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

27. 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.

28. Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales

vigentes.

APARTADO 2

Solicito la siguiente información.

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

30. 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 ;

31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;

32. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente 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?;

33. Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;

34. 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;

35. 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;

36. Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;

37. Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;

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

39. 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.

40. Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;

41. Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;

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

43. 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 ey 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;

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

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

46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;

47. 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.

48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.

APARTADO 3

49.Indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial.

50.En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia.

51.En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad , favor de indicar el sujeto obligado que pudiera contener dicha información. Me gustaría saber de qué manera aplican medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al momento de brindar

	servicios a la ciudadanía. En caso de que no, saber si se tienen proyectos para aplicar dicho tipo de tecnología. A su vez se pide conocer lo siguiente: 52.Qué programas, algoritmos, sistemas de inteligencia artificial, sistemas de decisiones judiciales asistidas, algoritmos o programas de selección aleatoria de casos a jueces, tiene y opera. 53.El número de registros existentes de lo solicitado en el punto anterior. a. Las fechas de operación. b. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta. c. Los contratos de su uso o adquisición. 54.¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas se selección y asignación aleatoria de casos? 55.¿Qué datos se utilizan para la selección y asignación aleatoria de casos? (sic)"

En caso que esa área a su cargo estime la actualización de los siguientes supuestos, se informa los plazos y términos para su comunicación a esta Unidad Técnica:

Supuesto	Plazo
Datos insuficientes o erróneos para atender la solicitud	Dos días hábiles[1]
Inexistencia de la información	Tres días hábiles
Ampliación del plazo para atender la solicitud	Seis días hábiles
Clasificación de la información	Seis días hábiles

Lo anterior, conforme al procedimiento establecido en el artículo 14 del Reglamento en Materia de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Organización de Archivos del Organismo Público Local Electoral del Estado de Veracruz, consultable a través de la siguiente dirección electrónica o el código QR:

https://goo.su/x7Zw

Ahora bien, de contar con la información requerida deberá enviarse en un plazo no mayor a cinco días hábiles a fin de que ésta sea comunicada a la persona solicitante, por lo que agradeceré su colaboración institucional para el debido cumplimiento del término señalado.

En espera de su pronta respuesta, sirva el presente para saludarle cordialmente.

ATENTAMENTE

IXCHEL ALEJANDRA FLORES PÉREZ

TITULAR DE LA UNIDAD TÉCNICA DE TRANSPARENCIA

C.c.p. Archivo

IAFP/kpp/nnhu*

---

[1] Todos los plazos se computarán a partir de la recepción de la solicitud por parte del área.

Para tal efecto, me permito informarle a usted lo correspondiente, remitiendo el siguiente oficio adjunto al presente debidamente firmado de manera electrónica mediante Código de Integridad tipo HASH.

NOM. DE ARCHIVO	CÓDIGO DE INTEGRIDAD
TURNO-UTSI-SAI 398.pdf	B71406617299A94F0DC01A4128C68C 0A6F0C6A5DEB1AF88BB5AA2B198F61B056

TURNO-UTSI-SAI 398.pdf
2503K

F-1535

Unidad Técnica de Transparencia
OPLE Veracruz
RECIBIDO
Fecha_____ Hora_____

08-Nov-2024
13:50 hrs.

OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Proceso 2024 Electoral 2025
AYUNTAMIENTOS
Mi voto es mi voz

DIRECCIÓN EJECUTIVA DE ADMINISTRACIÓN

Xalapa, Veracruz, a 08 de noviembre de 2024
"Transmitimos valores para construir democracia".

Oficio: OPLEV/DEA/1775/2024

MTRA. IXCHEL ALEJANDRA FLORES PÉREZ
TITULAR DE LA UNIDAD TÉCNICA DE TRANSPARENCIA
P R E S E N T E .

En atención al oficio número **OPLEV/UTT/1791/2024** de fecha 22 de octubre del año en curso, a través del cual remite la solicitud de acceso a la información presentada en la Plataforma Nacional de Transparencia con número de folio **300564024000398**, en la cual requieren la siguiente información:

"...Informar sí se cuenta con un Inventario institucional de bienes y servicios de TIC..." *(sic).*

Al respecto, me permito hacer de su conocimiento que toda la información relativa al inventario de bienes muebles e inmuebles del OPLE Veracruz, que incluye altas y bajas, es pública y se encuentra disponible en el Portal de Obligaciones de Transparencia de este Organismo autónomo que puede consultar en la siguiente liga electrónica: https://www.oplever.org.mx/sitiotransparencia/portal_2024/index2024.php, donde podrá verificar el contenido de la fracción XXXIV. INVENTARIO DE BIENES MUEBLES E INMUEBLES (formatos A, B, C, D, E, F y G). Con la finalidad de facilitar su verificación, proporciono las siguientes direcciones electrónicas:

