

FORMULARIO PARA DOCUMENTAR UNA BUENA PRÁCTICA DE LA ADMINISTRACIÓN PÚBLICA ESTATAL

I. Datos de identificación de la práctica

1.1. Nombre	Sistema de Gestión de Seguridad de la Información basado en la Norma Internacional ISO_IEC 27001			
1.2. Población usuaria	Personas adultas mayores	<input type="checkbox"/>	1.3. Ámbito de aplicación	
	Mujeres	<input type="checkbox"/>		
	Niñez	<input type="checkbox"/>	Estatal <input checked="" type="checkbox"/>	
	Jóvenes	<input type="checkbox"/>	Municipal <input type="checkbox"/>	
	Personas migrantes	<input type="checkbox"/>		
	Personas con discapacidad	<input type="checkbox"/>		
	Personas servidoras públicas	<input checked="" type="checkbox"/>		
	Personas empresarias	<input type="checkbox"/>		
	Comunidad estudiantil	<input type="checkbox"/>		
	Personas agroproductoras	<input type="checkbox"/>		
Otro	<input type="checkbox"/>			
	¿Cuál?			
1.4. Categoría	Atención Ciudadana	<input type="checkbox"/>		
	Mejora de la Gestión Pública	<input type="checkbox"/>		
	Transparencia y Rendición de Cuentas	<input type="checkbox"/>		
	Auditoría, Control y Evaluación	<input type="checkbox"/>		
	Compras Gubernamentales	<input type="checkbox"/>		
	Combate a la Corrupción	<input type="checkbox"/>		
	Recursos Humanos	<input type="checkbox"/>		
	Participación Ciudadana y Contraloría Social	<input type="checkbox"/>		
	Responsabilidades	<input type="checkbox"/>		
	Tecnologías de la información	<input checked="" type="checkbox"/>		
	Legislación y Normatividad	<input type="checkbox"/>		
Bienes Patrimoniales	<input type="checkbox"/>			
1.5. Año en que inició a operar la práctica	2020-01-07			
1.6. Dirección electrónica y redes sociales donde se difunde la práctica	Página web:	https://ifrem.edomex.gob.mx/		
	Facebook:			
	Twitter:			

II. Información de la práctica

2.1. ¿En qué consiste la práctica?	<p>El Instituto de la Función Registral del Estado de México (IFREM) a través de la Unidad de Informática reconoce la importancia de proteger sus activos de información, ya que resguarda bases de datos con información sensible de la población usuaria que gestiona servicios de publicidad a la situación jurídica de los bienes y derechos, así como a los actos y hechos jurídicos que conforme a la Ley deban registrarse para surtir efectos contra terceros, mediante la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), el cual se encuentra certificado con el número de registro IS 717661 otorgado por la compañía BSI Group; mismo que opera eficientemente a través de la identificación continua de riesgos de seguridad de la Información y la implementación de controles para minimizarlos, fortaleciendo los valores y el compromiso de sus colaboradores para lograr los objetivos estratégicos del Instituto. De esta manera se garantiza la continuidad y disponibilidad de los trámites y servicios Registrales y Notariales soportados por las TIC.</p>
2.2. ¿Qué problemática o necesidad se resuelve con la implementación de la práctica?	<p>Evitar la divulgación, modificación, utilización o destrucción no autorizada de la información, a través de la identificación continua de riesgos de seguridad de la Información y la implementación de controles para minimizarlos, a fin de proveer la seguridad de la información en los trámites que ofrece el IFREM, mediante los procesos que se ejecutan en la Unidad de Informática.</p>
2.3. Objetivo general de la práctica	

Establecer las directrices y principios que regirán el modo en que la Unidad de Informática del IFREM gestionará y protegerá su información, a través de la implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001.

2.4. Describir los elementos sobresalientes e innovadores de la práctica

Los 114 controles recomendados por la Norma Internacional ISO/IEC 27001:2013, haciendo uso de las Tecnologías de la Información y Comunicación (TIC) para el establecimiento de políticas, procedimientos, directrices, recursos y actividades asociados a mantener la confidencialidad, integridad y disponibilidad de la información.

2.5. ¿Cómo contribuye la práctica en la mejora de los procesos, trámites y servicios de la Administración Pública Estatal

Proveer seguridad en la información; generar confianza en las y los usuarios al saber que sus datos están protegidos.

2.6. ¿Cuáles son los elementos de Gobierno Electrónico utilizados en la operación de la práctica?

