GOBIERNO DE EL SALVADOR

MINISTERIO DE CULTURA

MINISTERIO DE CULTURA
DESPACHO MINISTERIAL DE CULTURA

DIRECCIÓN GENERAL DE INFORMÁTICA Y SISTEMAS

PLAN OPERATIVO ANUAL
AÑO 2025

Ing. Guillermo Adalberto Jandres Escobar
Director General de Informática y Sistemas

EL SALVADOR, 2025

GOBIERNO DE EL SALVADOR

MINISTERIO DE CULTURA

ÍNDICE

I. Introducción.

La Dirección General de Informática y Sistemas es la dependencia del Ministerio de Cultura que tiene por objetivo sostener la infraestructura tecnológica y de comunicación de la institución. Es crucial para alcanzar los objetivos institucionales propuestos. No solo brindan y sostienen la compleja estructura tecnológica, también se encarga de implementar mejoras y procurar la innovación constante implementando controles internos de seguridad, integridad y confiabilidad de los sistemas informáticos que se utilizan en el desarrollo de las actividades del Ministerio de Cultura.

Para prestar sus servicios cuenta con las siguientes dependencias: Coordinación de Redes y Soporte Informático, Coordinación de Aplicaciones y Medios Informáticos, Coordinación de Infraestructura Informática.

En la planificación de actividades se incluyen los resultados esperados, indicadores, medios y fuentes de verificación, responsables de cumplimiento y el presupuesto de las acciones programadas, todo con la finalidad de alcanzar los objetivos del Plan Estratégico Institucional.

Basados en dicho objetivo y los establecidos en el Plan Estratégico Institucional se presenta el Plan Operativo Anual 2025 de la Dirección General de Informática y Sistemas el cual contempla: un análisis del entorno, la identificación y gestión de riesgos y la planificación y programación de actividades.

II. Objetivos del POA

General

Establecer y definir las acciones que realizará la Dirección General de Informática y Sistemas durante el año 2025 y los resultados que se obtendrán en apoyo al cumplimiento de los objetivos institucionales.

Específicos

1. Brindar el servicio de soporte técnico informático de forma adecuada y oportuna.
2. Mantener la infraestructura de redes de datos sobre los cuales se proporcionan los servicios de comunicación de forma segura continua.
3. Proveer los medios de comunicación web institucionales necesarios para la promoción y difusión del quehacer artístico y cultural.

4. Crear y mejorar las aplicaciones informáticas implementadas en apoyo a las necesidades de los usuarios de las dependencias para la prestación de los servicios.

III. Análisis del Entorno.

Factores Internos	
Fortalezas	**Debilidades**
❖ Personal capacitado para brindar soporte técnico. ❖ Se cuenta con personal capacitado para el cambio de repuestos de forma oportuna antes que falle alguna otra pieza. ❖ Existencia de repuestos necesarios para suplir necesidades de usuario y equipos. ❖ Se cuenta con personal capacitado para limpieza de equipo informático. ❖ Existencia de insumos y herramientas necesarios para la limpieza de equipos. ❖ Posibilidad de contar con herramienta informática para registro y actualización de inventario de equipos. ❖ Personal con los conocimientos adecuados en hardware y software ❖ Personal capacitado en el diseño, creación y mantenimiento de redes de datos. ❖ Herramientas y materiales adecuados para la realización de mantenimiento de redes de datos. ❖ Administración y control sobre los dispositivos conectados a la red de datos institucional. ❖ Completo control sobre todos los dispositivos de Red inalámbricas ❖ Equipos de Seguridad Actualizados. ❖ Controles de Accesos Informáticos. ❖ Apoyo financiero para Actualización de equipos de Seguridad Informática ❖ Completo control sobre los equipos físicos, así como de los servicios que brinda el centro de Datos a nivel virtual. ❖ Completa constancia en la realización de mantenimientos semestrales.	❖ Poco personal en la Coordinación para atención oportuna en todas las dependencias. ❖ Existencia insuficiente de repuestos informáticos por alta demanda de insumos en oficinas centrales y dependencias. ❖ Falta de presupuesto para la compra de repuestos informáticos. ❖ Existencia insuficiente de insumos para limpieza de equipos. ❖ Falta de presupuesto para compra de insumos y herramientas de limpieza de equipos. ❖ Existencia insuficiente de materiales y herramientas para mantenimiento de redes de datos. ❖ Falta de presupuesto para compra de materiales y herramientas para mantenimiento de redes de datos. ❖ Usuarios a los que se les asignaron las claves de redes en un momento pero que ya no tengan privilegio de uso de la misma. ❖ Resistencia al cambio por parte de Usuarios Finales. ❖ Computadoras, equipos de Comunicación y servidores desactualizados. ❖ Equipos y servicios que ya no están en uso o que hayan sido sustituidos por uno nuevo que lo reemplace. ❖ Posibles fallas que pueda tener el equipo físico que comprende el centro de Datos ❖ Se dispone de una suite de correos en la nube con la cual se requiere licenciamiento anual para la administración de correos ❖ Desconocimiento de las plataformas. ❖ Personal con múltiples actividades asignadas reducen la cantidad de cursos y contenido a impartir en el año. ❖ Poco personal para satisfacer la demanda de creación y desarrollo de nuevos sistemas.

