PLATAFORMA NACIONAL DE TRANSPARENCIA

PLATAFORMA NACIONAL DE TRANSPARENCIA

ITAIT
INSTITUTO DE TRANSPARENCIA, DE ACCESO A LA INFORMACIÓN Y DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE TAMAULIPAS

21/10/2024 15:57:42 PM

# ACUSE DE RECIBO DE SOLICITUDES DE INFORMACIÓN

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

| | |
|---|---|
| Folio: | 280527624000186 |
| Fecha de presentación | 22/10/2024 |
| Nombre del solicitante: | |
| Sujeto Obligado: | Instituto Electoral de Tamaulipas (IETAM). |
| Información solicitada: | APARTADO 1<br>1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;<br>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.<br>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 ;<br>4. Informar sí se emplea la firma electrónica avanzada en la institución;<br>5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;<br>6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;<br>7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;<br>8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;<br>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.<br>10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;<br>11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;<br>12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;<br>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;<br>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. |

**FECHA DE INICIO DEL TRÁMITE**

Con fundamento en el Artículo 146 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas, su solicitud será atendida en el menor tiempo posible, que no podrá ser mayor de veinte días, contados a partir del siguiente día de su presentación. Además, se precisará el costo y la modalidad en que será entregada la información, atendiendo en la mayor medida de lo posible a la solicitud del interesado.

Excepcionalmente, este plazo podrá ampliarse hasta por diez días más cuando existan razones fundadas y motivadas, y le será notificada antes de su vencimiento. No podrán involucrarse como causales de ampliación del plazo aquellos motivos que supongan negligencia o descuido del sujeto obligado en el desahogo de la solicitud.

21/10/2024 15:57:42 PM

# ACUSE DE RECIBO DE SOLICITUDES DE INFORMACIÓN

La solicitud recibida después de las 15:00 hora de un día hábil o en cualquier hora de un día inhábil, se tendrá por recibida el día hábil siguiente.

**PLAZOS DE RESPUESTA Y POSIBLES NOTIFICACIONES A SU SOLICITUD**

| | | |
|---|---|---|
| 1) Respuesta a su solicitud: | 20 días hábiles | 20/11/2024 |
| 2) En caso de que se requiera más información: | 5 días hábiles | 29/10/2024 |
| 3) Respuesta si se requiere más tiempo para localizar la información: | 30 días hábiles | 04/12/2024 |

IETAM
INSTITUTO ELECTORAL DE TAMAULIPAS

# UNIDAD DE TRANSPARENCIA

**Solicitud:** UT/SIP/185/2024
**Folio:** 28052762400186
Cd. Victoria, Tamaulipas; a 31 de octubre de 2024

**C.**
**PRESENTE**

Por este conducto y en atención a su escrito de fecha 22 de octubre del presente año, recibida a través de la Plataforma Nacional de Transparencia, recayéndole el número de folio 28052762400186 por el cual solicita de este Instituto:

***"APARTADO 1***
***1. Informar si 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 si se cuenta con un inventario institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar si se ha desarrollado e implementado el plan 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 si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuando se implementó; h) informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar si se cuenta con un Equipo de Repuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.***
***3. Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en su caso de respuesta afirmativa, informar lo siguiente (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;***
***4. Informar si se emplea la firma electrónica avanzada en la institución;***
***5. Informar si 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 si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;***
***8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;***
***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: 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 si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información institucional por parte de los servidores públicos;***
***11. Informar si la pagina web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;***
***12. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;***
***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; b) indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;***
***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; cuando se implementó".***

Analizando la petición de cuenta y a efecto de dar cumplimiento al artículo 39 fracciones II, III y XVI; y 146 numeral 1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas; y en apego al principio de máxima transparencia y privilegiando el acceso a la información pública, mediante oficios UT/449/2024 y UT/450/2024 esta Unidad de Transparencia turnó su solicitud a la Dirección de Administración del IETAM y a la Dirección de Tecnologías de la Información y Comunicaciones el IETAM, con la finalidad de que proporcionaran la información requerida y que obra en su archivo.