Formato A
https://docs.google.com/spreadsheets/d/14NVCsf5DEOD3vLMIVYsLSM9NaLIbo_zv/edit?gid=1532600106#gid=1532600106
Formato B
https://docs.google.com/spreadsheets/d/1E6O7OohVfFPdYJ4uQ8t4J7LzGm3tOqIk/edit?gid=204162731#gid=204162731
Formato C
https://docs.google.com/spreadsheets/d/1q6dNq5XfGqs7wTWfgNI4lIK7AFmRmNyG/edit?gid=114360586#gid=114360586
Formato D
https://docs.google.com/spreadsheets/d/1gOU8eB1OBAKlbEd1qxFn4OpIZ9BBtogA/edit?gid=65618128#gid=65618128
Formato E
https://docs.google.com/spreadsheets/d/15X2AH_rl8m1P8AXfTsqLdxUJ_7ryopBz/edit?gid=1256353588#gid=1256353588
Formato F
https://docs.google.com/spreadsheets/d/1CeQSdbIuSzEyNEuiT-vT98YQFCnoobM3/edit?gid=286999690#gid=286999690
Formato G
https://docs.google.com/spreadsheets/d/1Vvm-1vPRcRS5SXZ6gSVy9dt2O9JPlJ-W/edit?gid=1510027388#gid=1510027388

DIRECCIÓN EJECUTIVA DE ADMINISTRACIÓN

Xalapa, Veracruz, a 08 de noviembre de 2024
"Transmitimos valores para construir democracia".

Finalmente, y en aras de garantizar el acceso a la información, se proporcionan las referidas direcciones electrónicas en formato Word, mismas que respetuosamente solicito a esa Unidad Técnica de Transparencia, le sean enviadas a la parte solicitante para garantizar la consulta correspondiente.

Sin otro particular, y en espera de haber atendido su solicitud en tiempo y forma, quedo a sus órdenes para cualquier aclaración y aprovecho la ocasión para enviarle un cordial saludo.

ATENTAMENTE

L.C. José Lauro Villa Rivas
Director Ejecutivo de Administración

C.c.p. **Lic. Amara Anaya García**, Subdirectora Administrativa. Para su conocimiento.
Archivo.

F-1502

29-oct-2024
10:22 hrs.

Unidad Técnica de Transparencia
RECIBIDO
Fecha _____ Hora _____

Unidad Técnica de Servicios Informáticos

Xalapa, Veracruz; 29 de octubre de 2024
Transmitimos valores para construir democracia

OPLEV/UTSI/562/2024

Asunto: Respuesta a solicitud **300564024000398**

Mtra. Ixchel Alejandra Flores Pérez
Titular de la Unidad Técnica de
Transparencia del OPLE Veracruz
P r e s e n t e

Con fundamento en los artículos 6 y 14 del Reglamento en Materia de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Organización de Archivos de este Organismo Público Local Electoral del Estado de Veracruz, y en atención a su oficio número **OPLEV/UTT/1792/2024**, mediante el cual se comunica la presentación de la solicitud de información **300564024000398**, me permito hacer de su conocimiento lo siguiente:

Solicitud	Atención
1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;	**Después de una búsqueda exhaustiva y razonable no se cuenta en los archivos de esta Unidad Técnica** con documentación relacionada con "gobierno de seguridad de la información o ciberseguridad".
2. Señalar sí se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;	**a) Después de una búsqueda exhaustiva y razonable no se cuenta en los archivos de esta Unidad Técnica** con documentación de procesos de contratación y adquisición en materia de TIC´s y de seguridad de la información. **Después de una búsqueda exhaustiva y razonable no se cuenta en los archivos de esta Unidad Técnica** con documentación de levantamiento de inventarios institucionales. c) Sí, se cuenta con Planes de Continuidad para Sistemas informáticos específicos: - Programa de Resultados Electorales Preliminares 2024, 2022, 2021, 2018, 2016; - Candaditas y Candidatos, Conóceles 2024; - Sistema Integral de Cómputos Distritales 2024; - Sistema de Seguimiento de Paquetes 2024; y - Sistema de Registro de Candidaturas Locales 2024. d) Sí, se cuenta dentro de los Planes de Continuidad para Sistemas informáticos específicos: - Programa de Resultados Electorales Preliminares 2024, 2022, 2021, 2018, 2016; - Candaditas y Candidatos, Conóceles 2024; - Sistema Integral de Cómputos Distritales 2024; - Sistema de Seguimiento de Paquetes 2024; y