Nivel de gestión de seguridad de la información, a través de un esquema, entendiéndose como un "Esquema de gestión de riesgos", el cual es una herramienta que identifica actividades o procesos sujetos a riesgos, y se lleva a cabo el análisis de riesgos, a fin de garantizar la confidencialidad, integridad y disponibilidad de las operaciones críticas del instituto soportadas por tecnología.

2.7. ¿Existen prácticas similares implementadas en otras dependencias de la Administración Pública Estatal o instancias de otros gobiernos?

Sí		¿Dónde?
No	X	

2.8. Ventajas competitivas de la práctica

Ventajas competitivas que tiene la práctica que se documenta en relación con otras similares	Ventajas que tienen otras prácticas similares
Proteger todas las bases tecnológicas de información del instituto a través de la identificación continua de riesgos de seguridad de la información implementando controles para minimizarlos, garantizando la disponibilidad de los trámites y servicios registrales y notariales soportados en las TIC.	No se tiene registro de prácticas similares.

2.9. Operación de la práctica

¿Cuál es el procedimiento antes de implementarla?	¿Cuál es el procedimiento después de implementarla?
Se contaban con buenas prácticas de seguridad de la información; sin embargo, no se hacía en estricto apego a la Norma Internacional ISO/IEC 27001, la cual proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.	Se gestionan diferentes controles aplicados, estos son los establecidos en el "Anexo A de la Norma ISO/IEC 27001:2013" como políticas, procedimientos, directrices, recursos y actividades asociados a mantener la seguridad de la información en cada una de las fases del ciclo de vida de un trámite o servicio proporcionado por el instituto, mediante dos principales procesos que pertenecen a la Unidad de Informática: Desarrollo de Aplicaciones Informáticas y Soporte Técnico a Infraestructura de Redes y Comunicación.

2.10. ¿Se han realizado mejoras significativas a la práctica?

Sí	X	No	
----	---	----	--

¿Por qué no se han realizado mejoras?

2.11. Mejoras realizadas a la práctica

Acciones ejecutadas	Resultados alcanzados con las mejoras realizadas a la práctica
De manera permanente se contempla la mejora continua mediante una gestión de riesgos que se realiza de manera frecuente, con el objetivo de fortalecer los controles, las políticas y los procedimientos del SGSI y se garantiza la confidencialidad, integridad y disponibilidad de la información, dando cumplimiento a los objetivos del SGSI.	En el año 2022, se capacitó al 90 % del personal de la Unidad de Informática en materia de Seguridad de la Información. Se mantuvo la eficacia de atención a incidentes de Seguridad de Información al 100 %. Se aseguró el cumplimiento del 100 % de las pólizas de mantenimiento preventivo y correctivo contratadas. Se garantizó la funcionalidad de los sistemas operacionales en más del 99 %.

2.12. Fecha en la que se realizó la última mejora

2022-09-13

III. Fundamento jurídico y/o administrativo de la práctica

3.1. ¿La implementación de la práctica se sustenta en ordenamiento(s) jurídico(s)-administrativo(s)?

Sí	X	No	
----	---	----	--

En caso de ser afirmativo, señalar el(los) fundamento(s) de la práctica

Tipo de ordenamiento	Nombre del ordenamiento
----------------------	-------------------------

Ordenamiento(s) jurídico(s)	Ley de Protección de Datos Personales del Estado de México, art. 38, publicada en el Periódico Oficial "Gaceta del Gobierno" el 30 de mayo de 2017. Ley de Gobierno Digital del Estado de México y Municipios, artículos 10,15,17, 46, 58, 70 y 72, publicada en el Periódico Oficial "Gaceta del Gobierno" 6 de enero de 2016. Reglamento de la Ley de Gobierno Digital del Estado de México y Municipios, art. 40, publicada en el Periódico Oficial "Gaceta del Gobierno" el 23 de agosto de 2019.
Ordenamiento(s) administrativo(s)	Manual General de Organización del Instituto de la Función Registral del Estado de México, publicado en el Periódico Oficial "Gaceta del Gobierno" el 03 de noviembre de 2014. Manual de Procedimientos de la Unidad de Informática del Instituto de la Función Registral del Estado de México, publicado en el Periódico Oficial "Gaceta del Gobierno" el 04 de agosto de 2016.
Vinculación con el Plan de Desarrollo del Estado de México 2017-2023	
Pilar / Eje transversal	Pilar Seguridad. Estado de México con Seguridad y Justicia
Estrategia	Fortalecer el uso de las Tecnologías de Información y Comunicación para la Seguridad.
Línea de Acción:	Fomentar la construcción e implementación del Sistema de Información Oportuna en Seguridad.
En caso de ser negativo, mencionar ¿Por qué la práctica no cuenta con fundamento?	
3.2. ¿La práctica se encuentra documentada?	Sí <input type="checkbox"/> X <input checked="" type="checkbox"/> No <input type="checkbox"/>
En caso de ser afirmativo, señalar la documentación de la que se dispone:	
Mapa de procesos	X
Manual de procedimientos	X
Guía técnica o metodológica	X
Otro	X ¿Cuál? Manual del Sistema de Gestión de Seguridad de la Información (SGSI).
En caso de ser negativo, indique ¿Por qué?	