Por medio del oficio ADMINISTRACIÓN/1479/2024, la Directora de Administración manifiesto lo siguiente:

***"En relación al punto 2, respecto a la consulta siguiente: "Informar si se cuenta con un inventario institucional de bienes y servicios de TIC", me permito informar que la Dirección de Administración sí cuenta con inventario instituciona de bienes y servicio de TIC.***

***En cuanto a los demás puntos planteados, esta Dirección no posee la información solicitada, ya que no se encuentra dentro de su ámbito de competencia."***

A través del oficio DTIC/SIP-008/2024, el Director de Tecnologías de la Información y Comunicaciones del IETAM, remitió su respuesta en los siguientes términos:

*"Por lo anterior, se informa que está Dirección de Tecnologías de la Información y Comunicaciones al respecto de los puntos anteriores tiene, realiza y/o atiende de la siguiente manera este tema:*

*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;*
***Respecto a este inciso, la totalidad de la información requerida no está dentro del marco de competencia de esta Dirección, salvo en lo referente al "marco de mejores prácticas aplicables a la gestión de las TIC", en cuyo caso no se ha estipulado marco alguno por parte de esta Dirección de Tecnologías de la Información y Comunicaciones.***
*c) un plan de continuidad de operaciones, y señalar la fecha de implementación;*
***No se cuenta con un plan de continuidad de operaciones.***
*d) Informar si se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;*
***No se cuenta con un plan de recuperación ante desastres.***
*e) desarrollado e implementado un programa de gestión de vulnerabilidades;*
***No sé a 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);*
***No se cuenta***
*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;*
***No se cuenta***
*h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;*
***No se cuenta***
*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.*
***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;*
***No se cuenta con una estrategia de ciberseguridad dentro de la institución.***

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

*5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;*
***No se realizan simulacros***

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

*7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;*
***Son propios.***

*8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;*
***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:*
*a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información;*
***No***
*c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;*
***Si***
*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;*
***Si***
*e) cuenta con cifrado en el envío de información.*
***No***

*10. Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;*
***No se cuentan con mecanismos para evitar la divulgación no autorizada***

*11. Informar sí la página web de la institución cuenta con:*
*a) aviso de privacidad;* ***Si***

*b) certificados digitales vigentes;* ***Si***

*12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;* ***No, no se ha capacitado.***

*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;*
***No***
*b) Indicadores que permitan medir la madurez institucional en la gestión de seguridad de la información;*
***No***

*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 se cuenta con un programa de formación en la cultura de la seguridad de la información"***

Una vez analizado el contenido de las respuestas remitidas por el Director de Tecnologías de la Información y Comunicaciones y la Directora de Administración y es dable concluir que se encuentra apegada a derecho.

La información aquí proporcionada es de conformidad con lo que establece el artículo 16, el numeral 4 de la Ley de Trasparencia y Acceso a la Información Pública del Estado de Tamaulipas, que establece:

> ***"(...)***
> ***4. La información pública se proporcionará con base en que la misma exista en los términos planteados por el solicitante.***
> ***(...)".***

Por lo anteriormente expuesto y fundado, remítase el presente acuerdo al solicitante.

El Instituto Electoral de Tamaulipas se reitera a sus órdenes para brindarles cualquier tipo de asesoría u orientación que requiera sobre los mecanismos y procedimientos de acceso a la información y protección de datos personales que contempla la Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas.

**ATENTAMENTE**

IETAM
INSTITUTO ELECTORAL DE TAMAULIPAS
UNIDAD DE TRANSPARENCIA

**Lic. Nancy Moya de la Rosa**
**Titular de la Unidad de Transparencia del IETAM**

IETAM

UNIDAD DE TRANSPARENCIA
INSTITUTO ELECTORAL DE TAMAULIPAS

Oficio No. **UT/449/2024**
Cd. Victoria, Tamaulipas, a 23 de octubre 2024

**MTRA. IRILIANN YAZBETH NARVÁEZ WONG**
**DIRECCIÓN DE ADMINISTRACIÓN**
**PRESENTE**

*Estimada Maestra:*

Por medio del presente, le envió una solicitud de información, recibida a través de la Plataforma Nacional de Transparencia con los siguientes datos:

| Día de presentación | Folio Interno IETAM | Folio Plataforma Nacional de Transparencia |
|---|---|---|
| **22/10/2024** | **UT/SIP/185/2024** | **280527624000186** |

