MATRIZ DE GESTIÓN DE RIESGOS

Código de Registro: UTSI/MR/01
Revisión registro: 02

Área responsable Unidad Técnica de Servicios Informáticos **Fecha del análisis** 12-ago-24 **Fecha de revisión de la SGC:** 12/08/2024 **Folio de actualización en el repositorio del SGCE** F2024-28

SECCIÓN 1 IDENTIFICACIÓN DE LOS RIESGOS							SECCIÓN 2 ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS										SECCIÓN 3 TRATAMIENTO DE LOS RIESGOS				
N°	Subproceso o actividad contenida en el programa integral respectivo (PIPEI, PIPP o PIEC), de ser el caso; o actividad sustantiva de la que se trata.	Clasificación del riesgo	Riesgo a evaluar	Descripción del riesgo que afecte o pueda afectar el logro de los resultados previstos y CAUSAS QUE ORIGINAN EL RIESGO	Consecuencias en caso de materializarse el riesgo	Parte (S) Interesada (S) Afectada (S)	PROBABILIDAD: ALTO (3)	PROBABILIDAD: MEDIO (2)	PROBABILIDAD: BAJO (1)	IMPACTO: ALTO (3)	IMPACTO: MEDIO (2)	IMPACTO: BAJO (1)	NIVEL DE RIESGO INICIAL (NRI)	CONTROLES EXISTENTES	EFECTIVIDAD DEL CONTROL: ALTO (3)	EFECTIVIDAD DEL CONTROL: MEDIO (2)	EFECTIVIDAD DEL CONTROL: BAJO (1)	NIVEL DE RIESGO RESIDUAL (NRR)	TRATAMIENTO A:ABY14O:X	ACCION (ES) PARA TRATAR LOS RIESGOS	FECHA DE INICIO (dd/mm/aa)	FECHA DE TÉRMINO (dd/mm/aa)	ÁREA RESPONSABLE DEL SEGUIMIENTO DE LA ACCIÓN
1	Mantenimiento preventivo	Operacionales	Falta de contratos de mantenimiento	Podría haber una deficiencia en los servicios y operación institutcional en temas informáticos, debido a la falta de actualización, limpieza y funcionalidad en los componentes que se encuentran en el centro de cómputo, en los racks de comunicaciones y cómputo que se encuentran con los usuarios, tales como equipos de seguridad, comunicación, telefonia, red inalambrica, cctv, bienes informáticos, aire acondicionado, energía de respaldo, sensores de temperatura, entre otros.	1.-Afectación a la continuidad operativa de las aplicaciones y sistemas que utilizan de las personas funcionarias del IECM en las actividades ordinarias y de proceso. 2.- Bajo rendimiento de la infraestructura de cómputo y comunicaciones.	1. Alta Dirección 2. Personas funcionarias del IECM			2			3	6	1. Contar con infraestructura de cómputo y comunicaciones de respaldo (nueva u obsoleta) en condiciones funcionales. 2. Contratos de mantenimiento preventivo y correctivo, así como pólizas de soporte en caso de ocurrir fallas en la infraestructura 3. Monitoreo de la infraestructura de servidores y equipos de telecomunicaciones para tomar acciones preventivas			2	2.2	Reducir riesgo	1. Contar con la infraestructura de cómputo y comunicaciones actualizada en licenciamiento, firmware y con un tiempo de vida menor a 5 años. 2. Dependencia del presupuesto institucional que se autorice e ir solicitando a la alta dirección la importancia de la adquisición de equipo se desactualice.	ene-25	dic-25	Dirección de Infraestructura
2	Mantenimiento preventivo	Tecnológicos	Falta de actualización de cableado, telefonía, licenciamiento y servicio de Internet.	Si algún componente de redes, telefonia, enlaces de internet o liciamiento fallará porque están desactualizados o en mal estado, es decir, cables rotos o mal conectados, licenciamiento no vigente ni en su última versión, sin la renovación del servicio de internet principal o de respaldo.	1. Afectación en la correcta disponibilidad de los sistemas y aplicaciones que utilizan las personas funcionarias del IECM, tanto en la operación ordinaria como en los procesos electorales y de participación ciudadana. 2. Bajo rendimiento de aplicativos y servicios.	1. Alta Dirección 2. Personas funcionarias del IECM			2			2	4	1. Realizar la actualización de la infraestructura básica. 2. Contar con cableado, telefonía, licenciameinto y servicios de Internet actualizados y que esten vigentes por el año de vigencia del tratamiento del riesgo. 3. Contar con cables y telefonos de respaldo (nuevos u obsoletos) en condiciones funcionales. 4. Monitoreo en los servicios de comunicaciones.			3		Nivel de riesgo aceptable (NRA)				
3	Mantenimiento preventivo	Tecnológicos	Falla en infraestructura central.	La falta de respuesta hacia la operación Institucional debido a que el equipo de cómputo, de comunicación o de seguridad tendran una desconexión no controlada, falta de energía, incendio o falla de algún componente físico interno de la infraestructura que se encuentra en el centro de cómputo del Instituto.	Genera una falta de atención de peticiones, afecta directamente en los tiempos de respuesta y de disponibilidad en los sistemas y aplicaciones que utilizan las personas funcionarias del IECM que operan en la dentro del centro de cómputo o infraestructura central del Instituto.	1. Alta Dirección 2. Personas funcionarias del IECM			2			2	4	1. Sistemas que se encuentran operando en la nube para mantener la continuidad operativa. 2. Servicios contratados en la nube como son correo electrónico, almacenamiento, DNS, Certificados, seguridad. 3.Centralización de los sistemas informáticos para su acceso desde Internet (Proxy). 4. Monitoreo los servicios del centro de cómputo (sensores de temperatura, servidores).			3		Nivel de riesgo aceptable (NRA)				