Factores Internos	
Fortalezas	**Debilidades**
❖ Mayor Seguridad contra vulnerabilidades hacia las cuentas de correo asociadas ❖ Se cuenta con la plataforma virtual para la educación tecnológica. ❖ Implementación de nuevas tecnologías para el desarrollo de sistemas con estándares vigentes en el mercado. ❖ Personal con las competencias y habilidades para la adopción de nuevas tecnologías según el estándar adoptado. ❖ Manejo de herramientas vigentes en el mercado para la creación de sitios web adoptado como estándar en el sector gubernamental. ❖ Se cuenta con personal capacitado en el diseño y creación de sitios web.	❖ Falta de capacitación al personal en nuevas tecnologías. ❖ Poco personal para la creación y desarrollo de nuevos sitios web. ❖ Debido a que el sitio web está alojado fuera de nuestra infraestructura, no es posible administrarlo de manera oportuna.

Factores Externos	
Oportunidades	**Amenazas**
❖ Alianzas estratégicas con instituciones educativas para obtener colaboración de estudiantes que necesitan realizar Servicio Social o Práctica Profesional en la institución. ❖ Gestiones de apoyo en soporte técnico con estudiantes en Servicio Social o Práctica Profesional. ❖ Gestiones de apoyo en soporte técnico externo por parte de proveedores y fabricantes. ❖ Gestiones de apoyo para actividades de mantenimiento preventivo con estudiantes en Servicio Social o Práctica Profesional. ❖ Disponibilidad de forma ágil y oportuna de consultar en línea de información de equipos y usuarios según inventario informático realizado. ❖ Mantener conexión de redes de datos estable en oficinas centrales y dependencias del Ministerio de Cultura.	❖ Falta de asignación de presupuesto para tecnologías informáticas. ❖ Afectación a la salud del personal por enfermedades varias. ❖ Falta de asignaciones de transporte para visitas a dependencias. ❖ Manipulación inadecuada de equipos informáticos por parte de los usuarios y personas ajenas a la institución. ❖ Problemas externos por caídas de la corriente eléctrica, incendios. Factores climatológicos como terremotos, huracanes que pudieran dañar las instalaciones de las dependencias donde existe equipo informático. ❖ Fallas en los enlaces de datos por parte del Proveedor de Servicios de Internet. ❖ Que el personal que posea las contraseñas de acceso a las redes inalámbricas proporcionen dicho acceso a usuarios no autorizados ❖ Hackers, usuarios internos inconformes.

