"2024 Bicentenario de Coahuila; 200 años de grandeza".

Saltillo, Coahuila de Zaragoza a 31 de octubre de 2024
Oficio No. UT/CJEM/072/2024
ASUNTO: Respuesta a Solicitud de Información

C.
N° de folio: 051277500004924
P R E S E N T E.-

En atención a la solicitud de información con número de folio 051277500004924, interpuesta y recibida de manera oficial por este Centro de Justicia y Empoderamiento para las Mujeres del Estado de Coahuila de Zaragoza el día veintiuno (21) de octubre del año en curso, a través de la Plataforma Nacional de Transparencia (PNT) con archivo adjunto el cual consta de cincuenta y cinco (55) preguntas, solicitud en la que designa como medio para recibir notificaciones el correo electrónico nacidoel1deenero@gmail.com y como medio de entrega electrónico a través del Sistema de Solicitudes de Acceso a la Información PNT, mediante el cual solicita la siguiente información:

"SECCION 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 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.
PARTADO 2
Solicito la siguiente información.
29. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
30. 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 ;
31. Informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;
32. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente 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?;
33. Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;
34. 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;
35. 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;

36. Informar si se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;
37. Informar si se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes; si, de acuerdo al programa de mantenimiento anual, el área de informática de cada centro
38. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores público;
39. 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.
40. Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;
41. Informar si se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;
42. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
43. 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 ey 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;
44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
45. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;
47. 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.
48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo. Si la colaboración institucional en el tema y es externa.
APARTADO 3
49. Indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial.
50. En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia.
51. En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad, favor de indicar el sujeto obligado que pudiera contener dicha información. Me gustaría saber de qué manera aplican medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al momento de brindar servicios a la ciudadanía. En caso de que no, saber si se tienen proyectos para aplicar dicho tipo de tecnología. A su vez se pide conocer lo siguiente:
52. Qué programas, algoritmos, sistemas de inteligencia artificial, sistemas de decisiones judiciales asistidas, algoritmos o programas de selección aleatoria de casos a jueces, tiene y opera.
53. El número de registros existentes de lo solicitado en el punto anterior.
Las fechas de operación.
El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.
Los contratos de su uso o adquisición.
54. ¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas se selección y asignación aleatoria de casos?
55. ¿Qué datos se utilizan para la selección y asignación aleatoria de casos?"... (Sic)

En aras de atender a su solicitud de información de manera oportuna y brindar respuesta a la misma, me permito informar lo siguiente:

Señalamos que este Centro de Justicia y Empoderamiento para las Mujeres del Estado de Coahuila, en sus seis Centros ubicados en las ciudades de Saltillo, Torreón, Matamoros, Frontera, Acuña y Piedras Negras, y al ser un ente de acción, tiene por objeto coordinar, articular y vincular bajo una política integral, multisectorial e interinstitucional, **las acciones, programas y servicios dirigidos a las mujeres y niñas víctimas del delito, violencia o de violación de sus derechos, a fin de garantizar el goce y el ejercicio pleno de sus**

derechos humanos y su acceso a la justicia, promoviendo su plena incorporación a la vida productiva, social, cultural y política en la sociedad, priorizando la protección de su integridad, la de sus hijas e hijos; según lo establecido en el Decreto de Creación y Decretos que Modifican al Decreto de Creación.

Acciones tendientes a detectar y atender las causas y manifestaciones de la violencia hacia las mujeres e implementar las medidas necesarias para salvaguardar su integridad física y emocional, tanto de la víctima como de sus hijas e hijos; erradicar y sancionar la violencia contra las mujeres, pero además, para apoyar el empoderamiento educativo, emocional y laboral de las mujeres.