4	**Desarrollo de Sistemas Informáticos**	**Tecnológicos**	**Falta de mantenimiento y/o actualización a los sistemas.**	Operación deficiente de los sistemas ya que no entregaría el resultado esperado para la continuidad operativa en las actividades ordinarias y de proceso.	Afectación en los flujos esperados de los sistemas que utilizan de las personas funcionarias del IECM para cumplir con las actividades ordinarias y de proceso.	1. Alta Dirección 2. Personas funcionarias del IECM	**2**	**1**	**2**	1. Seguimiento de los requerimientos de mantenimiento y/o actualización de los sistemas de las diferentes áreas del Instituto, de acuerdo a las actividades Institucionales. 2. Se cuenta con el inventario de sistemas para su mantenimiento y/o actualización. 3. Actualización de los sistemas de apoyo a la operación, administrativos y de participación ciudadana.	**2**	**0.7**	**Nivel de riesgo aceptable (NRA)**				
5	**Desarrollo de Sistemas Informáticos**	**Tecnológicos**	**Obsolescencia tecnológica en los sistemas**	Operación deficiente de los sistemas debido a que los sistemas operativos o software de desarrollo sean tecnologías de más de 3 años en el mercado y no han sido actualizadas o renovadas por lo que generan un desempeño deficiente o vulnerabilidades de seguridad y de funcionalidad en comparación con nuevas tecnologías	Afectación en los sistemas que utilizan de las personas funcionarias del IECM ya que se puede presentar lentitud o perdida de información por vulnerabilidades de seguridad o funcionalidad, presentadas al ser tecnología obsoleta.	1. Alta Dirección 2. Personas funcionarias del IECM	**1**	**3**	**3**	1. Contar con la tecnología de sistemas actualizada en licenciamiento y parches en su última versión. 2. Contar con respaldos del aplicativo/sistema y bases de datos en su última versión. 3. Se realiza la migración de sistemas a nuevas tecnologías de bases de datos.	**2**	**1.1**	**Nivel de riesgo aceptable (NRA)**				
6	**Desarrollo de Sistemas Informáticos**	**Operacionales**	**Falta de mantenimiento a los sistemas y aplicaciones para la operación ordinaria, de Proceso Electoral y de Participación Ciudadana.**	Operación deficiente de los sistemas y aplicaciones para la operación ordinaria, de proceso electoral y de participación ciudadana debido a que el área solicitante o el área de desarrollo no llegará a solicitar o realizar las actualizaciones o modificaciones, así como la implementación de nuevos flujos operativos o la eliminación de funcionalidades para cumplir con ley vigente y las necesidades institucionales.	Afectación en los flujos esperados, falta de acceso o disponibilidad de los sistemas y aplicación para la operación ordinaria, de proceso electoral y de paticipación ciudadana que utilizan las personas funcionarias del IECM para cumplir con las actividades de proceso.	1. Alta Dirección 2. Personas funcionarias del IECM	**2**	**2**	**4**	1. Seguimiento de los requerimientos de actualizaciones a los sistemas pre-electorales o de consulta de acuerdo a las actividades Institucionales. 2. Se cuenta con el inventario y respaldos de sistemas pre-electorales o de consulta para su actualización. 3. Se realiza el mantenimiento de los sistemas de preparación de la elección o la consulta.	**3**	**1.5**	**Nivel de riesgo aceptable (NRA)**				

