

## Registro de Solicitud

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

Acuse de Recibo No.:	261271924000460
Solicitante o Razón Social:	
Representante Legal:	
Número de Folio:	261271924000460
Fecha de ingreso de la Solicitud:	24/10/2024
Fecha Oficial de Recepción:	24/10/2024
Unidad de Atención:	Supremo Tribunal de Justicia del Estado de Sonora
Información Solicitada:	<p>APARTADO 1</p> <ol style="list-style-type: none"> <li>1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;</li> <li>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; 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 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.</li> <li>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 ;</li> <li>4. Informar si se emplea la firma electrónica avanzada en la institución;</li> <li>5. Informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;</li> <li>6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;</li> <li>7. Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;</li> <li>8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;</li> <li>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.</li> <li>10. Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;</li> <li>11. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;</li> <li>12. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;</li> <li>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;</li> <li>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.</li> </ol>
Correo electrónico.	
Forma de Entrega de la Solicitud:	Sistema de Solicitudes de Información de la Plataforma Nacional de Transparencia
Usuario que Elaboró la Solicitud:	nacidoel1deenero@gmail.com

## Registro de Solicitud

Para efecto del cómputo establecido en el Artículo 129 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sonora, se ha recibido su Solicitud con fecha: 24/10/2024.

En virtud de que su Solicitud fue presentada a través de la Plataforma Nacional de Transparencia, y haber aceptado los términos y condiciones del mismo, se entiende que las notificaciones y la respuesta que se formulen en atención a la misma, se pondrán a su disposición en los plazos establecidos en la Ley, por el mismo medio, el cual deberá consultar para dar seguimiento a su Solicitud.

Conforme se establece en el Artículo 124 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sonora, dentro de un plazo de 5 días hábiles contados a partir de la Recepción de su Solicitud, se le informará sobre la aceptación, improcedencia o declinación de la misma.

El seguimiento a su Solicitud deberá realizarlo directamente en la Unidad de Transparencia, competente, mediante el número de folio que se indica en este acuse.

Se recomienda conservar el presente Acuse para fines informativos y/o aclaraciones.

A T E N T A M E N T E  
TITULAR DE LA UNIDAD DE TRANSPARENCIA  
Supremo Tribunal de Justicia del Estado de Sonora