Dando respuesta al primer cuestionamiento de su solicitud relativo a ***"si dentro de la institución se cuenta con un gobierno de seguridad y cuales áreas participan"***, si cuentan con un sistema seguridad

Para dar contestación a la pregunta número dos referente a ***"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"*** le hacemos de conocimiento que para el apartado **a)** la Dirección de Adquisiciones del Estado de Coahuila es la encargada del proceso de contratación de adquisición, el arrendamiento de bienes o la prestación de bienes, esto regido por los lineamientos de la Ley de Adquisición, Arrendamientos y servicios del sector Público; en el apartado **b)** se cuenta con un inventario institucional el cuales administrado por parte de la Secretaria de Finanzas; en el inciso **c)**, se cuenta con un programa anual de mantenimiento, el cual se implementó desde el inicio de operaciones de cada uno de los centros (Torreón: 29 de noviembre de 2013; Matamoros: 24 de mayo de 2014; Saltillo: 03 de diciembre de 2014; Frontera: 25 de noviembre de 2015; Acuña: 27 de marzo de 2017 y Piedras Negras: 12 de octubre de 2022), en cuanto al apartado **d), e)** y **f)** hasta el momento no se han implementado, contestando al apartado **g), h)** e **i),** como se menciona anteriormente desde el inicio de operaciones (creación) de cada uno de los centros se contempla el programa anual de mantenimiento, cuyo objetivo es mantener el buen funcionamiento óptimo de los equipos y sistemas que se operan en los centros.

Para atender al cuestionamiento tres de su solicitud el cual nos habla sobre ***"si se cuenta con una estrategia de ciberseguridad dentro de la institución"***, no

En respuesta a la cuarta pregunta referente a ***"informar si emplea la firma electrónica avanzada en la institución"*** es de señalar que dentro en los seis Centros de Justicia de Empoderamiento para las mujeres no se emplea este sistema de firma o identificador.

Dando atención al cuestionamiento quinto en relación a ***"si se realizan simulacros sobre el plan de recuperación de desastres o incidentes cibernéticos"***, informamos que en estas situaciones se implementa de igual manera el programa anual de mantenimiento que como ya mencionamos tiene como objetivo mantener el buen funcionamiento de los equipos y del sistema de seguridad que se operan en los centros.

Respondiendo a la pregunta sexta relativo a ***"si se cuenta con lineamientos de programación y desarrollo de sistemas informáticos seguros"*** se hace de conocimiento que según las funciones de este Centro

de Justicia y empoderamiento de las Mujeres del Estado de Coahuila no es aplicable debido a que la institución no cuenta con un departamento especializado para la programación y desarrollo de sistemas.

En continuidad con su solicitud y en respuesta a la pregunta séptima en relación a ***"informar si los servicios de centros de datos son propios, de otra institución, gubernamental o de un tercero"*** es de señalar que los servicios de centros de datos derivan de otra institución gubernamental.

Para dar respuesta al cuestionamiento número ocho de su solicitud referente a ***"si se cuenta con lineamientos de seguridad para las videollamadas"*** por lo que se le informa que cuando se emplea el trabajo por videollamada es utilizada la plataforma de Telmex, el cual cuenta con lineamientos propios de seguridad, esto como parte del servicio que este proporciona.

En continuidad a su solicitud y dando respuesta a la pregunta nueve y derivando de ella los siguientes incisos ***"si se cuenta con correo electrónico institucional cuenta con a) inserción de leyenda de confidencialidad de la información, b) control institucional en totalidad de los correo contenidos en las carpetas de usuarias, c) solución de filtrado para correo no deseado así como programas informáticos que protejan el envío y recepción de correos con software malicioso, d) si cuenta con cifrado en el envió de información"*** se hace de conocimiento que este Centro de Justicia y Empoderamiento para las Mujeres del Estado de Coahuila, si cuenta con un correo electrónico institucional (cjem@coahuila.gob.mx) el cual está regido por el programa Microsoft Outlook mismo que tiene lineamientos y funciones ya establecidas.