Se anexa copia de la solicitud para que tenga a bien proporcionar de no haber inconveniente legal a esta Unidad los datos que obren en sus archivos respecto de lo solicitado de la solicitud anexa, por lo cual, se solicita de respuesta en un término de 20 días naturales.

Excepcionalmente, deberá contestar en un término no mayor a 24 horas, si se encuentra en uno de los supuestos siguientes:

Ante la negativa del acceso a la información o su inexistencia. (Art. 19 LTyAIPET)

Cuando no sea competente para atender la solicitud de información, por razón de su materia. (Art. 151 numeral 1 LTyAIPET)

Excepcionalmente, podrá ampliarse el plazo del vencimiento de la solicitud hasta por diez días más, siempre y cuando existan razones fundadas y motivadas, las cuales deberán ser aprobadas por el Comité de Transparencia y notificándosele al solicitante previo a su vencimiento. (Art. 38 fracción IV y 146 numeral 2 LTyAIPET)

Deberá remitirse la información en un plazo no mayor de 3 días si la información ya está disponible al público en medios impresos o en formatos electrónicos disponibles en internet. (Art. 144 LTyAIPET)

Mucho agradeceré que la información proporcionada sea en formato electrónico al correo de **unidad.transparencia@ietam.org.mx**, así como copia fotostática de la misma, a fin de estar en posibilidad de dar la respuesta que corresponda al planteamiento de referencia.

Sin otro particular, le reitero mi consideración más distinguida.

INSTITUTO ELECTORAL DE TAMAULIPAS
IETAM
10:46 hrs
23 OCT 2024
RECIBIDO
DIRECCIÓN DE ADMINISTRACIÓN

**ATENTAMENTE**

IETAM
INSTITUTO ELECTORAL DE TAMAULIPAS
UNIDAD DE TRANSPARENCIA

**LIC. NANCY MOYA DE LA ROSA**
**TITULAR DE LA UNIDAD DE TRANSPARENCIA**

C.c.p. Archivo

| Reviso y Valido | NMDLR | |
|---|---|---|

UNIDAD DE TRANSPARENCIA
INSTITUTO ELECTORAL DE TAMAULIPAS

Oficio No. **UT/450/2024**
Cd. Victoria, Tamaulipas, a 23 de octubre 2024

**DR. MARIO HUMBERTO RODRÍGUEZ CHÁVEZ**
**DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**
**Y COMUNICACIONES DEL IETAM**
**PRESENTE**

*Estimado Maestro:*

Por medio del presente, le envió una solicitud de información, recibida a través de la Plataforma Nacional de Transparencia con los siguientes datos:

| Día de presentación | Folio Interno IETAM | Folio Plataforma Nacional de Transparencia |
|---|---|---|
| **22/10/2024** | **UT/SIP/185/2024** | **280527624000186** |

Se anexa copia de la solicitud para que tenga a bien proporcionar de no haber inconveniente legal a esta Unidad los datos que obren en sus archivos respecto de lo solicitado de la solicitud anexa, por lo cual, se solicita de respuesta en un término de 20 días naturales.

Excepcionalmente, deberá contestar en un término no mayor a 24 horas, si se encuentra en uno de los supuestos siguientes:

Ante la negativa del acceso a la información o su inexistencia. (Art. 19 LTyAIPET)

Cuando no sea competente para atender la solicitud de información, por razón de su materia. (Art. 151 numeral 1 LTyAIPET)

Excepcionalmente, podrá ampliarse el plazo del vencimiento de la solicitud hasta por diez días más, siempre y cuando existan razones fundadas y motivadas, las cuales deberán ser aprobadas por el Comité de Transparencia y notificándosele al solicitante previo a su vencimiento. (Art. 38 fracción IV y 146 numeral 2 LTyAIPET)

Deberá remitirse la información en un plazo no mayor de 3 días si la información ya está disponible al público en medios impresos o en formatos electrónicos disponibles en internet. (Art. 144 LTyAIPET)

Mucho agradeceré que la información proporcionada sea en formato electrónico al correo de **unidad.transparencia@ietam.org.mx**, así como copia fotostática de la misma, a fin de estar en posibilidad de dar la respuesta que corresponda al planteamiento de referencia.