7	Desarrollo de Sistemas Informáticos	Operacionales	Falta o fuera de tiempo, de la definición de funcionalidades en los sistemas por parte de los usuarios de negocio o la Ley.	Se incumple o se atrasan los resultados en la operación Institucional, debido a que el área de desarrollo reciba de forma incompleta o a destiempo las solicitudes de nuevas funcionalidades, cambios dentro de la aplicación existente o los requerimientos de nuevos sistemas; de igual forma si las funcionalidades definidas en un sistema que va a entrar en operación depende de cambios en las Leyes, puede provocar redefinición en las funcionalidades de forma tardía.	1. Se generan atrasos en la entrega de sistemas. 2. Sistemas ineficientes por falta de prueba y simulacros por tiempo recortados. 3. Afecta la operación continua de las actividades institucionales que esten relacionadas con el desarrollo de los sistemas nuevos o modificados.	Alta Dirección	2	2	4	1. Seguimiento y atención inmediata a los requerimientos de sistemas de las áreas. 2. Acceso inmediato a la normativa cuando esta es modificada o actualizada, correspondiente a las actividades institucionales que afectan los diferentes sistemas del IECM. 3. Dar seguimiento a los requerimientos de sistemas y retroalimentación de los usuarios de negocio para cumplir con los objetivos Institucionales en tiempo y forma.	3	0.1	Nivel de riesgo aceptable (NRA)				
8	Desarrollo de Sistemas Informáticos	Operacionales	Falta del Sistema de Administración de Servicios	Si el equipo informático que contiene la aplicación deja de funcionar o por otro lado, la aplicación por falta de mantenimiento y parches del sistema operativo, deja de operar el sistema no permitiendo el registro y seguimiento a incidentes y servicios informáticos.	1. Afecta la resolución de incidentes y atención de servicios informáticos que solicitan las personas funcionarias del IECM. 2. Podría perderse el seguimiento en la atención de incidentes o servicios.	Personas funcionarias del IECM	2	1	2	1. Contar con niveles de servicio para resolver incidentes y atender servicios informáticos. 2. Contar con guiones de operación de los sistemas, inventarios de bienes informáticos y flujos de atención. 3. Contar con documento de excel para poder registrar y dar seguimiento inicidentes y servicios. 4. Hacer uso del correo electrónico para la asignación de la atención del incidente o servicios.	3	0.1	Nivel de riesgo aceptable (NRA)				
9	Desarrollo de Sistemas Informáticos	Ambientales	Presencia de desastres naturales.	La presencia de un huracan, terremoto, inundación, tormeta eléctrica o cualquier evento natural que puediera afectar las intalaciones del Instituto o de los Servicios que se tienen contratados como son las telecomunicaciones, seguridas, publicación. Por lo que al presentearse cualquier evento catalogado como desastre natural puede denegar el acceso los servicios e infraestructura.	Afectación a la continuidad operativa de las aplicaciones y sistemas que atienden todos los servicios del IECM.	1. Alta Dirección 2. Personas funcionarias del IECM	3	1	3	1. Sistemas que se encuentran operando en la nube para mantener la continuidad operativa. 2. Servicios contratados en la nube como son correo electrónico, almacenamiento, DNS, Certificados, seguridad. 3. Desarrollar un plan de recuperación de desastres para los procesos sustantivos informáticos y dar continuidad a los servicios.	3	0.1	Nivel de riesgo aceptable (NRA)				

