



Número de Oficio 047/2024.  
Asunto: El que se indica.

## A QUIEN CORRESPONDA

Chilpancingo, Guerrero a 08 de noviembre de 2024.

Con fundamento en lo dispuesto por el artículo 150 de la Ley número 207 de Transparencia y Acceso a la Información del Estado de Guerrero, este órgano autónomo emite contestación a su solicitud de información con número de folio **121175424000042**, en los términos siguientes:

Se le hace de su conocimiento que, en contra de la presente respuesta a su solicitud procede el recurso de revisión, mismo que deberá interponerse dentro de los quince días siguientes al en que le notifique la respuesta ante el ITAIGro o ante esta Unidad de Transparencia.

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

**R. No se cuenta con un gobierno de seguridad de la información o de ciberseguridad.**

2. Señalar sí de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021, 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.

**R. No se cuenta con estándares técnicos definidos por la Coordinación de Estrategia Nacional.**

- 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;

**R. No se cuenta con un marco de mejores prácticas aplicables a la gestión de las TIC's.**





- c) Informar sí se cuenta con un Inventario Institucional de bienes y servicios de TIC; un plan de continuidad de operaciones, y señalar la fecha de implementación;  
**R. No se cuenta con un Inventario Institucional de bienes y servicios de TIC.**
- d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;  
**R. No se ha desarrollado ni implementado el plan de recuperación ante desastres.**
- e) Desarrollado e implementado un programa de gestión de vulnerabilidades;  
**R. No se ha desarrollado un programa de gestión de vulnerabilidades.**
- f) Marco de Gestión de Seguridad de la Información (MGSI);  
**R. No se cuenta con el MGSI.**
- 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;  
**R. No se cuenta con una política de seguridad de la información.**
- h) Informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;  
**R. No se cuenta con un diagnóstico de identificación de los procesos y activos esenciales.**
- i) Informar si se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC).  
**R. No se cuenta con ERISC.**
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.  
**R. No se cuenta con una estrategia de ciberseguridad dentro de la Institución.**





4. Informar sí se emplea la firma electrónica avanzada en la institución;  
**R. No se emplea la firma electrónica avanzada.**
5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;  
**R. No se realizan simulacros sobre el plan de recuperación de desastres o incidentes cibernéticos.**
6. 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 CEDN, de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021.  
**R. No se tiene la contratación de servicios de seguridad de la información en Tecnologías, Comunicación y Seguridad de la Información.**
7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;  
**R. No contamos con centro de datos.**
8. 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:  
**R. Si se cuenta con correo electrónico Institucional.**
  - a) inserción de leyenda de confidencialidad de la información;  
**R. No se ha implementado.**
  - b) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;  
**R. Si se tiene a través de la aplicación web CPANEL.**
  - c) 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;  
**R. No se cuenta con soluciones de filtrado ni programas informáticos que protejan del envío y recepción de correos electrónicos.**
  - d) cuenta con cifrado en el envío de información.  
**R. No se cuenta con cifrado 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;

**R. El servidor Público, no está autorizado para la divulgación no autorizada de datos o información Institucional, ya que al hacerlo, incurre en una responsabilidad administrativa grave y será sancionado.**

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

**R. La página web, sí cuenta con aviso de privacidad y certificados digitales vigentes.**

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

**R. No se ha capacitado al personal 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 la madurez institucional en la gestión de seguridad de la información;

**R. No se cuenta con los mecanismos de supervisión y evaluación para la efectividad de los controles de seguridad de la información, ni con indicadores que permitan medir la madurez institucional.**

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.

**R. Un programa como tal, no, simplemente se van dando recomendaciones a los compañeros.**

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?;

**R. No se cuenta con un Sistema de Gestión de Protección de Datos Personales.**





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 los artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPO);

**R. No 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.**

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 los artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPO);

**R. No se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad.**

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

**R. No se cuenta con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución.**

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.

**R. Si se cuenta con el conocimiento. Pero no contamos con la infraestructura para poder llevar a cabo todos los mecanismos de seguridad.**

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

**R. No se han tenido brechas de ciberseguridad.**

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

**R. No se han adoptado esquemas de mejoras prácticas en materia de protección de datos personales.**





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;

**R. Sí, los sistemas que se han desarrollado dentro de la Institución manejan políticas y avisos de privacidad.**

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

**R. No se cuenta con documentos de seguridad en materia de protección de datos personales.**

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

**R. No se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información.**

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

**R. No se llevan a cabo actualizaciones de medidas de ciberseguridad dentro de la institución, ya que no se manejan.**

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

**R. No se han llevado a cabo auditorías de seguridad externas ni internas en materia de ciberseguridad.**

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

**R. No se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos**





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)

**R. No se cuenta con un Centro de Operaciones de Ciberseguridad y por el momento no hemos presentado incidentes.**

Se le hace de su conocimiento que, en contra de la presente respuesta a su solicitud procede el recurso de revisión, mismo que deberá interponerse dentro de los quince días siguientes al en que le notifique la respuesta ante el ITAIGro o ante esta Unidad de Transparencia.

ATENTAMENTE



DIRECCIÓN DE  
TECNOLOGÍAS

Ing. Nora Edna Cuenca Marino  
Directora de Tecnologías de la Información.