Solicitud	Atención
	- Sistema de Registro de Candidaturas Locales 2024.
e) desarrollado e implementado un programa de gestión de vulnerabilidades;	e) Sí, se cuenta dentro de los Planes de Continuidad y, en su caso, Plan de Seguridad para Sistemas informáticos específicos: - Programa de Resultados Electorales Preliminares 2024, 2022, 2021, 2018, 2016; - Candaditas y Candidatos, Conóceles 2024; - Sistema Integral de Cómputos Distritales 2024; - Sistema de Seguimiento de Paquetes 2024; y - Sistema de Registro de Candidaturas Locales 2024.
f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI);	f) **Después de una búsqueda exhaustiva y razonable no se cuenta en los archivos de esta Unidad Técnica** con documentación relativa a MGSI o SGSI.
g) Informar sí se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó;	g) **Después de una búsqueda exhaustiva y razonable no se cuenta en los archivos de esta Unidad Técnica** con documentación relativa a políticas generales citadas.
h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;	h) Sí, se cuenta dentro de los Planes de Continuidad y, en su caso, Plan de Seguridad para Sistemas informáticos específicos: - Programa de Resultados Electorales Preliminares 2024, 2022, 2021, 2018, 2016; - Sistema Candaditas y Candidatos, Conóceles 2024; - Sistema Integral de Cómputos Distritales 2024; - Sistema de Seguimiento de Paquetes 2024; y - Sistema de Registro de Candidaturas Locales 2024.
i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.	i) **Después de una búsqueda exhaustiva y razonable no se cuenta en los archivos de esta Unidad Técnica** con documentación relativa a equipos de respuesta mencionados.
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;	**Después de una búsqueda exhaustiva y razonable no se cuenta en los archivos de esta Unidad Técnica** con documentación denominada Estrategia de ciberseguridad.
4. Informar sí se emplea la firma electrónica avanzada en la institución;	**4. Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa al uso de la firma electrónica avanzada.

Solicitud	Atención
5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;	5. Sí, con motivo de la implementación de los siguientes sistemas: - Programa de Resultados Electorales Preliminares; - Sistema Candaditas y Candidatos, Conóceles; - Sistema Integral de Cómputos Distritales; - Sistema de Seguimiento de Paquetes; y - Sistema de Registro de Candidaturas Locales.
6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;	6. Acuerdo **OPLEV/CG029/2023**, por el que se aprueba el "manual para la realización del proceso técnico operativo de sistemas informáticos". Acuerdo **OPLEV/CG218/2023**, por el que se aprueba la guía para la generación de planes de continuidad y seguridad de los sistemas informáticos del Organismo Público Local Electoral del Estado de Veracruz.
7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;	7. Actualmente se utilizan servidores propios.
8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;	**8. Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa a los citados Lineamientos.
9· Informar sí se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información.	9. Sí se cuenta con correo electrónico institucional. a) **Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con dicha información. c) **Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con dicha información. d) Sí se cuenta con soluciones integradas al correo institucional de Anti-Virus y Anti-Spam. e) **Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con dicha información.
10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;	**10. Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;	11. a) Sí. b) Sí.
12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;	**12. Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa a capacitación impartida en la

Solicitud	Atención
	implementación del "Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos".
13. Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;	13. **a) y b) Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa a mecanismos supervisión, evolución y/o indicadores de seguridad de la información.
14. Informar sí dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
15. 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?;	En esta Unidad se cuenta con el "Sistemas de datos personales de personas físicas que deseen formar parte del Comité Técnico Asesor del Programa de Resultados Electorales Preliminares", mismo que fue aprobada mediante Acuerdo CT-EXP/OPLEV/159/2024 del Comité de Transparencia, el 7 de agosto de 2024.
16. 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;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
17. 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;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
18. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
19. 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.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
20. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.

Solicitud	Atención
22. 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;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
24. Informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
26. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;	Sí, al Programa de Resultados Electorales Preliminares y se realiza con motivo de cada proceso electoral local.
27. 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.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
28. Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
APARTADO 2 Solicito la siguiente información. 29. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
30. 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 ;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
32. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente Un sistema de gestión de protección de datos personales,	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.

Solicitud	Atención
en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;	
33· Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;	Sí, se cuenta con los Planes de Continuidad y, en su caso, los Planes de Seguridad para Sistemas informáticos específicos: - Programa de Resultados Electorales Preliminares; - Sistema Candaditas y Candidatos, Conóceles; - Sistema Integral de Cómputos Distritales; - Sistema de Seguimiento de Paquetes; y - Sistema de Registro de Candidaturas Locales.
34· 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;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
35· 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;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
36. Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;	Mediante circular SE/86/2023/OPLE, se invitó a la capacitación en "Ciberseguridad y Prevención de Delitos y Fraudes Cibernéticos", impartida por la Unidad de Policía Científica Preventiva del Estado de Veracruz, misma que se llevó a cabo el 9 de octubre de 2023.
37. Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;	Sí, se cuenta con los Planes de Continuidad y, en su caso, los Planes de Seguridad para Sistemas informáticos específicos: - Programa de Resultados Electorales Preliminares; - Sistema Candaditas y Candidatos, Conóceles; - Sistema Integral de Cómputos Distritales; - Sistema de Seguimiento de Paquetes; y - Sistema de Registro de Candidaturas Locales.
38. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
39· 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.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.

