GOBIERNO DE EL SALVADOR

MINISTERIO DE CULTURA

MINISTERIO DE CULTURA
DIRECCIÓN GENERAL DE ADMINISTRACIÓN

UNIDAD DE INFORMÁTICA Y SISTEMAS

PLAN OPERATIVO ANUAL
AÑO 2023

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

EL SALVADOR, 2023

INDICE

I. Introducción.

La Unidad de Informática y Sistemas es la dependencia del Ministerio de Cultura que tiene por objetivo Implementar 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

Basados en dicho objetivo y los establecidos en el Plan Estratégico Institucional se presenta el Plan Operativo Anual 2023 de la Unidad de Informática y Sistemas el cual contempla: un análisis del entorno, la identificación y gestión de riesgos y la planificación y programación de actividades.

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.

II. Objetivos del POA

General

Establecer y definir las acciones que realizará la Unidad de Informática y Sistemas durante el año 2023 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. 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 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 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 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.	✓ 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 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 ✓ Resistencia al cambio por parte de los usuarios. ✓ Desconocimiento de la plataforma.

Factores Internos	
Fortalezas	**Debilidades**
✓ Completa constancia en la realización de mantenimientos semestrales. ✓ Se tiene disponible la consulta 7/24 de correos vía cliente web. ✓ Mayor Seguridad contra vulnerabilidades hacia las cuentas de correo asociadas ✓ Capacitación y acompañamiento por parte de la Secretaría de Innovación para la implementación de nueva plataforma en la nube para la administración de las cuentas de correo electrónico Institucional. ✓ Se cuenta con la plataforma virtual para la educación tecnológica. ✓ Acceso a nueva plataforma de correo y ofimática de Google a nivel gubernamental. ✓ Se cuenta con el personal técnico capacitado para investigar nuevas herramientas de ofimática y correo electrónico. ✓ Implementación de nuevas tecnologías para el desarrollo de sistemas con estándares vigentes en el mercado. ✓ Personal con las competencias y habilidades para 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.	✓ Resistencia al cambio por parte de los usuarios. ✓ Poco personal para la creación y desarrollo de los cursos virtuales. ✓ 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. ✓ Falta de capacitación al personal en nuevas tecnologías. ✓ Poco personal para la creación y desarrollo de nuevos sitios web.

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. ✓ Monitoreo de funcionamiento de la red de datos. ✓ Monitoreo de las redes 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.	✓ Falta de asignación de presupuesto para tecnologías informáticas. ✓ Afectación a la salud del personal por COVID. ✓ 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. ✓ Falta de políticas para asignación de equipos informáticos hacia usuarios que posee equipo desfasados. ✓ Falta de asignaciones de transporte para visitas a dependencias. ✓ Afectación a la salud del personal por COVID. ✓ 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 personal que posea las contraseñas de acceso a las redes inalámbricas proporcionen dicho acceso a usuarios no autorizados ✓ Hackers, usuarios internos inconformes. ✓ 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

Factores Externos	
Oportunidades	**Amenazas**
✓ 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 2023, 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 graduación, pasantías y horas sociales en el área de desarrollo. ✓ Se cuenta con apoyo de la Secretaría de Innovación para la donación de	✓ 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**
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. ✓ Se tienen alianzas estratégicas con la Secretaría de Innovación que permiten contar con alojamiento en la nube de sitios web que tienen alta demanda, mostrando alta disponibilidad para el usuario final.	

