

TEEN

**TRIBUNAL ESTATAL
ELECTORAL
DE NAYARIT**

Oficio número: TEE-INF-91/2024

Asunto: "El que se indica"

Tepic, Nayarit a 31 de octubre de 2024

Lic. Fernando Joel García Yáñez
**Titular de la Unidad de Transparencia del
Tribunal Estatal Electoral de Nayarit
PRESENTE**



Con fecha 31 de octubre de la presente anualidad, el área de comunicación, Informática y redes a cargo de la suscrita, recibí el oficio TEEN/UT/110/2024 emitido por el Titular de la Unidad de Transparencia de este Tribunal, mediante el cual se me informa respecto de la solicitud de información solicitada a este órgano jurisdiccional con folio "181669024000033" y en razón de la información solicitada, le corresponde al área de la cual soy Encargada dar respuesta a dicha solicitud.

Por lo que, para dar cumplimiento a la solicitud realizada, me permito responder a cada uno de los cuestionamientos en los términos siguientes:

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

Actualmente este Órgano no cuenta con un gobierno de seguridad de la información o ciberseguridad.

2.- Señalar si de conformidad con el acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021, se han implementado las siguientes medidas:

a) estándares técnicos definidos para la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios de seguridad de la información o de tecnologías de la información y comunicación

No se cuenta con la Coordinación de Estrategia Digital Nacional, por ende, no se han creado estándares técnicos

b) 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

Si se cuenta con un inventario institucional de bienes y servicios de TIC



El presente documento es una copia de la información pública que se encuentra en el portal de transparencia de la Unidad de Transparencia.

Con fecha 31 de octubre de 2024, se recibió la solicitud de acceso a la información pública de la Unidad de Transparencia, en virtud de la Ley de Acceso a la Información Pública, para que se proporcionara la información solicitada.

Por lo tanto, se ha procedido a la entrega de la información solicitada, de acuerdo con lo establecido en la Ley de Acceso a la Información Pública.

La información solicitada se encuentra disponible en el portal de transparencia de la Unidad de Transparencia, en el siguiente enlace: [enlace]

En caso de que la información solicitada no se encuentre disponible en el portal de transparencia, se procederá a la entrega de la información solicitada, de acuerdo con lo establecido en la Ley de Acceso a la Información Pública.

La información solicitada se encuentra disponible en el portal de transparencia de la Unidad de Transparencia, en el siguiente enlace: [enlace]

En caso de que la información solicitada no se encuentre disponible en el portal de transparencia, se procederá a la entrega de la información solicitada, de acuerdo con lo establecido en la Ley de Acceso a la Información Pública.

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 ha desarrollado e implementado el plan de recuperación

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

No se ha desarrollado un sistema 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 con un marco de Gestión de Seguridad de la Información o sistema de Gestión de Seguridad de la Información

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.

No se cuenta con dicha política de seguridad

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

No se cuenta con un diagnóstico de identificación

i) Informar si se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC)

No se cuenta con un equipo de respuesta

3.- Informar si es que 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) cuales áreas participaron en la creación de dicha estrategia

No se cuenta con una estrategia, sin embargo, la plataforma que utilizamos para la pagina web cuenta con seguridad del sitio web

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

Hasta el momento no se ha empleado la firma electrónica avanzada

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

No se realizan simulacros

6.- Señalar si en la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información, de ha contado con el Dictamen Técnico favorable expedido por la CEDN, de conformidad con el acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021.

Si

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

No se cuenta con centros de datos

8.- Informar si se cuenta con un correo electrónico; 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**

Se cuentan con correos electrónicos que juegan el papel de ser institucionales, sin embargo, la extensión sigue siendo @Gmail para el manejo de estos, por ende, no se cuenta con la inserción de leyenda de confidencialidad

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

No se cuenta con un control institucional

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

No se cuenta con soluciones de filtrado para correo no deseado o correo no solicitado

e) Cuenta con cifrado en el envío de información

No se cuenta con cifrado

1.- Informar al superior jerárquico de los resultados de la investigación.

2.- Informar al superior jerárquico de los resultados de la investigación y de los resultados de la investigación.

3.- Informar al superior jerárquico de los resultados de la investigación y de los resultados de la investigación.

4.- Informar al superior jerárquico de los resultados de la investigación y de los resultados de la investigación.

5.- Informar al superior jerárquico de los resultados de la investigación y de los resultados de la investigación.

6.- Informar al superior jerárquico de los resultados de la investigación y de los resultados de la investigación.

7.- Informar al superior jerárquico de los resultados de la investigación y de los resultados de la investigación.

8.- Informar al superior jerárquico de los resultados de la investigación y de los resultados de la investigación.

9.- Informar si se cuentan con mecanismos para evitar la divulgación no autorizadas de datos o información institucional por parte de los servidores públicos

No se cuenta con mecanismos para evitar la divulgación

10.- Informar si la pagina web de la institución cuenta con:

a) aviso de privacidad

b) certificados digitales vigentes

La pagina web si cuenta con aviso de privacidad y certificados digitales SSL vigentes

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

Aún no se ha capacitado

12.- 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 se cuenta mecanismos de supervisión y evaluación

b) Indicadores que permitan medir la madurez institucional en la gestión de seguridad de información

No se cuenta con indicadores para medir la madurez institucional

13.- 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 y cuantas horas de capacitación en ciberseguridad se realizan de forma anual.

