

COORDINACION DE SISTEMAS

Asunto. Respuesta a solicitud de información

Chihuahua, Chihuahua, a 4 de noviembre de 2024

**A QUIEN CORRESPONDA
P r e s e n t e.-**

Vista su solicitud de información recibida y registrada en la Plataforma Nacional de Transparencia, bajo el folio 080159424000042, se informa lo siguiente:

1. Informar si dentro de la institución se cuenta con un gobierno de la información o ciberseguridad y cuales áreas participan.

No se cuenta con un documento que compile las características con las que debemos de contar para el manejo de la documentación interna; esta se encuentra dividida en los lineamientos del Reglamento Interno así como de la Ley de Archivos del Estado de Chihuahua y la Ley de Transparencia.

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 de materia de TIC y de seguridad de la información.

Se tienen lineamientos que se deben de seguir para adquisiciones de bienes materiales y de servicio, se realiza en conjunto con el área Administrativa ya que toda consulta de adquisición debe pasar por el Comité de Adquisiciones, para ser evaluado y considerar presupuesto.

b)informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC

Si se tiene Inventario institucional que se realiza entre el área Administrativa y de sistemas para tener un control de nuestro activo.

c) un plan de continuidad de operaciones, y señalar la fecha de implementación

El área de sistemas se encuentra en crecimiento y estamos realizando capacitaciones de las funcionalidades que debe tener el departamento. Por lo que manuales de operatividad y división de tareas se esta trabajando.

d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación.

Si hemos tenido contingencias donde hemos implementado las mitigaciones de riesgos, este va creciendo con la experiencia que se obtiene de cada proceso electoral; durante este pasado proceso se tuvo un evento en los meses de abril-mayo del 2024.

e) Desarrollado e implementado un programa de gestión de vulnerabilidades.

Cada inicio de procesos ya se tiene un plan a llevar a cabo para la mitigación y forma de abordar sucesos que puedan interrumpir el trabajo. Por lo que es implementado al año anterior al inicio de los procesos electorales.

f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI)

El área de Sistemas no tiene un departamento de seguridad en sí, por lo que implementamos una gestión del almacenamiento de la información.

g) Informar si se cuenta con una política general de seguridad de la información y en su caso, quien interviene y desde cuándo se implementó.

Si se cuenta ya que el cuidado de los expedientes generados tienen un control desde su recepción hasta su culminación en los archivos del Tribunal. Siempre se han implementado para tener certeza en el contenido de estos. Y se ha estado creciendo al aprobarse la Ley de Archivos la cual no agrega varias especificaciones para su cuidado y almacenamiento. Se interviene desde oficialía de partes, la Secretaría General, el área de Archivo y el área de sistemas para su cuidado y preservación.

h) Informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la institución.

Se tiene identificada la ruta crítica de los procesos del expediente.

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.

Internamente no se cuenta con ese Equipo, pero se contempla el apoyarnos con expertos en caso de incidentes.

3. Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente:

si

(i) referir la fecha de creación. (ii) la fecha de implementación (iii) si es que se ha actualizado o modificado y en cuantas ocasiones; (iv) cuales áreas participaron en la creación de dicha estrategia.



Cada año se realiza un informe de las actividades del departamento de Sistemas, por lo que la última actualización es del 5 de febrero de 2024. Siempre involucrando al área de Archivo y Secretaría General.

4. Informar si se emplea la firma electrónica avanzada en el instituto:

Si se utiliza firma electrónica.

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

No se realizan este tipo de simulacros

6. Señalar si se cuenta con lineamientos de programación y desarrollo de sistemas informáticos seguros.

No se cuenta con dichos lineamientos

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

Es propio el DataCenter.

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

No existen lineamientos, pero se utiliza el Meet de Google y es requerido conexión con cuenta institucional.

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:

Si se cuenta con un correo institucional

a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información.

No cuenta con dicha leyenda; esta se encuentra en la página de internet

c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;

Si se tiene control de la cantidad de correos

d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que los protejan del envío y recepción de correos electrónicos con software malicioso;



La suite contratada con Google si cuenta con dichos filtros.

e)cuenta con cifrado en el envío de información;

Si cuenta con esta característica

10. Informar si se cuenta con mecanismos para evitar la divulgación no autorizada de datos o información institucional por parte de los servidores públicos;

Estos mecanismos se encuentran en los lineamientos de reglamento interno del Tribunal.

11. Informar si la página web de la institución cuenta con: a) aviso de privacidad

Si cuenta con el aviso

b)certificados digitales vigentes

Si se tiene los SSL (Secure Sockets Layer) correspondiente.

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

Haber realizado una capacitación de este protocolo no se ha realizado.