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	1. Intervenidos los Equipos informáticos						-	-	-	-	
RO	1.1 Atención a equipos informáticos por medio de soporte técnico.	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 de la unidad. - Manipulación inadecuada de equipos informáticos por parte de los usuarios y personas ajenas a la institución. - Falta de políticas para asignación de equipos informáticos hacia usuarios que posee equipo desfasados. - Afectación a la salud del personal por COVID.	Técnicos Coordinación de Redes y Soporte Informático	Muy Probable	Muy Serio					Riesgo Extremo
RO	1.2 Realización de mantenimiento preventivo a equipos informáticos	Riesgo Operacional	- Falta de asignaciones de transporte para visitas a dependencias. - Afectación a la salud del personal por COVID.	Técnicos responsables de la Coordinación de Redes y Soporte Informático	Alta Probabilidad	Muy Serio					Riesgo Extremo
RO	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 COVID.	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	2. Controlada la Infraestructura informática de la institución										
RO	2.1 Realización de mantenimiento a redes de datos	Riesgo Tecnológico Y 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. - Afectación a la salud del personal por COVID.	Técnicos responsables de la Coordinación de Redes y Soporte Informático	Muy Probable	Grave					Riesgo Extremo
RO	2.2 Administración y mantenimiento de Accesos de Redes Inalámbricas	Riesgo Tecnológico Y Riesgo Operacional	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	2.3 Implementación y Mantenimiento de mecanismos de seguridad de accesos a redes de datos	Riesgo TecnológicoRiesgo Político	Accesos a equipos informáticos por usuarios no autorizados.Falta de seguimiento a Gobierno Digital	Coordinación de Infraestructura y Seguridad.	Muy Probable	Grave					Riesgo Extremo
RO	2.4 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	2.5 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	2.6 Realización de mejoras a la infraestructura de las aplicaciones informáticas implementadas	Riesgo Tecnológico y Operacional	Usuarios de correo institucional acceden o abren correos fraudulentos que contienen SPAM, virus o Phishing.	Coordinador de área o encargado de correos	Muy Probable	Muy Serio					Riesgo Extremo
RO	2.7 Administración del servicio de correo electrónico	Riesgo Estratégico	Desconocimiento de la plataforma	Coordinador de área o Responsable de Curso.	Alta Probabilidad	Serio					Riesgo Alto.
RO	2.7 Administración del servicio de correo electrónico	Riesgo Estratégico	Resistencia al cambio por parte de los usuarios	Coordinador de área o Responsable de Curso.	Alta Probabilidad	Serio					Riesgo Alto.
RO	3. Cursos gestionados en la plataforma virtual para la educación tecnológica										
RO	3.1. Administración de la plataforma para la enseñanza virtual	Riesgo Operacional	Falla en Internet o deficiencia en la velocidad y ancho de banda necesarios para realizar videoconferencias.	Coordinador de área o Responsable de Curso.	Alta Probabilidad	Serio					Riesgo Alto.
	3.2 Desarrollo de capacitaciones de herramientas de ofimática orientados a la nube.	Riesgo Estratégico	Resistencia al cambio por parte de los usuarios	Coordinador de área o Responsable de Curso.	Alta Probabilidad	Serio					Riesgo Alto.
RO	5. Implementados y actualizados los sistemas informáticos institucionales.										
RO	5.1 Desarrollo e Implementación de nuevos Sistemas informáticos y actualizaciones a sistemas existentes	Riesgo Estratégico	Falta de capacitación al personal en nuevas tecnologías.	Jefatura y coordinador del área.	Alta Probabilidad	Muy Serio					Riesgo Extremo
RO	6. Administrados los sitios web institucionales.										

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	6.1 Mantenimiento a sitios web institucionales	Riesgo Operacional	Alta demanda solicitudes de nuevos sitios web institucionales y no exista personal suficiente para cubrir la demanda. Desactualización de contenido y de complementos.	Coordinador de área o encargado de sitio web.	Alta Probabilidad	Muy Serio					Riesgo Extremo

V. Gestión del Riesgo.

Riesgos	Gestión del Riesgo
• 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.
• 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 de la unidad. • Manipulación inadecuada de equipos informáticos por parte de los usuarios y personas ajenas a la institución. • Falta de políticas para asignación de equipos informáticos hacia usuarios que posee equipo desfasados. • Afectación a la salud del personal por COVID.	• 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.
• Falta de asignaciones de transporte para visitas a dependencias. • Afectación a la salud del personal por COVID.	• 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.
• Falta de asignaciones de transporte para visitas a dependencias.	• Gestionar apoyo de transporte asignado para cobertura de rutas en jornadas completas para

Riesgos	Gestión del Riesgo
• Afectación a la salud del personal por COVID.	abarcar la mayor cantidad de dependencias posibles. • Trasladar responsabilidades de soporte y redes hacia otros compañeros que se encuentren en buen estado de salud.
• Fallas en los enlaces de datos por parte del Proveedor de Servicios de Internet. • Falta de asignaciones de transporte para visitas a dependencias. • Afectación a la salud del personal por COVID.	• Brindar un mantenimiento periódico a las redes de comunicación de datos en las dependencias de la institución solicitando al proveedor 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.
• 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.
• Accesos a equipos informáticos por usuarios no autorizados.	• Realizar campañas de concientización de usuarios para evitar ser víctima de fraude electrónico y las implicaciones que conlleva no notificar de algún comportamiento extraño de los equipos informáticos bajo su responsabilidad.

