07/06/2022 01:21:12 AM

Acuse de registro de solicitud de información pública

Se ha recibido exitosamente su solicitud de información pública, con los siguientes datos:

Datos de la Solicitud

Sujeto Obligado	TRIBUNAL SUPERIOR DE JUSTICIA (TSJ)
Folio	271473900023622
Fecha de solicitud	07/06/2022
Nombre del solicitante	qubit
Representante (en su caso)	

Detalle de la Solicitud

Información requerida	Solicito la siguiente información 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 seguirdad 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.
Datos adicionales	15. Informar sí de conformidad con la Ley General de Protección de Datos Personales en

Acuse de registro de solicitud de información pública

Datos adicionales	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.
Medio de notificación	Electrónico a través del sistema de solicitudes de acceso a la información de la PNT

* Especificar de manera clara y precisa los datos e información que requiere.
* No incluir datos personales.

Plazos de respuesta

Respuesta a la Solicitud (Positivo, negativo o inexistencia)	15 días hábiles	28/06/2022
Requerimiento de información (Prevención)	5 días hábiles	14/06/2022
Incompetencia	3 días hábiles	10/06/2022

La solicitud recibida en día hábil después de las 16:00 horas, o en día inhábil, se tendrá por presentada al siguiente día hábil según el calendario aprobado por el H. Pleno del Instituto Tabasqueño de Transparencia y Acceso a la Información Pública.
Los plazos señalados empezaran a correr al día siguiente de recibida la solicitud (LTAIPET).

RECOMENDACIONES:
*Dar seguimiento frecuente a la solicitud.

Tel. (993) 5 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa,

Folio PNT: 271473900023622
Número de Expediente Interno: PJ/UTAIP/238/2022
Acuerdo con Oficio No.: TSJ/UT/618/2022
ACUERDO DE DISPONIBILIDAD DE LA INFORMACIÓN.

Villahermosa, Tabasco a 28 de junio de 2022.

CUENTA: Con el oficio TSJ/DEIC/087/2022, signado por el Lic. Carlos Alberto Ulín Sastré Director de Estadística Informática y Computación, mediante el cual se proporciona respuesta a la solicitud de información con número de folio **271473900023622**. ----------
----------Conste----------

Vista la cuenta que antecede se acuerda:

PRIMERO: Por recibido el oficio de cuenta, por medio del cual se da respuesta a la solicitud de acceso a la información pública con número de folio **271473900023622**, recibida el siete de junio de dos mil veintidós a las una horas con veintiún minutos, presentada vía Plataforma Nacional de Transparencia, mediante la cual requiere: ***"...Solicito la siguiente información***
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.

Tel. (993) 5 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa,

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 seguirdad 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?;

Tel. (993) 5 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa,

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 ...". Por lo que se ordena agregar a los autos, el oficio de cuenta para que surta el efecto legal correspondiente. ----------

SEGUNDO: Con fundamento en los artículos 4, 6, 49, 50 fracciones III y IV y el 138 en relación con el 133, todos de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, así como el artículo 45 de su Reglamento, se acuerda que la información solicitada ante esta Unidad de Transparencia es pública.----------

PODER JUDICIAL DEL ESTADO DE TABASCO

En tal virtud, se acuerda entregar al requirente de información el oficio de cuenta, por medio del cual el área competente, se pronuncia dando respuesta a la solicitud de acceso a la información motivo del presente acuerdo.----------

El oficio de respuesta que se proporciona se describe a continuación:

No.	Número de Oficio	Área	Responsable
1	TSJ/DEIC/087/2022	Dirección de Estadística Informática y Computación	Lic. Carlos Alberto Ulín Sastré

Es importante señalar que, el objeto del Derecho de Acceso a la Información, consiste en acceder a la información generada, obtenida, adquirida, transformada o en poder de los sujetos obligados, contenida en cualquier registro que documente el ejercicio de las facultades, funciones, competencias o las actividades de los sujetos obligados y sus servidores públicos, en el entendido que, dicha información se entregará en el estado en que se encuentre, ya que no se tiene imperativo legal alguno de procesarla conforme al interés del solicitante, es decir, que no se cuenta con la obligación de generar un documento ad hoc para responder el requerimiento informativo.----------

Para sustentar lo anteriormente señalado, se cita el Criterio 009-10, emitido por el Pleno del Instituto Nacional de Transparencia y Acceso a la Información, Protección de Datos Personales, antes IFAI, mismo que se transcribe:

Criterio 009-10

Las dependencias y entidades no están obligadas a generar documentos *ad hoc* para responder una solicitud de acceso a la información. Tomando en consideración lo establecido por el artículo 42 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que establece que las dependencias y entidades sólo estarán obligadas a entregar documentos que se encuentren en sus archivos, las dependencias y entidades no están obligadas a elaborar documentos *ad hoc* para atender las solicitudes de información, sino que deben garantizar el acceso a la información con la que cuentan en el formato que la misma así lo permita o se encuentre, en aras de dar satisfacción a la solicitud presentada.

