



**UNIDAD DE TRANSPARENCIA
COORDINACIÓN DE TRANSPARENCIA
Oficio No. UT/2569/2024
Asunto: Oficio de Respuesta**

Ciudad de México, 12 de noviembre de 2024

SOLICITANTE DEL FOLIO 330029524000825

P R E S E N T E.

De conformidad con el Artículo 6, inciso A, fracción I de la Constitución Política de los Estados Unidos Mexicanos, así como los artículos 45, fracción II de la Ley General de Transparencia y Acceso a la Información Pública y 61, fracción IV de la Ley Federal de Transparencia y Acceso a la Información Pública, se recibió la solicitud de acceso a la información con número de folio **330029524000825**, a través de la Plataforma Nacional de Transparencia, el pasado veintiuno de octubre, mediante la cual se requiere lo siguiente:

{...} SECCION 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 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 se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;

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

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

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

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

12. Informar si 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 la madurez institucional en la gestión de seguridad de la información;

14. 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.

Otros datos para su localización:

15. 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?;

16. 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;

17. 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;

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

19. 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.

Otros datos para su localización:

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

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

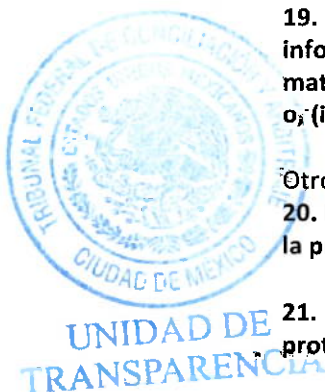
22. Informar si algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar si se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;

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

24. Informar si 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 si 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 si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.

SECCION 2

Solicito la siguiente información.

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

30. 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;

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

32. Informar si 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? (...) "(Sic).

Modalidad preferente de entrega: Electrónico a través del Sistema de Solicitudes de Acceso a la Información de la PNT

La DIRECCIÓN DE INFORMÁTICA JURÍDICA de este Tribunal Federal de Conciliación y Arbitraje, Informa que, con fundamento en el artículo 123 de la Ley Federal de los Trabajadores al Servicio del Estado, Reglamentaria del apartado B) del artículo 123 Constitucional publicada en el Diario Oficial de la Federación el 28 de diciembre de 1963, señala en su párrafo segundo lo siguiente:

(...) Artículo 123...

Los gastos que origine el funcionamiento del Tribunal serán cubiertos por el Estado, consignándose en el presupuesto de la Secretaría de Gobernación"



Por lo anterior, la Dirección de Informática Jurídica no está en posibilidades de proporcionar la información requerida, ya que dicha información la integra, controla e informa la Dirección General de Tecnologías de la Información y comunicaciones (DGTIC), de la Secretaría de Gobernación (SEGOB)

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



hazarmaveth