En cuando al cuestionamiento número diez que a la letra dice ***"si se cuenta con mecanismos para evitar alguna divulgación no autorizada de datos o información institucional por parte de servidores públicos"*** *esta institución si cuenta con un mecanismo de confidencialidad* además de que el centro se basa en los lineamientos y mecanismos establecidos en los artículos 21, 22, 24 y demás relativos a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila de Zaragoza así como al artículo 68 y demás relativos de la Ley General de Transparencia y Acceso a la Información Pública.

Para dar respuesta a pregunta once de su solicitud de información referente a ***"si la página web cuenta con a) aviso de privacidad, b) certificados digitales"*** se le hace de conocimiento que la página web si cuenta con los avisos de privacidad, mismos que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila de Zaragoza en sus artículos 20, 21 y 22. En cuanto a los certificados digitales por el momento no se han aplicado a la página web. Así mismo me permito proporcionarle la página web del Centro.- http://www.cjemcoahuila.gob.mx/

En cuanto a la pregunta número doce ***"si el personal responsable está capacitado en la implementación del Protocolo Nacional Homologado para Gestión de Incidentes Cibernéticos"*** Esta Institución cuenta con colaboraciones de gobierno, como lo es la Unidad de la Policía Cibernética de la Fiscalía General del Estado la cual cuenta con personal capacitado para brinda apoyo al Centro en temas cibernéticos.

Dando respuesta a su cuestionamiento número trece sobre ***"si se cuenta con mecanismos de supervisión y evaluación que permitan la medir la efectividad de los controles de seguridad de la información así como de indicadores que permitan medir la madurez institucional en la gestión de seguridad de la información"*** es de señalar que para este tipo de acciones se lleva a cabo el programa anual de mantenimiento el cual es aplicado desde la creación de operaciones de cada uno de los seis Centros de Justicia, mencionado anteriormente en la interrogante número 2.

En continuidad con la pregunta número catorce en donde se solicita ***"informar si dentro de la institución se cuenta con un programa de formación en la cultura de la seguridad de la información o ciberseguridad"*** no

"2024 Bicentenario de Coahuila; 200 años de grandeza".

En respuesta a su interrogante número quince el cual establece ***"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"*** hacemos de conocimiento que cada uno de los seis Centro de Justicia y Empoderamiento de las Mujeres del Estado de Coahuila de Zaragoza, cuenta con un sistema de gestión llevando a cabo los lineamientos establecidos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en los artículos 27, 28, 30 y demás relativos de la presente Ley.

En cuanto a su pregunta número dieciséis sobre ***"si se cuenta con modelo o sistema de comunicación para informar a la sociedad sobre los eventos o incidentes de seguridad de la institución"*** es de señalar que no se cuenta con un modelo como tal ya que este tipo de información se maneja meramente interno a no ser que sea el o la titular de la información a la cual se le tenga que rendir una aclaración.

Dando contestación a la pregunta diecisiete referente a ***"si se cuenta con modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información"*** hacemos de conocimiento que no existe un modelo o sistema establecido como tal, pero si se realizan comunicados internos (oficios o tarjetas informativas) para los titulares de la información para que estos tengan conocimiento de lo acontecido en caso de que llegue a pasar alguna incidencia; esto implementado desde el inicio de la creación de operaciones de cada uno de los seis centros en colaboración con cada una de las áreas.

Para su cuestionamiento número dieciocho sobre ***"si se cuenta con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución por parte de los servidores públicos"*** le comunicamos que los lineamiento utilizados por esta institución al momento de realizar alguna acción de esta índole son los que proporciona la Secretaria de Fiscalización y Rendición de Cuentas en cuanto a temas de inventario.

En cuanto a su interrogante número diecinueve sobre ***"Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en la materia de transparencia, protección de datos personales, archivos públicos, seguridad de la información"*** le informamos que el personal se encuentra constantemente en capacitación en cuanto a los temas anteriormente mencionados, tomando en cuenta cada una de las leyes establecidas en los temas de interés para llevar a cabo las actividades encomendadas por el centro de una manera adecuada y eficaz. Me permito proporcionarle el link del programa de capacitaciones del centro.- https://www.coahuilatransparente.gob.mx/RutaDataFiles/otrainfo/documentos_otrainfo/Programa%20Anual%20de%20Capacitaci%C3%B3n%202023.pdf
https://www.coahuilatransparente.gob.mx/RutaDataFiles/otrainfo/documentos_otrainfo/Programa%20Anual%20de%20Capacitaci%C3%B3n%202024.pdf

Atendiendo a su pregunta numero veinte relativo a ***"Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas"*** no.