Expedientes:

0438/08 Pemex Exploración y Producción – Alonso Lujambio Irazábal
1751/09 Laboratorios de Biológicos y Reactivos de México S.A. de C.V.– María Marván Laborde
2868/09 Consejo Nacional de Ciencia y Tecnología – Jacqueline Peschard Mariscal
5160/09 Secretaría de Hacienda y Crédito Público – Ángel Trinidad Zaldívar
0304/10 Instituto Nacional de Cancerología – Jacqueline Peschard Mariscal.

También sirve de apoyo el criterio 03-17 del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que a la letra menciona:

No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información. Los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública, señalan que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las características físicas de la información o del lugar donde se encuentre. Por lo anterior, los sujetos obligados deben garantizar el derecho de acceso a la información del particular, proporcionando la información con la que cuentan en el formato en que la misma obre en sus archivos; sin necesidad de elaborar documentos ad hoc para atender las solicitudes de información.
Resoluciones:
•RRA 0050/16. Instituto Nacional para la Evaluación de la Educación. 13 julio de 2016. Por unanimidad. Comisionado Ponente: Francisco Javier Acuña Llamas.
•RRA 0310/16. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. 10 de agosto de 2016. Por unanimidad. Comisionada Ponente. Areli Cano Guadiana.
•RRA 1889/16. Secretaría de Hacienda y Crédito Público. 05 de octubre de 2016. Por unanimidad. Comisionada Ponente. Ximena Puente de la Mora.

Por último, es importante destacar que la actuación de este sujeto obligado se desarrolló con apego al principio de buena fe, entendido éste como un principio que obliga a todos a observar una determinada actitud de respeto y lealtad, de honradez en el tráfico jurídico y esto tanto cuando se ejerza un derecho, como cuando se cumpla un deber y por ello esta Institución, en uso de sus atribuciones, atendió la solicitud conforme a su literalidad y al marco jurídico que rige el derecho de acceso a la información.----------

TERCERO: En caso de no estar conforme con el presente acuerdo, hágasele saber a la persona interesada que dispone de 15 días hábiles, contados a partir del día hábil siguiente a la notificación de este proveído, para interponer por sí misma o a través de representante legal, recursos de revisión ante el Instituto Tabasqueño de Transparencia y Acceso a la Información Pública o ante esta Unidad de Transparencia, debiendo acreditar lo requisitos previstos en el numeral 150 de la Ley en la materia.----------

CUARTO: Notifíquese la solicitud recibida, el presente acuerdo y la respuesta dada, a través de la Plataforma Nacional de Transparencia, medio indicado por la persona interesada en su solicitud y en su oportunidad, archívese el presente asunto como total y legalmente concluido.-
----------Cúmplase.----------

PODER JUDICIAL DEL ESTADO DE TABASCO

Tel. (993) 5 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa,

Así lo acuerda, manda y firma, el Director de la Unidad de Acceso a la Información del Poder Judicial del Estado de Tabasco. ----------

Esta hoja de firmas corresponde al Acuerdo de Disponibilidad de la Información de fecha 28 de junio de 2022, dictado en el expediente relativo a la solicitud de información identificada con el número de folio 271473900023622. ----------

Tel. (993) 5 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa, Tab.

Villahermosa, Tabasco, Junio 06 de 2022

OFICIO No. TSJ/UT/567/2022

LIC. CARLOS ALBERTO ULÍN SASTRÉ
DIRECTOR DE ESTADÍSTICA, INFORMÁTICA Y COMPUTACIÓN
DEL PODER JUDICIAL DEL ESTADO DE TABASCO
P R E S E N T E.

Por medio del presente, me permito solicitar a Usted, su amable colaboración para responder la solicitud de información, que a la letra dice:

PJ/UTAIP/238/2022: ***"...Solicito la siguiente información***
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;
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.
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;

Tel. (993) 5 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa, Tab.

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 ....."

No omito manifestar, que no se deben incluir datos personales. Así mismo le informo que el término para rendir la respuesta a lo solicitado es el **14 de Junio** del presente año. Sin otro particular, me permito enviarle un cordial saludo.

