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		**1.3. Ámbito de aplicación**	Federal	
	Mujeres			Estatal	X
	Niñez			Municipal	
	Jóvenes				
	Personas migrantes				
	Personas con discapacidad				
	Personas servidoras públicas	X			
	Personas empresarias				
	Comunidad estudiantil				
	Personas agroproductoras				
	Otro		¿Cuál?		
1.4. Categoría	Atención Ciudadana				
	Mejora de la Gestión Pública				
	Transparencia y Rendición de Cuentas				
	Auditoría, Control y Evaluación				
	Compras Gubernamentales				
	Combate a la Corrupción				
	Recursos Humanos				
	Participación Ciudadana y Contraloría Social				
	Responsabilidades				
	Tecnologías de la información	X			
	Legislación y Normatividad				
	Bienes Patrimoniales				
1.5. Año en que inició a operar la práctica			2020-01-07		
1.6. Dirección electrónica y redes sociales donde se encuentra información de la práctica	Página web:		https://ifrem.edomex.gob.mx/		
	Facebook:				
	Twitter:				
	Otro:				

II. Información de la práctica

2.1. ¿En qué consiste la práctica?
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 protege 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.
2.2. ¿Qué problemática se resuelve a partir de la implementación de la práctica?

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 a través de la Unidad de Informática.

2.3. Objetivo general
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. Contribución de 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. Nivel de automatización de la práctica en las Tecnologías de la Información y Comunicación
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	
Ventajas competitivas que tiene la práctica que se documenta	Ventajas que tienen las otras prácticas

2.9. Operación de la práctica	
Procedimiento antes de implementarla	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 Sistema de Gestión de la Seguridad de la Información 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
De manera permanente se contempla la mejora continua mediante una gestión de riesgos que se realiza de manera permanente, 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 de seguridad de la información del SGSI.	Se capacitó al 80 % 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 en más del 80 %. Se aseguró el cumplimento del 100 % de las pólizas de mantenimiento preventivo y correctivo contratadas. Se garantizó la funcionalidad de los sistemas operacionales en más del 80 %.
2.12. Fecha en la que se realizó la última mejora	2020-08-31

III. Fundamento jurídico y/o administrativo de la práctica

3.1. ¿La implementación de la práctica se sustenta en ordenamiento(s) jurídico- 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 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 el 6 de enero de 2016. Reglamento de la Ley de Gobierno Digital del Estado de México y Municipios, art. 40, publicado el 23 de agosto de 2019.
Ordenamiento(s) administrativo(s)	Plan de Desarrollo del Estado de México 2017-2023n(Primera edición: Gobierno del Estado de México, 2018)

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. ¿El fundamento jurídico-administrativo que sustenta la práctica está vigente?	Sí	X	No		
3.3. ¿La práctica se encuentra documentada?	Sí	X	No		

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	X	No	
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	Capacitar al 80 % del personal de la Unidad de Informática en materia de Seguridad de la Información. Mantener la eficacia de atención a incidentes de Seguridad de Información al 80 %. Asegurar el cumplimento del 85 % de las pólizas de mantenimiento preventivo y correctivo contratadas. Garantizar la funcionalidad de los sistemas operacionales 80 %.

4.3. ¿Se mide la satisfacción de la población usuaria en relación con la implementación de la práctica?	Sí		No	X
En caso afirmativo, indicar de qué manera se mide				
4.4. ¿La práctica está certificada bajo un estándar?	Sí	X	No	

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	X	No	
En caso de ser afirmativo, mencionar los siguientes datos:				

Fecha en que recibió el reconocimiento	2021-03-25										
Sector que otorga el reconocimiento	Público							Privado	X		
Institución que emite el reconocimiento	El primero otorgado por: U-Gob, Segundo reconocimiento ortorgado 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		Nacional		Estatal	X	Municipal		Institucional		

V. Transferencia de la práctica

5.1. ¿La práctica es transferible?	Sí	X	No	
En caso de ser negativo, indique ¿Por qué?				
5.1.1 ¿La práctica ha sido transferida a otro ámbito de gobierno?	Sí		No	X
En caso de ser afirmativo, señalar a quién se ha trasferido:				

Ámbito de gobierno		Nombre
Federación		
Estados		
Municipios		
Dependencias u organismos auxiliares		
Organismos autónomos		

5.2. ¿Qué nivel de transferencia es permisible?	Réplica total	
	Réplica parcial	
	Asesoría o transferencia de conocimiento	X
	Apoyo técnico	

5.3. En caso de ser transferible, ¿Qué se requiere?	
Gestión administrativa	Contactar a la persona titular de la Unidad de Informática del IFREM, a través del correo: nancy.villegas@ifrem.gob.mx
Normatividad aplicable	ISO/IEC 27001:2013 Sistemas de gestión de seguridad de la información.
Recursos tecnológicos	Se definen de acuerdo al número de controles (Anexo A de la Norma ISO/IEC 27001:2013) a implementar, derivados del análisis de riesgos de seguridad de la información.
Recursos materiales	Se determinan con base en los controles (Anexo A de la Norma ISO/IEC 27001:2013) a implementar ,derivados del análisis de riesgos de seguridad de la información.
Recursos humanos	Personal certificado en materia de TI, Auditoría y Seguridad de la Información.

VI. Resultados obtenidos con la implementación de la práctica

6.1. Período de resultados reportados:	de	2021-01-17	al	2021-12-10
6.2. ¿En qué porcentaje se cumplió el objetivo de la práctica?	100%			
6.3. Meta inicial:	Asegurar 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
6.5. Cuantitativos	Capacitar al 80 % del personal de la Unidad de Informática en materia de Seguridad de la Información. Mantener la eficacia de atención a incidentes de Seguridad de Información al 80 %. Asegurar el cumplimento del 85 % de las pólizas de mantenimiento preventivo y correctivo contratadas. Garantizar la funcionalidad de los sistemas operacionales 80 %.
6.6. Resultados alcanzados con la aplicación de indicadores	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. Sin embargo, a efecto de contribuir con esta práctica, dicha información se podrá consultar con previa solicitud formal dirigida al titular de la Unidad de Informática.

6.7. 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	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	joseantonio.hernandez@ifrem.gob.mx		
7.5. Nombre de la o del enlace	Beatriz Ramírez González		
7.5.1 Cargo	Enlace		
Teléfono 1	7222362909	**Extensión 1**	54014
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	joseantonio.hernandez@ifrem.gob.mx		

Fecha de validación 2022-10-20