ichitaip
INSTITUTO CHIHUAHUENSE PARA LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

RECIBIDO
07 NOV 2024
15:35 hrs
INSTITUTO CHIHUAHUENSE PARA LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA
UNIDAD DE TRANSPARENCIA

Dirección / Área: Subcoordinación de Sistemas
No. de oficio: ICHITAIP/DS-7341/2024
Asunto: Respuesta a solicitud 080159224000274

Chihuahua, Chih., 7 de Noviembre de 2024

Lic. Diana Carolina Solís García
Jefa del Departamento de Sistema de Información Pública
Presente:

En atención a su correo electrónico enviado el 29 de Octubre de 2024, respecto a la Solicitud de Acceso a la Información folio **080159224000274**, mediante la cual requiere a esta Subcoordinación de Sistemas y Tecnologías de Información lo siguiente:

Descripción de la información solicitada:

"...

PREGUNTAS

APARTADO 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*

Av. Teófilo Borunda No. 2009
Col. Arquitos, C.P. 31205 Chihuahua, Chih., México ichitaip.org.mx
Conmutador: (614) 201 33 00 01 800 300 2552

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 seguridad 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.*

…"(Sic)

Respuestas

APARTADO 1

1. *Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;*
   R: No se cuenta

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;*
   b. *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.*

   R: No se cuenta

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

4. *Informar sí se emplea la firma electrónica avanzada en la institución;*
   R: No se emplea

5. *Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;*

R: No se realizan simulacros

6. *Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;*
   R: No se cuenta

7. *Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;*
   R: Centro de datos locales, servidor y almacenamiento local
8. *Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas*
   R: No se cuenta

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:*
   R: Si se cuenta con correo institucional
   a. *inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información;*
      R: Si se incluye leyenda
   b. *control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;*
      R: No se llega control institucional
   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: Se lleva un control Anti SPAM por parte del motor de correo
   d. *cuenta con cifrado en el envío de información.*
      R: El cifrado es realizado por el motor de correo

10. *Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;*
    R: No se cuenta con un método formal

11. *Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;*
    R: Si se cuenta con lo preguntado

12. *Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;*
    R: No se cuenta con dicha capacitación

13. *Informar si se cuentan con:*

Av. Teófilo Borunda No. 2009
Col. Arquitos, C.P. 31205 Chihuahua, Chih., México ichitaip.org.mx
Conmutador: (614) 201 33 00 01 800 300 2552

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;*

R: No se cuenta con estos mecanismos

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.*
R: No se cuenta

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?;*
R: No se cuenta

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;*
R: Se hacen uso de redes sociales, página web y comunicación directa con sujetos obligados para informar en caso de alguna incidencia por reportar. Intervienen las áreas de Comunicación Social y Sistemas. Se ha implementado a partir de la creación del instituto.

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;*
R: No se cuenta

18. *Informar sí 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

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.*
R: Si se cuentan con conocimientos de las áreas mencionadas

20. *Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;*
R: No se han identificado brechas de seguridad

21. *Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;*
R: No se cuenta

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;*
R: No se emplea

23. *Informas sí se cuenta con documento de seguridad en materia de protección de datos personales;*
R: Si se cuenta

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

25. *Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;*
R: Si bien no es una tarea definida, ni automatizada, se realizan revisiones de forma semanal de las actualizaciones disponibles para los equipos de acceso a la red y servidores internos. Con lo cual se aplican las actualizaciones disponibles a esos equipos cada semana.

26. *Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;*
R: No se realizan

27. *Señalar si se cuenta con un helpdesk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.*
R: No se cuenta con Help Desk, se atienden las solicitudes de forma directa.

Av. Teófilo Borunda No. 2009
Col. Arquitos, C.P. 31205
Chihuahua, Chih., México
ichitaip.org.mx
Conmutador: (614) 201 33 00
01 800 300 2552

28. *Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.*
R: El sitio web cuenta con un certificado de seguridad vigente y aplicable a todas las subpáginas del mismo portal.

Sin más por el momento, reciba un cordial saludo.

ATENTAMENTE

Ing. Jesús Alexandro Sandoval Loya
Subcoordinador de Sistemas