Oficio Núm. **IJLB/UT-121/2024**
Asunto: **Se da contestación a solictud de Información 182864624000016**
Tepic, Nayarit; 11 de noviembre de 2024.

C. Solicitante
nacidoel1deenero@gmail.com
P R E S E N T E

De conformidad con lo establecido en el artículo 124, 125 numeral 3, 140 y 141 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit (en adelante LTAIPEN), en atención a su solicitud de información recibida con fecha veintiuno de octubre del dos mil veinticuatro, a través de la Plataforma Nacional de Transparencia registrada con número de folio **182864624000016** dirigida a este sujeto obligado, en la cual solicitó:

APARTADO 1
1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
2. Señalar sí se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar 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 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 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 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 medirla efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir la 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. *(Sic)*.

- En atención a la información solicitada, me permito remitir a Usted, oficio de No. IJLBEN/IB/040/2024, signado por el Ingeniero Bryan Gilberto Hernández Montes, en su carácter de Titular del Departamento de Informática y Boletín del Instituto de Justicia Laboral Burocrática del Estado de Nayarit, mediante el cual remite respuesta a lo solicitado.

Sin más que agregar, espero dar respuesta a su solicitud de información registrada con número de folio 182864624000016, de conformidad a los artículos aplicables a la materia.

A T E N T A M E N T E

GOBIERNO DEL ESTADO DE NAYARIT 2021 - 2027 · INSTITUTO DE JUSTICIA LABORAL BUROCRÁTICA

LICENCIADA BRENDA LÓPEZ PARRA
TITULAR DE LA UNIDAD DE TRANSPARENCIA DEL INSTITUTO DE JUSTICIA LABORAL BUROCRÁTICA DEL ESTADO DE NAYARIT

c.c.p/archivo

No. Oficio: IJLBEN/IB/040/2024
Tepic, Nayarit; a 07 de noviembre de 2024

LICENCIADA BRENDA LÓPEZ PARRA
TITULAR DE LA UNIDAD DE TRANSPARENCIA DEL
INSTITUTO DE JUSTICIA LABORAL BUROCRÁTICA
DEL ESTADO DE NAYARIT
PRESENTE

Recibí
Brenda Parra
11/11/2024
11:35 am

Mediante la presente reciba un cordial saludo, aprovecho el medio para dar contestación a la solitud de información con numero de folio 182864624000016, recibida a través de la Plataforma Nacional de Transparencia y remitida a este departamento por medio del oficio IJLB/UT-120/2024 de fecha 22 de octubre de 2024.

La cual a la letra dice:

APARTADO 1

1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;

2. Señalar sí se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar sí se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.

3. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia;

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

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

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

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

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

9. Informar sí se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información.

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

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

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

13. Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medirla efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir la 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. (Sic).

Las repuestas se ordenan de acuerdo a la numeración de la cuestión y el inciso que corresponde.

1.- Actualmente no se cuenta con una comisión de seguridad informática.

2.-

a) Se siguen los procesos establecidos por el Instituto de Adquisiciones, Arrendamientos y Prestaciones de Servicios del Estado de Nayarit.

b) Si se cuenta con un inventario.

c)Se cuenta con un plan Institucional de Tecnologías de la Información el cual comenzó a desarrollarse.

d) No se ha desarrollado, por ende no se ha implementado.

e) No se ha desarrollado dicho plan.

F) No se cuenta con el MGSI ni el SGSI.

g) No se cuenta con una política de seguridad.

h) Aún no se realiza un diagnóstico pero se trabajará en ello.

i) No se cuenta con ello.

3.- No se cuenta con ninguna estrategia.

4.- Si se emplea la firma electrónica avanzada.

5.- No se realizan simulacros.

6..- No se cuenta con lineamientos

7.- No contamos con un centro de datos.

8.- No se cuenta con dichos lineamientos.

9.- Si se cuenta con correo institucional.

a) no cuanta con la inserción.
c) No se tiene control total sobre los correos institucionales.
D) Solo las establecidas por los clientes de correo electrónico.
f) No se cuenta con cifrado.
10.- No se cuenta con esos mecanismos.
11.-
a) No se cuenta con ello.
b) si se tiene el certificado vigente.
12.- No se ha capacitado.
13.- no se cuenta con ningún tipo de evaluación.
14.- No se cuenta con ello.

Sin otro particular quedo a sus órdenes reiterándole mis saludos.

ATENTAMENTE

GOBIERNO DEL ESTADO DE NAYARIT 2021 - 2027
INSTITUTO DE JUSTICIA LABORAL BUROCRÁTICA

ING. BRYAN GILBERTO HERNÁNDEZ MONTES
TITULAR DEL DEPARTAMENTO DE INFORMÁTICA Y BOLETÍN

C.c.p.- L.C. Víctor Manuel Sandoval Muro. - Director de Administración
C.c.p.- Archivo