Factores Externos	
Oportunidades	**Amenazas**
❖ Monitoreo de funcionamiento de la red de datos. ❖ Monitoreo de las redes y servidores para corroborar el correcto uso por parte de los usuarios que tengan dicho privilegio. ❖ Controlar los equipos de redes inalámbricas desde un servidor central para un manejo más eficiente y remoto de la red ❖ Publicación de Sitios Web Seguros. ❖ Brindar nuevos servicios informáticos a la población. ❖ Colaborar con apoyo a Transformación de gobierno digital. ❖ Generación de un registro sobre todos los equipos y servicios que el centro de datos posee para poder formar un control histórico de los mismos. ❖ El respaldo de los procesos realizados en el mantenimiento para respaldo histórico de los eventos solucionados y no solucionados en los equipos de centro de datos. ❖ Integración con el sistema de accesos de usuario por dominio ❖ Manejo y control de factores de autenticación para todos los usuarios en caso de vulnerabilidad de contraseñas ❖ Acceso y administración sin costo a nueva plataforma durante el año 2024, por gestión de la Secretaría de Innovación. ❖ La plataforma está disponible en línea para consulta 7/24 por parte de los participantes, incluso fuera de la institución. ❖ Existe material de apoyo disponible en internet para reforzar los contenidos de los cursos impartidos. ❖ Alianzas estratégicas con instituciones externas para obtener donación de sistemas para implementar en la institución. ❖ Gestión con instituciones educativas de nivel superior para obtener apoyo de estudiantes que realicen proyectos de	❖ Legislación que no regula la actividad informática. ❖ Problemas externos al centro de datos, así como caídas de la corriente eléctrica, incendios. Factores climatológicos como terremotos, huracanes que pudieran dañar la infraestructura que resguarda el centro de datos ❖ Usuarios de correo institucional acceden o abren correos fraudulentos que contienen SPAM, virus o Phishing. ❖ Usuarios que no quieran hacer uso de las herramientas de seguridad para su correo, así como el uso inadecuado del envío y recepción de correos no institucionales ❖ Falta de disponibilidad de tiempo de los empleados para participar en las capacitaciones de ofimática. ❖ Desinterés por parte de los usuarios para participar en los cursos impartidos. ❖ No contar con la velocidad y ancho de banda necesarios para realizar videoconferencias. ❖ Retraso en la implementación y puesta en marcha de Plataformas Gubernamentales. ❖ Cambio por prioridades institucionales que derivan en cambios a la planificación interna establecida. ❖ Falla en los servicios de internet. ❖ Daño o falla en los servidores que alojan los sitios web. ❖ Ataques de denegación de servicios o vulnerar la seguridad de los sitios web institucionales.

Factores Externos	
Oportunidades	**Amenazas**
graduación, pasantías y horas sociales en el área de desarrollo. ❖ Se cuenta con apoyo de la Secretaría de Innovación para la donación de sistemas para implementar en la institución. ❖ Se cuenta con lineamientos y estándares de diseño claros para los sitios web institucionales, provistos por la Secretaría de Innovación.	

IV. Identificación del Riesgo.

Códigos	Resultados y Acciones	Identificación del riesgo			Análisis del riesgo						Descripción de la calificación del riesgo
					Cualificación del riesgo		Nivel de Riesgo				
		Tipo de Riesgo	Descripción del Riesgo	Responsable	Probabilidad	Impacto	E	A	M	B	
RO	R.1. Intervenidos los equipos informáticos										
RO	A1.1. Atención a usuarios con equipos informáticos por medio de soporte técnico.	Riesgo Operacional	Falta de asignación de presupuesto para tecnologías informáticas.	Técnicos Coordinación de Redes y Soporte Informático	Muy Probable	Muy Serio					Riesgo Extremo
RO	A.1.2. Realización de mantenimiento preventivo a equipos informáticos.	Riesgo Operacional	Falta de asignaciones de transporte para visitas a dependencias. Retraso en la cobertura de requerimientos por aumento de la demanda de servicios debido a la falta de personal en la Dirección. Manipulación inadecuada de equipos informáticos por parte de los usuarios y personas ajenas a la institución. Afectación a la salud del personal por enfermedades varias.	Técnicos responsables de la Coordinación de Redes y Soporte Informático	Alta Probabilidad	Muy Serio					Riesgo Extremo
RO	A.1.3. Actualización de Inventario de equipos informáticos.	Riesgo Operacional	Falta de asignaciones de transporte para visitas a dependencias. Afectación a la salud del personal por enfermedades varias.	Técnicos responsables de la Coordinación de Redes y Soporte Informático	Alta Probabilidad	Serio					Riesgo Alto.