IV. Medición y reconocimiento de la práctica

4.1. ¿Se realiza medición de la práctica?	Sí <input type="checkbox"/> X <input checked="" type="checkbox"/> No <input type="checkbox"/>
4.2. Metodología utilizada para medir la práctica	
Describa los siguientes recursos de medición:	
Frecuencia de medición	Trimestral.
Instrumento de medición	Mediante estadísticas y registros en los sistemas de información.
Elementos que se evalúan	Reportes de incidencias, seguimiento de proyectos e indicadores de capacitación.
Indicador(es) aplicado(s) para conocer los resultados alcanzados con la implementación de la práctica	Se realiza mediante estadística y reporte; obteniendo capacitación del 80 % del personal de la Unidad de Informática en materia de Seguridad de la Información (Asistencia a las capacitaciones). Atención a incidentes de Seguridad de Información al 80 %, se realiza mediante reporte. Cumplimiento del 85 % de las pólizas de mantenimiento preventivo y correctivo contratadas. Se garantiza la funcionalidad de los sistemas operacionales 80 %. Se verifica mediante reporte. NOTA: Derivado de la certificación en ISO/IEC 27001 (Certificado No. IS 717661 otorgado por BSI Group) con que cuenta el Instituto de la Función Registral del Estado de México (IFREM) a través de la Unidad de Informática, la información referida se encuentra clasificada como confidencial, ya que su divulgación pudiera representar un riesgo de seguridad para el instituto.
4.3. ¿Se mide la satisfacción de la población usuaria en relación con la implementación de la práctica?	Sí <input type="checkbox"/> <input type="checkbox"/> No <input type="checkbox"/> X <input checked="" type="checkbox"/>
En caso afirmativo, indicar de qué manera se mide	
4.4. ¿La práctica está certificada bajo un estándar?	Sí <input type="checkbox"/> X <input checked="" type="checkbox"/> No <input type="checkbox"/>
En caso de ser afirmativo, mencionar los siguientes datos:	

Norma o estándar	ISO/IEC 27001:2013 Sistemas de gestión de seguridad de la información. Es un reconocido marco internacional de las mejores prácticas para un sistema de gestión de seguridad de la información.			
Fecha de certificación	2020-01-07			
Institución certificadora	BSI Group			
4.5. ¿La práctica ha recibido algún reconocimiento?	Sí	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
En caso de ser afirmativo, mencionar los siguientes datos:				
Fecha en que recibió el reconocimiento	2021-03-25			
Sector que otorga el reconocimiento	Público	<input type="checkbox"/>	Privado	<input checked="" type="checkbox"/>
Institución que emite el reconocimiento	El primero otorgado por: U-Gob, Segundo reconocimiento otorgado por CIO México en octubre-2022; Tercer reconocimiento otorgado por CyberSecurity Awards 2022 en octubre- 2022.			
Tipo o categoría del reconocimiento	Seguridad de la Información.			
Carácter del reconocimiento	Internacional	<input type="checkbox"/>	Nacional	<input type="checkbox"/>
		<input checked="" type="checkbox"/>	Estatal	<input type="checkbox"/>
			Municipal	<input type="checkbox"/>
			Institucional	<input type="checkbox"/>