Dando contestación a su cuestionamiento número veintiuno sobre ***"Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;*** el personal del Centro de Justicia y Empoderamiento de la Mujeres del Estado de Coahuila de Zaragoza tiene conocimiento y lleva a cabo los lineamientos establecidos por la ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Coahuila de Zaragoza, Ley de Acceso a la Información Pública, Ley General de Transparencia y Acceso a la Información Pública y Ley general de Protección de Datos

Personales en Posesión de Sujetos Obligados, ya que son de suma importancia para el buen funcionamiento del Centro, por lo que se revisa constantemente las Leyes de interés.

En cuanto a su interrogante numero veintidós referente a ***"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"*** hasta el momento no se ha empleado ningún tratamiento intensivo o relevante datos personales en esta Institución, haciendo la aclaración que para este tipo de acciones se deben llevar a cabo los lineamientos y criterios establecidos en los artículos del 72 al 79 y demás relativos de la Ley General de Protección de Datos en Posesión de Sujetos Obligados, por lo que hasta el día de hoy no se ha generado recomendación alguna.

En la interrogante número veintitrés relevante ***"Informas si se cuenta con documento de seguridad en materia de protección de datos personales"*** se informa que este Centro de Justicia y Empoderamiento de las Mujeres del Estado de Coahuila de Zaragoza, no cuenta con un documento de seguridad establecido.

Para dar respuesta a su pregunta número veinticuatro ***"Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;*** no.

En cuanto a su cuestionamiento número veinticinco ***"Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución"*** no aplica.

Para dar contestación a la pregunta veintiséis de su solicitud ***"Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad"*** no.

En cuanto a si interrogante número veintisiete relativo a ***"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"*** esta institución no cuenta con este tipo de servicio

Para dar respuesta a su pregunta numero veintiocho referente a ***"Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes"*** le hacemos de conocimiento que este tipo de información que usted solicita no es competencia de este Centro de Justicia y Empoderamiento de las Mujeres de Coahuila de Zaragoza. Por lo tanto, le comunicamos que la información que solicita es generada y administrada por la **Poder Judicial del Estado de Coahuila de Zaragoza.**

Dando continuidad a su solicitud de información, se le comunica que su cuestionamiento numero veintinueve, es considerada repetitiva a la primera de sus preguntas, así como también la interrogante número treinta que se encuentra replicada a la pregunta tres, a lo que fueron debidamente contestadas, por tal motivo se consideran contestada

"2024 Bicentenario de Coahuila; 200 años de grandeza".

Para dar respuesta a su cuestionamiento numero treinta y uno, relativa a ***"si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución"*** como se ha señalado con anterioridad en cuanto a la materia de seguridad de la institución es aplicable en todo momento el programa anual de mantenimiento para la seguridad y buen funcionamiento optimo del centro.

Para dar contestación a su interrogante numero treinta y dos que refiere ***"si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares, se cuenta con un sistema de gestión de protección de datos personales"*** hacemos de conocimiento que cada uno de los seis Centro de Justicia y Empoderamiento de las Mujeres del Estado de Coahuila de Zaragoza, cuenta con un sistema de gestión llevando a cabo los lineamientos establecidos por la **Ley Federal de Protección de Datos Personales en Posesión de Particulares** en su capítulo segundo el cual nos habla sobre el tratamiento de los datos personales, los avisos de privacidad de los cuales debe estar enterados los titulares de la información, así como la responsabilidad y obligaciones del responsable de manejar la información. Dichos lineamientos son importantes para el manejo de la información de los titulares, dicha gestión es aplicada desde la creación de cada uno de los centros para una mejor operación institucional.