Códigos	Resultados y Acciones	Identificación del riesgo			Análisis del riesgo						Descripción de la calificación del riesgo
					Cualificación del riesgo		Nivel de Riesgo				
		Tipo de Riesgo	Descripción del Riesgo	Responsable	Probabilidad	Impacto	E	A	M	B	
RO	R.2. Controlada la Infraestructura informática de la institución										
RO	A.2.1. Realización de mantenimiento a redes de datos.	Riesgo Tecnológico Riesgo Operacional	Fallas en los enlaces de datos por parte del Proveedor de Servicios de Internet. Falta de asignaciones de transporte para visitas a dependencias.	Técnicos responsables de la Coordinación de Redes y Soporte Informático y Coordinación de Infraestructura y Seguridad	Muy Probable	Grave					Riesgo Extremo
RO	A.2.2. Implementación y Mantenimiento de mecanismos de seguridad de accesos a redes de datos.	Riesgo Tecnológico Riesgo Político	Falla en el correcto funcionamiento de los medios de conexión inalámbrica por problemas en los equipos físicos. Pérdida de configuraciones o defectuosas en su caso, producto de interrupciones de energía eléctrica. Vulnerabilidad de que usuarios autorizados compartan credenciales de acceso a las redes inalámbricas.	Coordinación de Infraestructura y Seguridad	Muy Probable	Grave					Riesgo Extremo
RO	A.2.3. Administración del centro de datos.	Riesgo Tecnológico	Accesos a equipos informáticos por usuarios no autorizados. Falla en los equipos físicos que componen el centro de Datos. Fallas por ataques informáticos.	Coordinación de Infraestructura y Seguridad.	Alta Probabilidad	Grave					Riesgo Extremo
RO	A.2.4. Realización de mantenimiento preventivo de la infraestructura informática del centro de datos	Riesgo Tecnológico	Falla en los equipos físicos que componen el centro de Datos.	Coordinación de Infraestructura y Seguridad.	Alta Probabilidad	Grave					Riesgo Extremo

Códigos	Resultados y Acciones	Identificación del riesgo			Análisis del riesgo						Descripción de la calificación del riesgo
					Cualificación del riesgo		Nivel de Riesgo				
		Tipo de Riesgo	Descripción del Riesgo	Responsable	Probabilidad	Impacto	E	A	M	B	
RO	R.3. Cursos gestionados en la plataforma virtual para la educación tecnológica.										
RO	A.3.1 Desarrollo de capacitaciones.	Riesgo Operacional	Falta de capacitación al personal en nuevas tecnologías.	Coordinador de área o Responsable de Curso.	Alta Probabilidad	Serio					Riesgo Alto.
RO	R.4 Proporcionados los Accesorios informáticos a usuarios										
RO	A.4.1 Administración de los accesorios informáticos	Riesgo Operacional	Falta de asignaciones de transporte para visitas a dependencias. Afectación a la salud del personal por enfermedades varias.	Técnico responsable de suministro de accesorios	Alta Probabilidad	Serio					Riesgo Alto
RO	R.5. Actualizados los sistemas informáticos institucionales.										
RO	A.5.1 Desarrollo e Implementación de mejoras a Sistemas informáticos existentes.	Riesgo Estratégico	Poco personal para satisfacer la demanda de creación y desarrollo de nuevos sistemas.	Jefatura y coordinador del área.	Alta Probabilidad	Muy Serio					Riesgo Extremo
RO	R.6. Administrados los sitios web institucionales.										
RO	A.6.1 Mantenimiento a sitios web institucionales	Riesgo Operacional	Constantes ataques de denegación de servicios o intentos de vulneración de la seguridad de los sitios web institucionales. Que se presente una alta demanda de cambio o solicitudes de nuevos sitios web institucionales y no exista personal suficiente para cubrir la demanda.	Coordinador de área o encargado de sitio web	Alta Probabilidad	Muy Serio					Riesgo Extremo

