

Dependencia	PRESIDENCIA MUNICIPAL
Sección	SECRETARIA PARTICULAR
Número de oficio	SP-XXV-224-2024
Expediente	FOLIO SIDOM: 037744/2024
Asunto	SOLICITUD DE ACCESO A LA INFORMACION

Tijuana, Baja California, a 15 de noviembre de 2024

LIC. JUAN DÁMASO IBARRA BRIEESCA
DIRECTOR GENERAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN
Y PROTECCIÓN DE DATOS PERSONALES DE PRESIDENCIA MUNICIPAL
H. XXV AYUNTAMIENTO DE TIJUANA BAJA CALIFORNIA

PRESENTE.-

Anteponiendo un cordial y atento saludo, por medio del presente con fundamento en los artículos 6 y 38 del reglamento interno de la Presidencia de Tijuana Baja California municipal y en atención a la notificación del Folio: **020059024001060** con fecha del 30 de octubre de 2024. **Descripción de la solicitud:** Atender de acuerdo con sus facultades y atribuciones

- 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 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 autoridad correspondiente;

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 ADICIONALES

- 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 (LGPDPSO);
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 (LGPDPSO);
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;

Datos adicionales para localizar la información: 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)

La cual fue Turnada al secretario particular de Presidencia Municipal del XXV ayuntamiento de Tijuana, mediante oficio con número DGT-XXV-0401/2024 en fecha 11 de noviembre de 2024, procedente de la Dirección de Transparencia y Acceso a la Información Pública.

De acuerdo al seguimiento de la solicitud de los folios antes mencionados da contestación después de una búsqueda exhaustiva en los archivos físicos y digitales, en la manera cronológica a los cuestionamientos formulados (tal y como aparecen en la solicitud que se atiende), insertando la respuesta con el numeral e/o inciso correspondiente la oficina de la Dirección de Tecnologías de la Información del XXV Ayuntamiento de Tijuana. Correspondiente como lo indica el Artículo 33 y 35 del reglamento interno de la Presidencia Municipal.

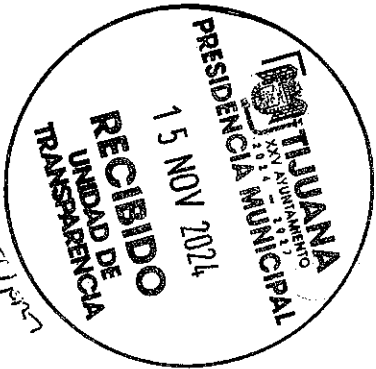
- 1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o de ciberseguridad y cuáles áreas participan: **No se cuenta con lo solicitado.**
- Señalar sí se han implementado las siguientes medidas: a) estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios de seguridad de la información o de tecnologías de la información y comunicación; b) mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGS/); 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); **No se cuenta con lo solicitado en los incisos de referencia.**
- Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia: **No se cuenta con estrategia de ciberseguridad.**
- Informar sí se emplea la firma electrónica avanzada en la institución: **No se emplea.**
- Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos: **No se realizan simulacros.**
- Señalar sí en la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información, de ha contado con el Dictamen Técnico favorable expedido por la autoridad correspondiente: **No se ha contado con el dictamen.**
- Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero: **Sí, son propios.**

- Informar sí se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información: **Sí se cuenta con correo electrónico, a) No cuenta con la leyenda de confidencialidad, b) Sí se cuenta, c) Sí se cuenta, d) Sí se cuenta, y e) Sí se cuenta.**
- Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos: **No se cuenta con los mecanismos señalados.**
- Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes: **a) No se cuenta con aviso de privacidad en el portal, b) sí cuenta con certificado vigente.**
- DATOS ADICIONALES
- Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos: No.
- 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: **No se cuentan con los mecanismos e indicadores señalados en los incisos.**
- 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 y cuántas horas de capacitación en ciberseguridad se realizan de forma anual: **No se cuenta con el programa de cultura de la seguridad de la información.**
- 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?: **En la Dirección de Tecnologías de la Información no se cuenta con un sistema de gestión de datos personales.**
- Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan e informar desde cuándo se implementó, lo anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPSO): **No se cuenta con un modelo o sistema.**

- Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó, o anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPSO): **No se cuenta con un modelo o sistema.**
- Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos: **No se cuenta con lo solicitado.**
- 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: **El personal de la Dirección de Tecnologías de la Información no cuenta con conocimientos que puedan ser comprobados en las materias a que refiere en los incisos.**
- Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas: **No se han registrado brechas de ciberseguridad.**
- Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son: **No se ha adoptado un esquema.**
- 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 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: **No se han llevado a cabo las referidas evaluaciones.**
- Informas sí se cuenta con documento de seguridad en materia de protección de datos personales; Datos adicionales para localizar la información: seguridad de la información: **No se cuenta con documento de seguridad en materia de protección de datos personales.**
- 24. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución: **No realizan actualizaciones en materia de ciberseguridad.**
- 25. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad: **No se llevan a cabo auditorías periódicas, sin embargo obra en los archivos de la Dirección de Tecnologías de la Información una auditoría externa en el año 2019.**
- 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: **Sí se cuenta con un help desk interno por cada uno de los departamentos de la Dirección de Tecnologías de la Información, los cuales son Soporte, Sistemas y Redes.**

- 27. Informar sí se cuenta con un Centro de Operaciones de Ciberseguridad Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles): No se cuenta con un Centro de Operaciones de Ciberseguridad.

Sin otro particular por el momento y agradeciendo su atención, me despido reiterándome a sus órdenes.



13:54 hrs

Lic. Iván Olivas Heredia
Secretario Particular de Presidencia Municipal
Del H. XXV Ayuntamiento de Tijuana, Baja California

C. e. p. Archivo

Atentamente