

MEMORÁNDUM

DIRIGIDO A: Lic. Mario Rodrigo Escalante Galaz/ Titular de la Unidad de Transparencia del Instituto Estatal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de Yucatán.

DE: Mtra. Sindy Jazmín Góngora Cervera/ Directora de Asuntos Jurídicos y Plenarios

FECHA: 28 de octubre de 2024.

MEMORÁNDUM NO.: DAJP. 060/2024.

ASUNTO: Se contesta solicitud 310586824000203.

En atención a la solicitud de información, con número de folio 310586824000203, recibida el 18 de octubre de 2024, remitida a esta Unidad Administrativa el 22 del mismo mes de octubre de 2024, a través de la cual requieren lo siguiente: *"...A quien corresponda: Por la presente, y en virtud de lo establecido en la Ley General de Transparencia y Acceso a la Información Pública Gubernamental, solicito de manera formal el acceso a la siguiente información: Que mecanismos de seguridad usan para garantizar la seguridad de la información que resguardan, como manejan los recursos públicos para que esa seguridad sea aplicada en su dependencia. De igual manera como destinan y usan esos recursos en temas de seguridad en el ámbito digital. Agradezco de antemano su atención a esta solicitud y quedo atenta a su pronta respuesta. De acuerdo con el artículo 124 de la ley mencionada, espero recibir la información solicitada lo antes posible. Atentamente:..."* (Sic.) me permito manifestar lo siguiente:

Con relación a *"Que mecanismos de seguridad usan para garantizar la seguridad de la información que resguardan"*. (Sic.) se informa al particular que después de haber realizado una búsqueda exhaustiva se encontró que para proteger los servidores institucionales contra los ataques cibernéticos, accesos no autorizados, filtraciones de datos y otros problemas de seguridad, se tienen implementado las siguientes:

Medidas de seguridad en el servidor web en AWS:

- Controles de acceso segregados y privilegios limitados por proceso, garantizando que cada usuario y sistema tenga acceso solo a lo que necesita.
- Contraseñas con política de seguridad de complejidad mínima de 256-bits.
- Copias de seguridad, una almacenada en la nube y otra en las instalaciones locales, lo que brinda una capa adicional de seguridad en caso de fallos o ataques.
- Instalación de actualizaciones de seguridad del sistema operativo.

Medidas de seguridad implementadas en el servidor de archivos local:

- Cuentas de usuario con acceso limitado a las carpetas autorizadas.
- Contraseñas con política de seguridad de complejidad mínima de 256-bits.
- Antivirus.
- Exposición aislada del internet para evitar ataques externos.

Se cuenta con un firewall de red como medida para una segura navegación en internet con los equipos de cómputo institucionales.

De igual forma la Coordinación de Tecnologías de la Información y Administración de Sistemas realiza las siguientes acciones de seguridad:

- Respaldo de los proyectos y aplicaciones en desarrollo.
- Respaldo de las bases de datos y archivos de las aplicaciones web.
- Respaldo de las bases de datos de los programas contables.
- Respaldo de la información generada en la intranet del Instituto.
- Revisión mensual de la integridad de los archivos en los respaldos institucionales.
- Revisión mensual de los registros de seguridad en el servidor web, de archivos, firewall, proxy y active directory institucionales.
- Agregar nuevos sitios de monitoreo/spyware a las listas de bloqueo para mejorar seguridad de la red Institucional.

Así mismo con la finalidad de proteger contra daño, pérdida y/o destrucción de la información generada y resguardada por este Instituto ante cualquier evento catastrófico que pueda presentarse, se implementa el Plan de Recuperación de Desastres el cual provee un conjunto de soluciones efectivas y/o recomendaciones que son utilizadas para reducir el impacto del desastre en la operación del instituto y garantizar la confidencialidad, integridad y disponibilidad de la



información; mismo que se envía como documento anexo a este requerimiento y que se encuentra publicado en la página oficial en la siguiente liga:
<https://www.inaipyucatan.org.mx/Transparencia/portals/0/pdf/reglamentoleyes/PlanRecuperacionDesastres.docx>

En cuanto a “...como manejan los recursos públicos para que esa seguridad sea aplicada en su dependencia. De igual manera como destinan y usan esos recursos en temas de seguridad en el ámbito digital”. (Sic.) se informa que entre las acciones que involucran costo, llevadas a cabo para proveer de seguridad a la información generada y resguardada por este Instituto se encuentran las siguientes:

- Renta del servidor web en AWS
- Pago de Licenciamiento del ESET EndPoint Antivirus
- Se adquirió el siguiente equipo:

| Cantidad | Equipo |
|----------|---|
| 1 | Servidor IBM X3250 M4 |
| 1 | Servidor HP PROLIANT ML-350 G6 |
| 1 | Sistema de Almacenamiento SYNOLOGY RS2211 |
| 8 | Disco duro WD 2tb, SATA 3 6Gbs 64Mb 7200rpm |

Sin embargo, cabe mencionar que los costos relacionados con lo antes mencionado, le competen a la Dirección de Administración, Finanzas y Recursos Humanos.

Sin más por el momento, me despido de usted, no sin antes agradecer la atención brindada al presente, le envío un cordial saludo y quedo a sus órdenes para cualquier duda y/o aclaración.

ATENTAMENTE

(RÚBRICA)

MTRA. SINDY JAZMÍN GÓNGORA CERVERA
DIRECTORA DE ASUNTOS JURÍDICOS Y PLENARIOS