V. Gestión del Riesgo.

N°	Riesgos	Gestión del Riesgo
1	Falta de asignación de presupuesto para tecnologías informáticas.	Gestionar alternativas financieras para obtener los recursos necesarios en la ejecución de actividades involucradas en tecnologías informáticas.
2	Falta de asignaciones de transporte para visitas a dependencias. Retraso en la cobertura de requerimientos por aumento de la demanda de servicios debido a la falta de personal en la Dirección. Manipulación inadecuada de equipos informáticos por parte de los usuarios y personas ajenas a la institución. Afectación a la salud del personal por enfermedades varias.	Brindar atención de requerimientos de forma remota para los casos en que sea factible apoyar a los usuarios de forma no presencial y gestionar apoyo de transporte asignado para cobertura de rutas en jornadas completas para abarcar la mayor cantidad de dependencias posibles. Realizar gestiones ante las autoridades competentes, para la contratación de personal técnico que fortalezca las áreas técnicas de redes de comunicación y soporte informático. Gestionar con instituciones educativas que los estudiantes realicen sus Prácticas Profesionales o Servicio Social para que apoyen en actividades técnicas de la Coordinación de Redes y Soporte Informático. Divulgar medidas de prevención para conservación y buen uso de los recursos informáticos. Sugerir y justificar a las autoridades (Directores y Jefaturas) del Ministerio de Cultura el riesgo de poseer equipos desfasados para la seguridad de la red institucional y resguardo de información. Trasladar responsabilidades de soporte y redes hacia otros compañeros que se encuentren en buen estado de salud.
3	Falta de asignaciones de transporte para visitas a dependencias. Afectación a la salud del personal por enfermedades varias.	Gestionar apoyo de transporte asignado para cobertura de rutas en jornadas completas para abarcar la mayor cantidad de dependencias posibles. Trasladar responsabilidades de soporte y redes hacia otros compañeros que se encuentren en buen estado de salud.
4	Fallas en los enlaces de datos por parte del Proveedor de Servicios de Internet. Falta de asignaciones de transporte para visitas a dependencias.	Brindar un mantenimiento periódico a las redes de comunicación de datos en las dependencias de la institución solicitando al proveedor el mantenimiento de sus equipos de comunicación de forma periódica. Gestionar apoyo de transporte asignado para cobertura de rutas en jornadas completas para abarcar la mayor cantidad de dependencias posibles. Trasladar responsabilidades de soporte y redes hacia otros compañeros que se encuentren en buen estado de salud.

N°	Riesgos	Gestión del Riesgo
5	Falla en el correcto funcionamiento de los medios de conexión inalámbrica por problemas en los equipos físicos. Pérdida de configuraciones o defectuosas en su caso, producto de interrupciones de energía eléctrica. Vulnerabilidad de que usuarios autorizados compartan credenciales de acceso a las redes inalámbricas.	Generar políticas internas de cambio periódico de las claves de acceso a las redes inalámbricas. Generar políticas de respaldo de configuraciones de los dispositivos.
6	Accesos a equipos informáticos por usuarios no autorizados. Falla en los equipos físicos que componen el centro de Datos. Fallas por ataques informáticos.	Generar políticas de respaldo de configuraciones y servicios de los dispositivos que componen el centro de Datos. Generar políticas de acceso al centro de datos por personal ajeno a la Unidad de Informática y Sistemas. Generar políticas de creación de claves de alta complejidad y de cifrado de archivos de respaldo.
7	Falla en los equipos físicos que componen el centro de Datos.	Generar políticas de renovación de los equipos del centro de Datos que ya hayan excedido su periodo de vida útil.
8	Falta de capacitación al personal en nuevas tecnologías.	Solicitar capacitaciones especializadas para el personal del área. Programación de capacitación interna, aprovechando la experiencia del nuevo personal, para replicarlo en toda el área.
9	Poco personal para satisfacer la demanda de creación y desarrollo de nuevos sistemas.	Buscar apoyo con personal externo, estudiantes de servicio social o programas de pasantías. Capacitación a personal en el uso de lenguajes de programación.
10	Constantes ataques de denegación de servicios o intentos de vulneración de la seguridad de los sitios web institucionales. Que se presente una alta demanda de cambio o solicitudes de nuevos sitios web institucionales y no exista personal suficiente para cubrir la demanda.	Administración de los sitios web institucionales mediante: Incorporación de certificados de seguridad para protección de identidad de sitios web institucionales. Actualización de componentes que conforman el sitio web institucional. Gestión de respaldos de los sitios web para prevención de pérdida de información. Buscar apoyo con personal externo, estudiantes de servicio social o programas de pasantías.