V. Transferencia de la práctica

5.1. ¿La práctica puede ser adoptada o transferible?	Sí	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
En caso de ser negativo, indique ¿Por qué?				
5.1.1 ¿La práctica ha sido transferida o adoptada por otro ámbito de gobierno?	Sí	<input type="checkbox"/>	No	<input checked="" type="checkbox"/>
En caso de ser afirmativo, señalar a quién se ha trasferido:				
Ámbito de gobierno		Nombre		
Federación	<input type="checkbox"/>			
Estados	<input type="checkbox"/>			
Municipios	<input type="checkbox"/>			
Dependencias u organismos auxiliares	<input type="checkbox"/>			
Organismos autónomos	<input type="checkbox"/>			
5.2. ¿Qué nivel de transferencia es permisible?	Total	<input type="checkbox"/>		
	Parcial	<input type="checkbox"/>		
	Asesoría o transferencia de conocimiento	<input checked="" type="checkbox"/>		
	Apoyo técnico	<input type="checkbox"/>		
5.3. En caso de ser transferible, ¿Qué se requiere?				
Gestión administrativa	Solicitar a través de oficio dirigido a la persona titular de la Unidad de Informática del Instituto de la Función Registral del Estado de México, indicando el interés de la transferencia, para que se establezcan los por menores de la práctica en comento.			
Normatividad aplicable	ISO/IEC 27001:2013 Sistemas de Gestión de Seguridad de la Información.			
Recursos tecnológicos	Se definen de acuerdo al número de controles establecidos en el Anexo A de la Norma ISO/IEC 27001:2013, a implementar derivados del análisis de riesgos de seguridad de la información. Computadoras, internet, en básico, porque ello, dependerá de los controles que se necesita y que están establecidos en la propia norma.			
Recursos materiales	Se definen de acuerdo al número de controles establecidos en el Anexo A de la Norma ISO/IEC 27001:2013, a implementar derivados del análisis de riesgos de seguridad de la información. Escritorios, sillas, en básico, porque ello, dependerá de los controles que se necesita y que están establecidos en la propia norma.			
Recursos humanos	Personal certificado en materia de Tecnologías de la Información, Auditoría y Seguridad de la Información.			

VI. Resultados obtenidos con la implementación de la práctica

6.1. Período de resultados reportados:	de	2022-01-01	al	2022-10-03
6.2. ¿En qué porcentaje se cumplió el objetivo de la práctica?	100%			
6.3. Meta programada en el período reportado	Asegurar al 100% la confidencialidad e integridad de los datos y de la información, así como de los sistemas.			
Resultados				
6.4. Cualitativos	Seguridad de la información y de los sistemas. Se ha logrado proteger la información a través de mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27001, dando seguimiento y buen resultado reflejado en las auditorías.			

6.5. Cuantitativos	En el año 2022, se capacitó al 90 % del personal de la Unidad de Informática en materia de Seguridad de la Información. Se mantuvo la eficacia de atención a incidentes de Seguridad de Información al 100 %. Se aseguró el cumplimiento del 100 % de las pólizas de mantenimiento preventivo y correctivo contratadas. Se garantizó la funcionalidad de los sistemas operacionales en más del 99 %. Se maneja en porcentaje, porque las capacitaciones se realizan por el número de personas convocadas, siendo diferente el quórum de personas en cada capacitación, por tal motivo no se podría realizar por número de personas, si no más bien por porcentaje como se refiere. Por tal motivo, no se podría realizar por número de personas, si no más bien por porcentaje como se refiere.
6.6. Evidencia gráfica	

VII. Datos de la Secretaría u Organismo Auxiliar responsable de administrar la práctica

7.1. Secretaría u Organismo Auxiliar	SECRETARÍA DE JUSTICIA Y DERECHOS HUMANOS		
7.2. Unidad administrativa responsable directa	INSTITUTO DE LA FUNCIÓN REGISTRAL DEL ESTADO DE MÉXICO		
7.2.1. Nombre de la persona titular responsable de la unidad administrativa responsable directa	Ing. José Antonio Hernández Flores		
7.2.2. Cargo	Jefe de la Unidad de Informática		
Teléfono 1	7222362909	Extensión 1	54016
7.3. Domicilio	Doctor Nicolás San Juan s/n, col. Ex Hacienda La Magdalena, C.P. 50010, Toluca, Estado de México.		
7.4. Correo electrónico	nancy.villegas@ifrem.gob.mx		
7.5. Nombre de la o del enlace	Mtra. Elva A. Juárez Vazquez		
7.5.1 Cargo	Enlace		
Teléfono 1	7222362909	Extensión 1	54012
7.5.2 Domicilio	Doctor Nicolás San Juan s/n, col. Ex Hacienda La Magdalena, C.P. 50010, Toluca, Estado de México.		
7.6. Correo electrónico	uni.modernizacion@ifrem.gob.mx		

Fecha de validación 2023-05-29