13. Informar si se cuenta con a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información.

Si se cuenta con mecanismos para estar monitoreando como se encuentra la información

b)indicadores que permita medir el madurez institucional en la gestión de seguridad de la información.

No se cuenta con esos indicadores

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 su caso afirmativo señalar: cuando se implemento.

Cada vez que entra nuevo personal debe ser capacitado para el manejo de la información dentro de la Institución.

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 se afirmativa esta pregunta.¿desde cuando se adoptó y cuáles áreas participaron en su desarrollo e implementación.

Si se cuenta con un programa que nos ayuda a no divulgar información considerada delicada. Este no fue desarrollado intermitentemente, ya que fue proporcionado con ayuda de nuestro titular de la Unidad de Transparencia, por el Instituto Chihuahuense de Transparencia y Acceso a la Información Pública (ICHITAIP). Se implemento hace dos años. Anteriormente se realizaba con herramientas proporcionadas por suite ofimática.

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 cuando se implementó

Para informar a la sociedad en general se utiliza la página web y las redes sociales como son Facebook, instagram, X, tiktok y YouTube. Siendo desde el 2014 cuando se empezaron a implementar las redes sociales. Sistemas y el área de Comunicación Social se encargan de la difusión.

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.

Se realiza por medio de vías de comunicación rápidas, como son la telefonía interna de la institución o con los teléfonos particulares, ya que es un hecho que tiene que ser resuelto a la brevedad. Las áreas que se involucran son Secretaria General, Sistemas y la Unidad de Transparencia. Se ha implementado desde 2018.

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

Si cada servidor público se requiere mover o trasladar un activo debe cumplir otorgándose la información correspondiente al área administrativa.

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.

Se ha asistido a conferencias y capacitaciones en materia de transparencia, protección de datos personales y de archivo. En cuanto a la seguridad de la información son conocimientos que recaen en la formación académica de los integrantes del área de Sistemas.

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

Se han tenido 2 acontecimientos de ciberseguridad, mas no directamente con la información que se maneja internamente, esto se ha sufrido a nuestra pagina de internet que contiene información pública y no se encuentra en servidores conectados al interior de esta institución.

21. Informar si se han adoptado esquemas de mejores practicas en materia de protección de datos personales y señalar cuales son.

Se ha adquirido un programa de teste de datos personales así como capacitaciones sobre el tema.

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 cuales han sido las recomendaciones vertidas por el INAI, en su caso.

Al momento no contamos con sistema o plataforma informática que implique tratamiento de datos personales intensivo. Se tiene captura de datos biométricos de formar interna para el control de acceso al personal del Tribunal, los cuales están resguardados en el área de Administrativo, para utilizarse únicamente en red interna.

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

Si se cuenta con documentos de información 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.

De igual forma que si se suscitará una brecha de información de datos personales, un incidente de seguridad informática, debe ser comunicado de forma rápido por lo que se realiza por medio de la telefonía interna o por medio de los teléfonos particulares.

25. Informar cada cuando tiempo se actualizan las medidas de ciberseguridad dentro de la institución.

Se realizan de forma anual, ya que es el tiempo en cuando se presentan informes de forma general de la institución y se pueden abordar requerimientos en las diferentes áreas que conforman a la institución.

26. Informar sí se llevan auditorias de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;

No, al momento no se llevan a cabo auditorias de ciberseguridad.

27. Señalar si se cuenta con un help desk que recojámoste las incidencias repostadas eso los servidores públicos, y en su caso señalar sis es interno o externo.

Si el help desk que se tiene en el instituto es interno y se lleva el control de los incidentes en los bienes inmuebles electrónicos.

28. Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tiene certificados digitales vigentes.

Si la página web del tribunal donde se localizan las sentencias emitidas por este órgano jurisdiccional se encuentran con certificados vigentes.

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

No se cuenta con un documento que compile las características con las que debemos de contar para el manejo de la documentación interna; esta se encuentra dividida en los lineamientos del Reglamento Interno así como de la Ley de Archivos del Estado de Chihuahua y la Ley de Transparencia.

30. Informar si se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa.

si

(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.

Cada año se realiza un informe de las actividades del departamento de Sistemas, por lo que la última actualización es del 5 de febrero de 2024. Siempre involucrando al área de Archivo y Secretaría General.

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

Aunque a través del cuestionario se pronunció que se cuenta con lineamientos de políticas de seguridad, procesos de gestión de riesgos, controles de seguridad y capacitación para asegurar la información de manera íntegra y con disponibilidad, la realización de auditorías es un componente esencial para validar la efectividad y el cumplimiento de todas esas medidas. Sin auditorías, el sistema de gestión de seguridad de la información (SGSI) no estaría completo, ya que no se estaría verificando de manera objetiva si todas las acciones implementadas están funcionando de acuerdo a lo planeado. Al momento estamos trabajando para llegar a implementarlas.