VI. Programación de Actividades.

Códigos	Resultados y Acciones	Indicadores	Medios de Verificación	Fuente de Datos	Persona Responsable de Ejecución	Unidad de Medida	Meta Anual (Cantidad de Resultados y Acciones)	Presupuesto (Dato Proporcionado por DGFI)	Meses											
									E	F	M	A	M	J	J	A	S	O	N	D
RO	R.1. Intervenidos los equipos informáticos.	Equipos intervenidos				Equipos Informáticos	36	-												
RO	A.1.1. Atención a usuarios con equipos informáticos por medio de soporte técnico.		Informe Mensual de Atención de equipos informáticos	A101.3.1-01 Mantenimiento y soporte informático	Angela Merino	Cantidad de usuarios atendidos	12	-	1	1	1	1	1	1	1	1	1	1	1	1
RO	A.1.2. Realización de mantenimiento preventivo a equipos informáticos.		Informe Mensual de Mantenimientos preventivos Ejecutados	A101.3.1-01 Mantenimiento y soporte informático	Salvador Urrutia	Cantidad de equipos intervenidos	12	-	1	1	1	1	1	1	1	1	1	1	1	1
RO	A.1.3. Actualización de Inventario de equipos informáticos.		Informe Mensual de Equipos Informáticos Inventariados	A101.3.1-01 Mantenimiento y soporte informático	Josué Díaz	Cantidad de equipos intervenidos	12	-	1	1	1	1	1	1	1	1	1	1	1	1
RO	R.2. Controlada la Infraestructura informática de la institución	Infraestructura Informática controlada				Servicios	12	-												
RO	A.2.1. Realización de mantenimiento a redes de datos.		Informe trimestral de redes de datos atendidas	A101.3.3-01 Seguridad y accesos informáticos	José Aragón	Informe	4	-			1			1			1			1
RO	A.2.2. Implementación y Mantenimiento de mecanismos de seguridad de accesos a redes de datos.		Informe trimestral de seguridad de accesos a las redes de datos	A101.3.3-01 Seguridad y accesos informáticos	Giovanni Cartagena	Informe	4	-			1			1			1			1

Códigos	Resultados y Acciones	Indicadores	Medios de Verificación	Fuente de Datos	Persona Responsable de Ejecución	Unidad de Medida	Meta Anual (Cantidad de Resultados y Acciones)	Presupuesto (Dato Proporcionado por DGFI)	Meses											
									E	F	M	A	M	J	J	A	S	O	N	D
RO	A.2.3. Administración del centro de datos.		Informe semestral de configuraciones de administración realizadas en el centro de datos	A101.3.3-02 Infraestructura de servidores	Jorge Batres y Giovanni Cartagena	Informe	2	-						1						1
RO	A.2.4 Realización de mantenimiento preventivo de la infraestructura informática del centro de datos.		Informe de mantenimientos preventivos ejecutados de la infraestructura del centro de datos	A101.3.3-02 Infraestructura de servidores	Jorge Batres y Giovanni Cartagena	Informe	2	-						1						1
RO	R.3. Cursos gestionados para la educación tecnológica	Número de Cursos gestionados				Cursos	2	-												
RO	A.3.1 Desarrollo de capacitaciones		Informe de gestiones realizadas	A101.3.2-04 Educación tecnológica	Claudia de Campos	Cursos	2	-						1						1
RO	R.4. Proporcionados los Accesorios informáticos a los usuarios.	Accesorios informáticos proporcionados				Accesorios Informáticos	12	-												
RO	A.4.1 Administración de los accesorios informáticos		Informe Mensual de Entregas de Accesorios Informáticos	A101.3.1.03 Correspondencia	Vangie Vigil	Cantidad de accesorios entregados	12	-	1	1	1	1	1	1	1	1	1	1	1	1
RO	R.5. Actualizados los sistemas informáticos institucionales.	Sistemas Informáticos actualizados				Sistemas	2	-												
RO	A.5.1 Desarrollo e Implementación de mejoras a Sistemas informáticos existentes.		Sistema en funcionamiento	A101.3.2-01 Aplicaciones informáticas	William Pineda, Sara Galán, Marcela Calero, Claudia de Campos	Sistemas	2	-						1						1
RO	R.6. Administrados los sitios web institucionales.	Sitios web administrados				Sitios Web	2	-												