En respuesta a su interrogante numero treinta y tres referente a ***"si se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física"*** no aplica

En cuanto a la pregunta treinta y cuatro de su solicitud la cual es repetitiva a la pregunta número dieciséis y a su vez la interrogante treinta contiene la misma narrativa de su pregunta número diecisiete, a las cuales se le proporciono una respuesta, es por ellos que se consideran contestadas los presentes cuestionamientos.

En contestación a su pregunta número treinta y seis referente a ***"si se realiza capacitación continua a los servidores públicos en materia de ciberseguridad"*** el personal a cargo de la seguridad cibernética de este Centro de Justicia y Empoderamiento para las Mujeres del Estado de Coahuila de Zaragoza, cuenta con la colaboración de otras instituciones gubernamentales para el apoyo en esta materia, así como el personal que se encuentra dentro de esta institución cuanta con el conocimiento para el manejo de seguridad del centro.

Continuando con su solicitud y en respuesta al cuestionamiento número treinta y siete relativo en cuanto a ***"si se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad"*** se implementa el programa anual de mantenimiento en este tipo de casos, dicho programa es llevado a cabo por el área de Informática de este Centro.

Tomando en cuenta que la pregunta numero treinta y ocho es repetitiva a la numero dieciocho de su solicitud, así como la interrogante numero treinta y nueve que posee el mismo contenido de la pregunta numero diecinueve y a las cuales ya se le brindo una debida respuesta, es por ello que las presentes se consideran contestadas.

En respuesta a la pregunta numero cuarenta respecto a ***"Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas"*** no.

"2024 Bicentenario de Coahuila; 200 años de grandeza".

Dando contestación a la interrogante número cuarenta y uno la cual consiste en ***"si se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución"*** no.

En cuanto a la interrogante número cuarenta y dos es de señalar que es repetitiva a la pregunta número veintiuno, así como también la pregunta numero cuarenta y tres de su solicitud replica el mismo contenido de la pregunta número venidos y toda vez que ya se brindaron las respuestas pertinentes a cada uno de ellas, las presentes se consideran contestadas.

Para dar contención a su interrogante número cuarenta y cuatro referente a ***"cada cuanto tiempo se actualizan las medidas de ciberseguridad dentro de la institución"*** reiterando que para este tipo de medidas se implementa el programa anual de mantenimiento el cual se actualiza de manera bimestral.

En continuidad con su solicitud de información y considerando que la interrogante numero cuarenta y cinco posee el mismo contenido de la pregunta número veintiséis, y toda vez que a esta última ya se brindó una respuesta, se considera contestado dicho cuestionamiento.

Dando respuesta a la pregunta número cuarenta y seis de su solicitud consistente en ***"si se cuenta con un sistema de gestión de incidentes"*** señalamos que para la gestión en materia de seguridad se utiliza el programa anual de mantenimiento el cual el área de informática está encargado de llevar a cabo este programa.

Tomando en consideración que la pregunta número cuarenta y siete es repetitiva a la interrogante número veintisiete de su solicitud, y de la cual se ya se brindó una respuesta, se establece que la presente ya se dio por contestada.

Dando contestación a la pregunta número cuarenta y ocho referente a ***"si se cuenta con un equipo de respuesta a incidentes cibernéticos"*** no

Finalmente en cuanto al apartado tres que consiste en las interrogantes del cuarenta y nueve al cincuenta y cinco, precisamos que con fundamento en el artículo 95, Primer Párrafo, de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza, que a la letra dice:

> **"Artículo 95.** Cuando las Unidades de Transparencia determinen la notoria incompetencia por parte de los sujetos obligados dentro del ámbito de su aplicación, para atender la solicitud de acceso a la información, deberán de comunicarlo al solicitante, dentro de los tres días posteriores a la recepción de la solicitud y, en caso de poder determinarlo, señalarán al solicitante el o los sujetos obligados competentes."
>
> Énfasis añadido.