Sin otro particular, le reitero mi consideración más distinguida.

INSTITUTO ELECTORAL DE TAMAULIPAS
IETAM
10:43 hrs
23 OCT 2024
RECIBIDO
DIR. DE TECNOLOGÍAS DE LA INFORM...

**ATENTAMENTE**

IETAM
INSTITUTO ELECTORAL DE TAMAULIPAS
UNIDAD DE TRANSPARENCIA

**LIC. NANCY MOYA DE LA ROSA**
**TITULAR DE LA UNIDAD DE TRANSPARENCIA**

C.c.p. Archivo

| | | |
|---|---|---|
| Reviso y Valido | NMDLR | |
| laboro | YBCW | |

**OFICIO N° ADMINISTRACIÓN/1479/2024**
Ciudad Victoria, Tamaulipas; a 24 de octubre de 2024



**LIC. NANCY MOYA DE LA ROSA**
**TITULAR DE LA UNIDAD DE TRANSPARENCIA DEL IETAM**
**PRESENTE**

Hago referencia a su oficio UT/449/2024, de fecha 23 de octubre del 2024, por el cual remite la solicitud de información formulada a través de la Plataforma Nacional de Transparencia; registrada con los folios siguientes:

| Día de la presentación | Folio Interno IETAM | Folio Plataforma Nacional de Transparencia |
|---|---|---|
| 22/10/2024 | UT/SIP/185/2024 | 280527624000186 |

Con la cual se requiere la información siguiente:

*"APARTADO 1*

*1. Informar si 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 si se cuenta con un inventario institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar si se ha desarrollado e implementado el plan 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 si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuando se implementó; h) informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar si se cuenta con un Equipo de Repuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.*

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

*4. Informar si se emplea la firma electrónica avanzada en la institución;*

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

*8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;*

*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: 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 si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información institucional por parte de los servidores públicos;*

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

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

*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; b) indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;*

*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; cuando se implementó.*

En relación al punto 2, respecto a la consulta siguiente: "*Informar si se cuenta con un inventario institucional de bienes y servicios de TIC",* me permito informar que la Dirección de Administración sí cuenta con inventario instituciona de bienes y servicio de TIC.

En cuanto a los demás puntos planteados, esta Dirección no posee la información solicitada, ya que no se encuentra dentro de su ámbito de competencia.

Sin otro particular, reciba un cordial saludo.

**ATENTAMENTE**

IETAM
INSTITUTO ELECTORAL DE TAMAULIPAS
DIRECCIÓN DE ADMINISTRACIÓN

**MTRA. IRILIANN YAZBETH NARVÁEZ WONG**
**DIRECTORA DE ADMINISTRACIÓN**

C.c.p.-Archivo.

| | | |
|---|---|---|
| Autorizó: | | |
| Validó: | IYNW | |
| Elaboró: | AEEL | |

**No. de Oficio: DTIC/SIP-008/2024**
Ciudad Victoria, Tamaulipas, a 28 de octubre de 2024

**LIC. NANCY MOYA DE LA ROSA**
**TITULAR DE LA UNIDAD DE TRANSPARENCIA**
**P R E S E N T E.-**

29 OCT 2024
Bernice 03:58

En respuesta a su oficio **UT/450/2024** mediante el cual solicita a esta Dirección se remita la información que obre en nuestros archivos, con respecto a la solicitud con Folio **280527624000186** misma que requiere se atienda y proporcionen diversos datos, los cuales mencionan de la siguiente manera:

