PODER JUDICIAL

RESOLUCIÓN RELATIVA A LA SOLICITUD DE AMPLIACIÓN DEL PLAZO DE RESPUESTA DE LA SOLICITUD FOLIO: 210425322000380

Resolución del Comité de Transparencia del Poder Judicial del Estado de Puebla, correspondiente al punto Segundo del Orden del Día de la Décima Tercera Sesión Ordinaria, celebrada el día cuatro de julio de dos mil veintidós. ----------

---

---------- **ANTECEDENTES** ----------

I. Con fecha veinte de mayo de dos mil veintidós, fue presentada la solicitud de Acceso a la Información, registrada con el número de folio **210425322000380,** que a la letra señala: "*Solicito la siguiente información 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 seguirdad 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." ----------

---

II. Con fecha siete de junio del presente año, mediante oficio número UTPJ/0634/2022, se solicitó a la Dirección de Informática, informe lo conducente. ----------

---

---------- **CONSIDERANDO** ----------

Competencia: El Comité de Transparencia del Poder Judicial del Estado de Puebla es competente para conocer y resolver el presente asunto, en términos de lo dispuesto en el artículo 22 fracción II de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla.----------

Materia de la prórroga: Conforme al artículo 150 párrafo segundo de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla, que establece que excepcionalmente, el plazo de veinte días hábiles para dar respuesta a una solicitud de información podrá ampliarse hasta por diez días hábiles más, siempre y cuando existan razones fundadas y motivadas, lo que se actualiza por el volumen de la información solicitada.----------

En el caso concreto, la prórroga solicitada refiere a compilar y revisar los datos que fueron remitidos a la Unidad de Transparencia, por lo que es necesaria la prórroga, para otorgar una respuesta completa.----------

Por lo anterior, este Comité de Transparencia determina que la Unidad Administrativa de referencia, conforme a sus atribuciones se encuentra en el proceso de compilación de información, con la finalidad que pueda entregarse una respuesta correcta y completa al solicitante, y es necesario la ampliación del plazo de respuesta. ----------

Por las consideraciones de hecho y de derecho previamente establecidas, este Comité resuelve: -------

PRIMERO: CONFIRMAR LA PRÓRROGA por diez días hábiles más, para dar respuesta **a** la solicitud de Acceso a la Información con número de folio **210425322000380** en términos de lo dispuesto en los artículos 22 fracción II y 150 párrafo segundo de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla.----------

SEGUNDO: Se instruye a la Titular de la Unidad de Transparencia, para que notifique la presente resolución al solicitante.----------

Así, por unanimidad de votos lo resolvieron los integrantes del Comité de Transparencia del Poder Judicial del Estado de Puebla. ----------

LIC. RAFAEL PÉREZ XILOTL
PRESIDENTE DEL COMITÉ DE TRANSPARENCIA
DEL PODER JUDICIAL DEL ESTADO DE PUEBLA

LIC. CAROLINA TULES ZENTENO HERRERA
INTEGRANTE DEL COMITÉ DE TRANSPARENCIA
DEL PODER JUDICIAL DEL ESTADO DE PUEBLA

LIC. ERASMO PEDRAZA CASTILLO
INTEGRANTE DEL COMITÉ DE TRANSPARENCIA
DEL PODER JUDICIAL DEL ESTADO DE PUEBLA

TERCERA SESIÓN ORDINARIA, CELEBRADA EL DÍA CUATRO DEJULIO DE DOS MIL VEINTIDÓS.LA PRESENTE HOJA DE FIRMAS CORRESPONDE A LA RESOLUCIÓN DERIVADA DEL PUNTO SEGUNDO DEL ORDEN DEL DÍA DE LA DÉCIMA