Precisamos que la información que usted solicita **no es competencia** de este Centro de Justicia y Empoderamiento para las Mujeres del Estado de Coahuila, por lo tanto, le comunicamos que la información que solicita es generada y administrada por la **Poder Judicial del Estado de Coahuila de Zaragoza**, de conformidad con el artículo 2, 16, 17 y 115 y demás relativos de la Ley Orgánica del Poder Judicial del Estado de Coahuila.

Instancia	Teléfono	Sitio Web	Correo electrónico
Poder Judicial para el Estado de Coahuila de Zaragoza.	844 777 4498	https://www.pjecz.gob.mx/ https://www.pjecz.gob.mx/poder-en-linea/	poderjudicialcoahuila@pjecz.gob.mx

Reiterando que este Centro de Justicia y Empoderamiento de las Mujeres del Estado de Coahuila de Zaragoza tiene por objeto coordinar, articular y vincular bajo una política integral, multisectorial e interinstitucional, las acciones, programas y servicios dirigidos a las mujeres y niñas víctimas del delito, violencia o de violación de sus derechos, a fin de garantizar el goce y el ejercicio pleno de sus derechos humanos y su acceso a la justicia, promoviendo su plena incorporación a la vida productiva, social, cultural y política en la sociedad, priorizando la protección de su integridad, y garantizando así el buen tratamiento y protección de datos personales estableciendo un entorno seguro para las usuarias, sus hijos e hijas.

Sin otro particular por el momento, le reitero la seguridad de mi atenta y distinguida consideración.

ATENTAMENTE

Licda. Paola Karina Fernández Hernández.
Titular de la Unidad de Transparencia del Centro de Justicia y Empoderamiento para las Mujeres del Estado de Coahuila de Zaragoza.

c.c.p. Lcda. Deyanira Nájera Muñoz, Directora General del Centro de Justicia y Empoderamiento para las Mujeres en Coahuila de Zaragoza
c.c.p. Archivo

PLATAFORMA NACIONAL DE
TRANSPARENCIA

ACUSE DE RECIBO

icai

21/10/2024 15:24:38 PM

SOLICITUD DE ACCESO A LA INFORMACIÓN

DATOS GENERALES DE LA SOLICITUD

Número de Folio	051277500004924
Fecha de Presentación	21/10/2024
Nombre del Solicitante	
Sujeto Obligado	Centro de Justicia y Empoderamiento de la Mujer
Información Solicitada	SECCION 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 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 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 si 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.
E-mail del Solicitante	nacidoel1deenero@gmail.com

FECHA DE INICIO DE TRÁMITE

De conformidad con el artículo 99 de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza, su solicitud será atendida a partir del primer día hábil posterior a la fecha oficial de recepción, y la respuesta le será notificada en un plazo no mayor a nueve días hábiles, contados a partir del día siguiente de la recepción de la solicitud. Además, se precisará el costo y la modalidad en que será entregada la información.

Este plazo podrá ampliarse hasta por cinco días más cuando existan razones que lo motiven. Dicha ampliación se notificará a más tardar el octavo

PLATAFORMA NACIONAL DE
TRANSPARENCIA

ACUSE DE RECIBO

21/10/2024 15:24:38 PM

SOLICITUD DE ACCESO A LA INFORMACIÓN

FECHA DE INICIO DE TRÁMITE

día del plazo descrito en el párrafo anterior.

La solicitud recibida después de las 16:00 horas de un día hábil o en cualquier hora de un día inhábil, se tendrá por recibida el día hábil siguiente.

PLAZO DE RESPUESTA Y POSIBLES NOTIFICACIONES A SU SOLICITUD

Respuesta a su solicitud	09 días hábiles	01/11/2024
Si se requiere aclaración de la información solicitada	03 días hábiles	24/10/2024
Si se requiere ampliación del plazo de respuesta	14 días hábiles	08/11/2024