No se cuenta con ningún programa de formación

14.- Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados se cuenta con un sistema de gestión de protección de datos personales, en caso de ser afirmativa esa pregunta ¿desde cuando se adoptó y cuáles áreas participaron en su desarrollo e implementación?

No se cuenta con un sistema de gestión de protección de datos personales

15.- Informar si se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó, lo anterior en términos de lo establecido por el artículo 40, 41 y 42 de la Ley General de Protección de datos personales en posesión de sujetos obligados (LGPDPPO)

No se cuenta con un modelo o sistema de comunicación

16.- Informar sobre si se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó, o anterior en términos de lo establecido por el artículo 40, 41 y 42 de la Ley general de protección de datos personales de sujetos obligados (LGPDPPO)

No se cuenta con un modelo o sistema de comunicación

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

Si se cuenta con lineamientos

18.- 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

iv. seguridad de la información

La dirección de administración cuenta con los currículum de todos los trabajadores o se encuentran en la pagina web de este Órgano.

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

No se ha suscitado una brecha de ciberseguridad

20.- Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son

No se han adoptado esquemas

21.- 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 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

No se cuenta con algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales

22.- Informas si se cuenta con documento de seguridad en materia de protección de datos personales

No se cuenta con documento de seguridad en materia de protección de datos personales

23.- Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de información

No se cuenta con un plan de comunicación

24.-Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución

Cada año

25.-Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad

El Órgano Interno de Control es el encargado de realizar auditorías, sin embargo desconozco si el área realiza las auditorías de seguridad.

26.-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. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización

No se cuenta con un help desk

27.- informar si se cuenta con un Centro de Operaciones de Ciberseguridad

Ademas informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles)

No se cuenta con un Centro de Operaciones de Ciberseguridad

No se han tenido incidentes de ciberseguridad

Sin más por el momento quedo a sus ordenes para cualquier duda y/o aclaración al respecto.

ATENTAMENTE

Ing. Lilian Michel Campos Aguirre
Área de comunicación, informática y redes del
Tribunal Estatal Electoral de Nayarit

El informe de la Comisión de la Verdad y la Reconciliación (CVR) es un documento de gran importancia que ha permitido conocer la verdad sobre los hechos ocurridos durante el conflicto armado interno en el Perú. Este informe es el resultado de un proceso de investigación que ha sido largo y complejo, pero que ha sido necesario para poder entender lo que realmente sucedió.

El informe de la CVR es un documento de gran importancia que ha permitido conocer la verdad sobre los hechos ocurridos durante el conflicto armado interno en el Perú. Este informe es el resultado de un proceso de investigación que ha sido largo y complejo, pero que ha sido necesario para poder entender lo que realmente sucedió.

El informe de la CVR es un documento de gran importancia que ha permitido conocer la verdad sobre los hechos ocurridos durante el conflicto armado interno en el Perú. Este informe es el resultado de un proceso de investigación que ha sido largo y complejo, pero que ha sido necesario para poder entender lo que realmente sucedió.

El informe de la CVR es un documento de gran importancia que ha permitido conocer la verdad sobre los hechos ocurridos durante el conflicto armado interno en el Perú. Este informe es el resultado de un proceso de investigación que ha sido largo y complejo, pero que ha sido necesario para poder entender lo que realmente sucedió.

El informe de la CVR es un documento de gran importancia que ha permitido conocer la verdad sobre los hechos ocurridos durante el conflicto armado interno en el Perú. Este informe es el resultado de un proceso de investigación que ha sido largo y complejo, pero que ha sido necesario para poder entender lo que realmente sucedió.

El informe de la CVR es un documento de gran importancia que ha permitido conocer la verdad sobre los hechos ocurridos durante el conflicto armado interno en el Perú. Este informe es el resultado de un proceso de investigación que ha sido largo y complejo, pero que ha sido necesario para poder entender lo que realmente sucedió.

El informe de la CVR es un documento de gran importancia que ha permitido conocer la verdad sobre los hechos ocurridos durante el conflicto armado interno en el Perú. Este informe es el resultado de un proceso de investigación que ha sido largo y complejo, pero que ha sido necesario para poder entender lo que realmente sucedió.

El informe de la CVR es un documento de gran importancia que ha permitido conocer la verdad sobre los hechos ocurridos durante el conflicto armado interno en el Perú. Este informe es el resultado de un proceso de investigación que ha sido largo y complejo, pero que ha sido necesario para poder entender lo que realmente sucedió.

1787-1788

El informe de la CVR es un documento de gran importancia que ha permitido conocer la verdad sobre los hechos ocurridos durante el conflicto armado interno en el Perú. Este informe es el resultado de un proceso de investigación que ha sido largo y complejo, pero que ha sido necesario para poder entender lo que realmente sucedió.