Códigos	Resultados y Acciones	Indicadores	Medios de Verificación	Fuente de Datos	Persona Responsable de Ejecución	Unidad de Medida	Meta Anual (Cantidad de Resultados y Acciones)	Presupuesto (Dato Proporcionado por DGFI)	Meses											
									E	F	M	A	M	J	J	A	S	O	N	D
RO	A.6.1 Mantenimiento a sitios web institucionales.		Informe de Sitio web en funcionamiento	A101.3.2-03 Medios de Comunicación Web	William Pineda	Sitios Web	2	-						1						1
LAIP	R.1. Presentado el informe sobre la información de tipo oficiosa identificada de la unidad administrativa u otra que el oficial solicite.	Número de Información entregada				Información	8	-												
LAIP	A.1.3.1. Remisión del Directorio de cada unidad administrativa relativa a directores, jefes, coordinadores, y administradores.		Memorándum e información entregada	A101.3-01 Correspondencia (interna y externa)	Vangie Vigil	Información	4	-	1			1			1			1		
LAIP	A.1.3.2. Remisión del Currículo vitae de aquellos nuevos miembros que se integren a este grupo de funcionarios o que se necesite actualizar.		Memorándum e información entregada	A101.3-01 Correspondencia (interna y externa)	Vangie Vigil	Información	4	-	1			1			1			1		
LAIP	R.2. Presentado el informe sobre la información de tipo reservada de la unidad administrativa.	Número de Información entregada				Información	2	-												
LAIP	A.2.1. Remisión del Memorándum indicando la información a reservar, o actualización de la ya reservada		Memorándum e información entregada	A101.3-01 Correspondencia (interna y externa)	Vangie Vigil	Información	2	-	1						1					
LGDA	R.1. Fortalecido el Sistema de Gestión Documental y Archivo.	Número de acciones realizadas				Acción	5	-												
LGDA	A.1.1 Crear y Actualizar el Cuadro de Clasificación Documental		Cuadro de Clasificación Documental Creado o Actualizado firmado y sellado	Digital	Vangie Vigil	Acta Firmada por UGDA y Cuadro de Clasificación Documental	1	-			1									

Códigos	Resultados y Acciones	Indicadores	Medios de Verificación	Fuente de Datos	Persona Responsable de Ejecución	Unidad de Medida	Meta Anual (Cantidad de Resultados y Acciones)	Presupuesto (Dato Proporcionado por DGFI)	Meses											
									E	F	M	A	M	J	J	A	S	O	N	D
LGDA	A.1.2. Remitir a la UGDA la Tabla de Plazos de Conservación Documental de todas las series de su Cuadro de Clasificación Documental		Tabla de Plazos de Conservación Documental (Formulario completo firmado y sellado y en debida forma)	Correo Electronico	Vangie Vigil	Tabla de Plazos de Conservación Documental (Formulario)	1	-						1						
LGDA	A.1.3. Elaborar los inventarios de todas las series documentales del año 2024.		Documento de inventario firmado y sellado	Correspondencia Interna y Externa	Vangie Vigil	Archivo en formato xls.	1	-		1										
LGDA	A.1.4. Remitir a la UGDA para revisión en hoja electrónica (Excel) los inventarios de todas las series documentales del año 2024. En caso de no tener alguna serie, justificar por qué no lo envía.		Correo Electrónico a Jefe de la UGDA, conteniendo el archivo de Excel	Correspondencia Interna y Externa	Vangie Vigil	Archivo en formato xls.	1	-		1										
LGDA	A.1.5. Remitir un plan de trabajo para levantamiento de inventario documentales anteriores a 2024		Plan de Trabajo autorizado, presentado a la UGDA	Información	Vangie Vigil	Documento	1	-			1									
LMA	R.3. Ejecutadas las Acciones de ecoeficiencia	Número de Acciones realizadas				Acción	13	-												
LMA	A.3.1 Apoyar por lo menos en una de las jornadas de reforestación que realice la DGA.		Fotografías de personal en eventos de reforestación	Archivo digital de Documentos	Vangie Vigil	Asistencia	1	-							1					
LMA	A.3.2 Aplicar los criterios de compras públicas sostenibles en los procesos de compra de obras, bienes y servicios basándose en lo que establece la Ley de Compras Públicas		Informe sobre las solicitudes de compra con criterios de sostenible	Archivo digital de Documentos	Angela Merino, Claudia de Campos y Jorge Chamul	Informe	12	-	1	1	1	1	1	1	1	1	1	1	1	1
LMA	R.4. Fortalecido el personal de la institución con acciones de educación y cultura ambiental	Número de participaciones				Participación	4	-												