ATENTAMENTE

DR. JULIO DE JESUS VAZQUEZ FALCON
DIRECTOR DE LA UNIDAD DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN

PODER JUDICIAL
DEL ESTADO DE TABASCO

C.c.p. **Archivo**
DR.JJVF/QFB.JRIV

Villahermosa, Tab., a 14 de junio de 2022
Oficio N° TSJ/DEIC/**087**/2022

DR. JULIO DE JESÚS VÁZQUEZ FALCÓN
TITULAR DE LA UNIDAD DE TRANSPARENCIA
P R E S E N T E.

En respuesta a su oficio TSJ/UT/567/2022, de fecha 06 de junio de 2022, mediante el cual solicita información referente a respuestas a un cuestionario de seguridad en la gestión de las TIC. Al respecto se remiten las respuestas a su cuestionario.

1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan:
R: Se cuentan con políticas establecidas para la seguridad de las redes y los sistemas. Las áreas que participan son: Enlaces y comunicaciones, Desarrollo de sistemas.

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:
R: No.

b) Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC;
R: Sí se cuenta con el inventario de bienes y servicios administrado por el departamento de inventarios de la institución.

c) un plan de continuidad de operaciones. y señalar la fecha de implementación;
R: No.

d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres. Señalar la fecha de desarrollo e implementación;
R: Sí se cuenta con el plan de recuperación de desastres, desarrollado en junio de 2021.

e) desarrollado e implementado un programa de gestión de vulnerabilidades;
R: En cuestión de informática se cuenta con un equipo de seguridad perimetral que cuenta con políticas muy específicas de acceso a la información, solo personal autorizado tiene acceso a los sistemas.

f) Marco de Gestión de Seguridad de la Información (MGSJJ Sistema de Gestión de Seguridad de la Información (SGSI);
R: Se cuentan con políticas ya establecidas.

g) Informar sí se cuenta con una política general de seguridad de la información y en su caso o quienes intervienen y desde cuándo se implementó;
R: Sí se cuenta con políticas generales. Intervienen el área de redes dando accesos o restringiendo accesos, se monitorea los ataques externos e internos.

h) Informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;
R: No.

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: Se cuenta con un comité directivo de seguridad, integrado por:
1. Arq. Gloria Guadalupe Ascencio Lastra
2. Lic. Félix Emmanuel Brown Zentella
3. Lic. Jesús David Hernández Delgado
4. Lic. Guillermo Enrique Pensado Beer
5. C. Carlos Santiago Garcia

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: *R: Creado anterior al año 2020*
(ii) la fecha de implementación: *R: Implementado en años anteriores a 2020.*
(iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; *R: Se a implementado 3 actualizaciones.*
(iv) cuáles áreas participaron en la creación de dicha estrategia. *R: El área de redes.*

4. Informar sí se emplea la firma electrónica avanzada en la institución;
R-: Sí se emplea la Firma electrónica institucional. http://ficepoj.tsj-tabasco.gob.mx/login/

5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;
R: No, debido a que constantemente se hacen ventanas de tiempos para las actualizaciones, respaldos y mejoras, en los sistemas fuera de los horarios jurisdiccionales establecidos.

6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;
R: Actualmente se implementan las guías y buenas prácticas de desarrollo emitidos por Microsoft.
https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-4.0/ms184412(v=vs.100)?redirectedfrom=MSDN

Tel. (993) 5 92 27 80 ext. 4070 y 4072
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000. Villahermosa, Tab.

7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero.
R: Son Propios.

8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;
R: Si. El área de tecnologías genera los LINKS (invitaciones) y claves de acceso para las reuniones vía zoom.

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: No existe una cultura de uso de la leyenda de confidencialidad, así como un estándar para la misma.

c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;
R: SÍ.

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

e) cuenta con cifrado en el envío de información.
R: SÍ.

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.

11. Informar si la página web de la institución cuenta con:
a) aviso de privacidad; *R: SÍ.*
b) certificados digitales vigentes: *R: SÍ.*

12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
R: SÍ.

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:
R: Actualmente nos encontramos desarrollando estos mecanismos de evaluación.

Tel. (993) 5 92 27 80 ext. 4070 y 4072
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa, Tab.

b) Indicadores que permitan medir la madurez institucional en la gestión de seguridad de la información;
R: Actualmente nos encontramos desarrollando estos 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 caso afirmativo señalar: cuándo se implementó"
R: Actualmente nos encontramos desarrollando este programa y sus campañas de formación.

Sin más por el momento, aprovecho la ocasión para enviarle un cordial saludo.

ATENTAMENTE

LIC. CARLOS ALBERTO ULIN SASTRE
DIRECTOR DE ESTADÍSTICA, INFORMÁTICA Y COMPUTACIÓN

C.c.p. C.c.p. Arq. Gloria Guadalupe Ascencio Lastra.- Oficial Mayor Judicial.- Para su conocimiento.
Archivo.
LIC. JAP / mavv.