10	Asignación, Préstamo o Devolución de Bienes Informáticos	Operacionales	Falta del formato con la firma del solicitante de asignación, préstamo o devolución.	La inexistencia del formato de control de bienes informáticos o documento sin firma afecta la gestión de bienes informáticos con los usuarios.	Al no contar con el formato generado y firmado, que respalde el bien informático que fue asignado, préstado o devuelto, se pierde el control del equipo por robo o extravío, o simplemente no se gestiona la devolución de personal de baja, lo que provoca problemas de Control Patrimonial.	1. Alta Dirección 2. Personas funcionarias del IECM	1	1	1	1. Tener un documento de excel que apoye al registro de los bienes informáticos asignados, prestados o devueltos. 2. Apoyarse con el área de Almacén de Control Patrimonial para conocer los resguardos de bienes informáticos. 3. Llenar los formatos de correspondientes y que firme el solicitante al momento de la entrega del bien informático.	3	1.5	Nivel de riesgo aceptable (NRA)				
11	Nuevas Tecnologías	Tecnológicos	Obsolescencia de la Infraestructura de cómputo, seguridad y comunicaciones.	La infraestructura de cómputo tiene un tiempo promedio de vida de 5 años, debido al uso continuo en la operación y la evolución tecnológica el desempeño de los equipos en operación empieza a disminuir, así como las actualizaciones de software y firmware que ya no son renovadas provocando vulnerabilidades de seguridad y funcionalidad en comparación con las nuevos equipos de cómputo, seguridad y comunicaciones.	1. Puede generar lentitud o falta de disponibilidad en los sistemas y aplicaciones que utilizan de las personas funcionarias del IECM. 2. Afectación por pérdida de información debido a las vulnerabilidades de seguridad y funcionalidad de la infraestructura obsoleta.	1. Alta Dirección 2. Personas funcionarias del IECM	2	2	4	1. Contar con la infraestructura de cómputo y comunicaciones con un tiempo de vida menor a 5 años. 2. Contar con infraestructura de cómputo y comunicaciones de respaldo (nueva u obsoleta) en condiciones funcionales. 3. Actualización de la infraestructura de cómputo y comunicaciones que se encuentran en grado de obsolescencia o al final de su vida útil.	2	1.5	Nivel de riesgo aceptable (NRA)				
12	Gestión de las Tecnologías	Políticos	Disminución de solicitudes informáticas por recorte presupuestal del Instituto.	Existen solicitudes de infraestructura por obsolescencia o bien nuevas necesidades informáticas, las cuales pueden disminuir debido a que el presupuesto autorizado para el Instituto sea menor al que se requiere para operar.	1. Que las personas funcionarias del IECM no cuenten con los bienes informáticos necesarios para cumplir con sus actividades de operación y de proceso. 2. Que la infraestructura tecnológica exceda el tiempo de vida útil en terminos de funcionalidades, actualizaciones de componentes o existencia de insumos y refacciones.	1. Alta Dirección 2. Personas funcionarias del IECM	2	3	6	1. Contar con infraestructura tecnológica de respaldo en condiciones funcionales. 2. Contratos de mantenimiento por evento abiertos, así como pólizas de soporte en caso de ocurrir fallas en la infraestructura	2	2.2	Reducir riesgo	1. Que la alta dirección garantice la adquisición minima de la infraestructura tecnológica requerida para la operación institucional.	ene-25	dic-25	UTSI

13	**Gestión de las Tecnologías**	**Tecnológicos**	**Ataques cibernéticos y robo de información en la infraestructura informática y en los Sistemas Electorales y de Participación Ciudadana.**	Podría haber una deficiencia y desconfianza en los servicios y operación institucional por la falta de seguridad informatica en la infraestructura tecnológica, sistemas electorales y de participación ciudadana, como podría ser la desconfianza del votante por tener un voto desprotegido, con vulnerabilidad ante ataques o robo de información.	1. Que las personas funcionarias del IECM y los votantes desconfien porque su voto este desprotegido o pueda existir un robo de información, derivado de un ataque cibernético. 2. Que la infraestructura tecnológica tenga componetes o sistemas operativos desactualizadas.	1. Alta Dirección 2. Personas funcionarias del IECM	**2**	**3**	**6**	1. Contratos de mantenimiento preventivo y correctivo, así como pólizas de soporte para mantener sus componectes actualizados y seguros. 2. Monitoreo de la infraestructura de servidores y equipos de telecomunicaciones para tomar acciones preventivas ante alguna anormalidad y accesos no permitidos. 3. Los contratos de software de seguridad para protección de la infraestructura tecnológica y sistemas de operación ordinaria, proceso electoral y de participación ciudadana.	**2**	**2.2**	**Reducir riesgo**	1. Que la alta dirección garantice la adquisición de los mantenimientos, renovaciones de sofware de seguridad y polizas de soporte de la infraestructura tecnológica requerida para la operación institucional.	**ene-25**	**dic-25**	**UTSI**

ALTO	Es necesario dar tratamiento al Riesgo.
MEDIO	Es recomendable dar tratamiento al Riesgo.
BAJO	Nivel de Riesgo Aceptable.

	Elaboró	Aprobó
Nombre:	Ana Angelica González Oliva	Estefanía Mena Ibarra
Puesto:	Subdirectora de Seguridad, Redes y Cómputo	Titular de la Unidad Técnica de Servicios Informáticos
Firma:		