Códigos	Resultados y Acciones	Indicadores	Medios de Verificación	Fuente de Datos	Persona Responsable de Ejecución	Unidad de Medida	Meta Anual (Cantidad de Resultados y Acciones)	Presupuesto (Dato Proporcionado por DGFI)	Meses											
									E	F	M	A	M	J	J	A	S	O	N	D
LMA	A.4.1. Participar en las capacitaciones que de la Dirección General Ambiental convoque sobre los documentos institucionales y otros.		Informe: Descripción de la actividad, Resultados, Lecciones aprendidas, Fotografías.	Archivo digital de Documentos con fotografías	Vangie Vigil	Participaciones	4	-		1			1			1			1	
LMA	5. Entregados los datos e informes en cumplimiento de indicadores de gestión ambiental	Número de acciones medio ambientales				Acción	2	-												
LMA	A.5.2 Presentar informes semestrales (última semana de junio y última semana de diciembre), sobre todas las acciones ambientales realizadas.		Informe semestral	Archivo digital l de Documentos	Vangie Vigil	Documentos	2	-						1						1
PNI 2021-2025	R.2. Creada y ejecutándose una estrategia cultural que aporten a la transformación de los modelos sexistas y discriminatorios en el arte, la gestión del conocimiento, el patrimonio cultural y la cultura comunitaria.	Número de participaciones				Acción	2	-												
PNI 2021-2025	A.2.2. Participar en dos actividades en el marco de la conmemoración de fechas emblemáticas para contribuir al fomento de la igualdad, no discriminación y respeto de los derechos de las mujeres. (en marzo y noviembre).		Convocatoria y Listas de asistencias	A101.3-01 Correspondencia (Interna y Externa)	Vangie Vigil	Convocatoria	2	-			1								1	
LIE	R.1. Desarrolladas actividades que promueven la igualdad, equidad, y erradicación de la violencia y discriminación de género con personal de la institución.	Número de participaciones				Participar	3	-												

Códigos	Resultados y Acciones	Indicadores	Medios de Verificación	Fuente de Datos	Persona Responsable de Ejecución	Unidad de Medida	Meta Anual (Cantidad de Resultados y Acciones)	Presupuesto (Dato Proporcionado por DGFI)	Meses											
									E	F	M	A	M	J	J	A	S	O	N	D
LIE	A.1.1. Participar en las convocatorias de capacitación que realice la Unidad de Género para contribuir al fomento de la igualdad, no discriminación y respeto de los derechos de las mujeres.		Convocatoria y Listas de asistencias	A101.3-01 Correspondencia (Interna y Externa)	Vangie Vigil	Convocatoria	3	-					1		1		1			
AD	R.3.3.4. Implementar la plataforma para el seguimiento a la simplificación administrativa y a los planes de mejora regulatoria en las oficinas de Gobierno	Nuevos sistemas implementados				Innovación	2	-												
AD	A.3.3. Modernización de Servicios (Nuevos Sistemas para el servicio de la población o internos)		Informe Semestral	Sistema en funcionamiento	William Pineda, Sara Galán, Marcela Calero, Claudia de Campos	Sistemas Informáticos	2	-						1						1

Guillermo Adalberto Jandres Escobar
Jefe de la Unidad de Informática y Sistemas

VII. Autorización.

Autorizado: _____

Raúl Neftalí Castillo Rosales
Ministro de Cultura.

Visto Bueno: _____

Ing. Kathya Escalante
Directora General Ejecutiva

Revisado: _____

Ing. Jesús Manuel Bran Bermudez
Director General de Planificación y Desarrollo Institucional

Formulado y
Elaborado: _____

Guillermo Adalberto Jandres Escobar
Director General de Informática y Sistemas

_____

Vangie Grissel Vigil Ortiz
Técnico Enlace

Fecha de Autorización: FEB 2025