

Sección: Unidad Técnica de Transparencia y
Acceso a la Información

Expediente: IEPC/UTTAI/2024

Número: 419/2024

Asunto: Respuesta

Chilpancingo de los Bravo, Gro., 04 de noviembre de 2024.

**A QUIEN CORRESPONDA
PRESENTE. -**

Con fundamento en los artículos 54 fracción I) inciso a), fracción II) inciso a) y 150 párrafo primero de la Ley Número 207 de Transparencia y Acceso a la Información Pública del Estado de Guerrero, me refiero a su atenta solicitud, recibida a través de la Plataforma Nacional de Transparencia, identificada con el número de folio **120310824000169**, mediante la cual requiere la siguiente información:

"1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan; 2. Señalar si 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 si se cuenta con un 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) o Sistema de Gestión de Seguridad de la Información (SGSI); 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) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC. 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 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 el 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".

Derivado de lo anterior, me permito adjuntar al presente, respuesta proporcionada por la Dirección General de Informática de este Instituto, quien a través del oficio 514, atiende a cada una de las preguntas planteadas.

Nos remitimos a sus órdenes en caso de dudas o comentarios, a través del correo electrónico: transparencia@iepcgro.mx y/o del teléfono de oficina: 7474712144.



IEPC
GUERRERO
UNIDAD TÉCNICA DE
TRANSPARENCIA Y
ACCESO A LA
INFORMACIÓN
CHILPANCIINGO, GRO.

ATENTAMENTE



C. MARTHA PATRICIA CERDENARES MORALES
JEFA DE LA UNIDAD TÉCNICA

c. c. p.- Mtro. Pedro Pablo Martínez Ortiz.- Secretario Ejecutivo del IEPC Guerrero. Para su conocimiento.
Archivo