*"APARTADO 1*
*1. Informar si 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 si se cuenta con una Inventario Institucional de bienes y servicios de TIC; e) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar si 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 si 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 diagnósticc de identificación de los procesos y activos esenciales de la Institución; 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.*
*3. Informar si 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) si es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia;*
*4. Informar si se emplea la firma electrónica avanzada en la institución;*
*5. Informar si 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 si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;*
*8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;*
*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: a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; e) 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 si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;*
*11. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;*
*12. Informar si 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 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."*

Por lo anterior, se informa que está Dirección de Tecnologías de la Información y Comunicaciones al respecto de los puntos anteriores tiene, realiza y/o atiende de la siguiente manera este tema:

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;
   **Respecto a este inciso, la totalidad de la información requerida no está dentro del marco de competencia de esta Dirección, salvo en lo referente al "marco de mejores prácticas aplicables a la gestión de las TIC", en cuyo caso no se ha estipulado marco alguno por parte de esta Dirección de Tecnologías de la Información y Comunicaciones.**
   c) un plan de continuidad de operaciones, y señalar la fecha de implementación;
   **No se cuenta con un plan de continuidad de operaciones.**
   d) Informar si se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;
   **No se cuenta con un plan de recuperación ante desastres.**
   e) desarrollado e implementado un programa de gestión de vulnerabilidades;
   **No sé a 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);
   **No se cuenta**
   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;
   **No se cuenta**
   h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;
   **No se cuenta**
   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.
   **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;
**No se cuenta con una estrategia de ciberseguridad dentro de la institución.**

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

5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;
   **No se realizan simulacros**

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

7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;
   **Son propios.**

8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;
   **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:
   a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información;
   **No**
   *c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;*
   **Si**
   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;
   **Si**
   e) cuenta con cifrado en el envío de información.
   **No**

10. Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;
    **No se cuentan con mecanismos para evitar la divulgación no autorizada**

11. Informar sí la página web de la institución cuenta con:
    a) aviso de privacidad; **Si**

    b) certificados digitales vigentes; **Si**

12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos; **No, no se ha capacitado.**

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;
    **No**
    b) Indicadores que permitan medir la madurez institucional en la gestión de seguridad de la información;
    **No**

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 se cuenta con un programa de formación en la cultura de la seguridad de la información**

Sin otro particular por el momento, aprovecho la oportunidad para mandarle un cordial saludo.

A T E N T A M E N T E
"En Tamaulipas Todos Hacemos la Democracia"

**DR. MARIO HUMBERTO RODRÍGUEZ CHÁVEZ**
**DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES**

IETAM INSTITUTO ELECTORAL DE TAMAULIPAS
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

C.c.p.- Archivo

PLATAFORMA NACIONAL DE TRANSPARENCIA

PLATAFORMA NACIONAL DE TRANSPARENCIA

ITAIT
INSTITUTO DE TRANSPARENCIA, DE ACCESO A LA INFORMACIÓN Y DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE TAMAULIPAS

31/10/2024 16:12:25 PM

# NOTIFICACIÓN DE ENTREGA DE INFORMACIÓN VÍA PLATAFORMA

| | |
|---|---|
| Estimado(a): | |

En atención a la solicitud de información que presentó con los siguientes datos:

| | |
|---|---|
| Folio: | 280527624000186 |
| Fecha de presentación: | 22/10/2024 |
| Nombre del Solicitante: | |
| Sujeto Obligado: | Instituto Electoral de Tamaulipas (IETAM). |
| Información solicitada: | APARTADO 1<br>1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;<br>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.<br>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 ;<br>4. Informar sí se emplea la firma electrónica avanzada en la institución;<br>5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;<br>6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;<br>7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;<br>8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;<br>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.<br>10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;<br>11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;<br>12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;<br>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;<br>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. |

Con fundamento en lo dispuesto en la Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas y/o en la Ley de Protección de datos personales en posesión de sujetos obligados del Estado de Tamaulipas, la información solicitada ha sido entregada vía electrónica en la Plataforma Nacional de Transparencia.