Solicitud	Atención
40. Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
41. Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
42. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
43· 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;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
45. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;	Sí, al Programa de Resultados Electorales Preliminares y se realiza con motivo de cada proceso electoral local.
46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;	Para el caso de sistemas informáticos se cuenta con los Planes de Continuidad y, en su caso, con los Planes de Seguridad para Sistemas informáticos específicos: - Programa de Resultados Electorales Preliminares; - Sistema Candaditas y Candidatos, Conóceles; - Sistema Integral de Cómputos Distritales; - Sistema de Seguimiento de Paquetes; y - Sistema de Registro de Candidaturas Locales.
47· 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.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
APARTADO 3 49. Indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.

Solicitud	Atención
50. En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
51. En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad, favor de indicar el sujeto obligado que pudiera contener dicha información. Me gustaría saber de qué manera aplican medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al momento de brindar servicios a la ciudadanía. En caso de que no, saber si se tienen proyectos para aplicar dicho tipo de tecnología. A su vez se pide conocer lo siguiente:	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
52. Qué programas, algoritmos, sistemas de inteligencia artificial, sistemas de decisiones judiciales asistidas, algoritmos o programas de selección aleatoria de casos a jueces, tiene y opera.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
53. El número de registros existentes de lo solicitado en el punto anterior. a. Las fechas de operación. b. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta. c. Los contratos de su uso o adquisición.	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
54. ¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas se selección y asignación aleatoria de casos?	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.
55. ¿Qué datos se utilizan para la selección y asignación aleatoria de casos? (sic)"	**Después de una búsqueda exhaustiva y razonable no se cuenta** en los archivos de esta Unidad Técnica con documentación relativa.

Sin otro particular, reciban un cordial saludo.

Atentamente

Ing. Rafael González Ortiz
Titular de la Unidad Técnica de Servicios Informáticos

C.c.p-. Archivo.

UNIDAD TÉCNICA DE TRANSPARENCIA
Xalapa–Equez., Ver. a 08 de noviembre de 2024
Transmitimos valores para construir democracia

Asunto: Se remite enlaces electrónicos

Estimado Solicitante
P R E S E N T E.

Con motivo a la solicitud de acceso a la información **300564024000398** se envía en formato PDF los enlaces electrónicos activos y verificados, los cuales son señalados en el oficio **OPLEV/DEA/1775/2024**.

Los siguientes links podrá abrirlos seleccionándolos y copiándolos uno por uno en algún navegador u oprimir en su teclado la tecla control y sin dejar de oprimir clic con el botón izquierdo del mouse:

PORTAL DE TRANSPARENCIA

https://www.oplever.org.mx/sitiotransparencia/portal_2024/index2024.php

Formato A

https://docs.google.com/spreadsheets/d/14NVCsf5DEOD3vLMIVYsLSM9NaLIbo_zv/edit?gid=1532600106#gid=1532600106

Formato B

https://docs.google.com/spreadsheets/d/1E6O7OohVfFPdYJ4uQ8t4J7LzGm3tOqIk/edit?gid=204162731#gid=204162731

Formato C

https://docs.google.com/spreadsheets/d/1q6dNq5XfGqs7wTWfgNI4lIK7AFmRmNyG/edit?gid=114360586#gid=114360586

UNIDAD TÉCNICA DE TRANSPARENCIA
Xalapa–Equez., Ver. a 08 de noviembre de 2024
Transmitimos valores para construir democracia

Asunto: Se remite enlaces electrónicos

Formato D

https://docs.google.com/spreadsheets/d/1gOU8eB1OBAKlbEd1qxFn4OpIZ9BBtogA/edit?gid=65618128#gid=65618128

Formato E

https://docs.google.com/spreadsheets/d/15X2AH_rl8m1P8AXfTsqLdxUJ_7ryopBz/edit?gid=1256353588#gid=1256353588

Formato F

https://docs.google.com/spreadsheets/d/1CeQSdbIuSzEyNEuiT-vT98YQFCnoobM3/edit?gid=286999690#gid=286999690

Formato G

https://docs.google.com/spreadsheets/d/1Vvm-1vPRcRS5SXZ6gSVy9dt2O9JPlJ-W/edit?gid=1510027388#gid=1510027388