Riesgos	Gestión del Riesgo
• 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.
• 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.
• Usuarios de correo institucional acceden o abren correos fraudulentos que contienen SPAM, virus o Phishing.	• Realizar campañas constantes para capacitar y concientizar a los usuarios para identificar correos SPAM y la forma de eliminarlos.
• 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.
• 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.
• Constantes ataques de denegación de servicios o intentos de vulneración la seguridad de los sitios web institucionales.	• 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.
• Que se presente una alta demanda de cambio o solicitudes de nuevos sitios web institucionales y no exista personal suficiente para cubrir la demanda.	• 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	1. Intervenidos los Equipos informáticos	Equipos intervenidos				Equipos Informáticos	36													
RO	1.1 Atención a 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	$10,291.00	1	1	1	1	1	1	1	1	1	1	1	1
RO	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	$0.00	1	1	1	1	1	1	1	1	1	1	1	1
RO	1.3 Actualización de Inventario de equipos informáticos		Informe Mensual de Equipos Informáticos Inventariados	A101.3.1-01 Mantenimiento y soporte informático	Mercedes Santamaría	Cantidad de equipos intervenidos	12	$0.00	1	1	1	1	1	1	1	1	1	1	1	1
RO	2. Controlada la Infraestructura informática de la institución	Infraestructura Informática controlada				Servicios	16													
RO	2.1 Realización de mantenimiento a redes de datos		Informe mensual de redes de datos atendidas	A101.3.3-01 Seguridad y accesos informáticos	José Aragón	Informe	4	$6,215.00			1			1			1			1
RO	2.2 Administración y mantenimiento de Accesos de Redes Inalámbricas		Informe semestral de configuraciones de administración realizadas en el centro de datos	A101.3.3-01 Seguridad y accesos informáticos	Jorge Batres	Informe	2							1						1
RO	2.3 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	2.4 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	2.5 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	2.6 Administración del servicio de correo electrónico institucional.		Informe semestral de servicio de correo electrónico institucional	A101.3.2-02 Medios de comunicación electrónica	Claudia de Campos, Jorge Batres	Informes	2							1						1
RO	3. Cursos gestionados en la plataforma virtual para la educación tecnológica	Número de Cursos gestionados				Cursos	4													
RO	3.1 Desarrollo de capacitaciones de plataforma de Google Suite		Listas de asistencia de participantes de cursos	A101.3.2-04 Educación tecnológica	Teo de Renderos, Claudia de Campos	Cursos	4			1			1			1			1		
RO	4. Proporcionados los Accesorios informáticos a usuarios.	Accesorios informáticos proporcionados				Accesorios Informáticos	12	$2,190.00												
RO	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	5. Implementados y actualizados los sistemas informáticos institucionales.	Sistemas Informáticos nuevos o actualizados				Sistemas	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	5.1 Desarrollo e Implementación de nuevos Sistemas informáticos y actualizaciones a sistemas existentes		Sistema en funcionamiento	A101.3.2-01 Aplicaciones informáticas	Leonel López, Teo de Renderos, William Pineda, Claudia de Campos	Sistemas	2							1						1
RO	6. Administrados los sitios web institucionales.	Sitios web administrados			William Pineda, Claudia de Campos	Sitios web	2													
RO	6.1 Mantenimiento a sitios web institucionales		Sitio web en funcionamiento	A101.3.2-03 Medios de Comunicación Web	William Pineda, Claudia de Campos	Sitios Web	2							1						1
LAIP	1. Obtenido el nivel óptimo de información oficiosa actualizada y disponible.	Número de información entregada				Información	4													
LAIP	1.1 Presentar informe cada trimestre (enero, abril, julio y octubre) de la información de tipo oficiosa identificada que se deberá actualizar y reportar.		Memorándum e información entregada	A101.3-01 Correspondencia (interna y externa)	Vangie Vigil	Información	4		1			1			1			1		
LGDA	1. Implementado el sistema institucional de gestión documental y archivos, a partir del avance experimentado en 2022.	Número de inventarios				Inventarios	12													
LGDA	1.2 Elaborar inventarios documentales de las series: A101.3.01, A101.3.1.03, A101.03.05, y año: 2023.		Inventario elaborado por serie documental	A101.3-01 Correspondencia (interna y externa)	Vangie Vigil	Inventario	12		1	1	1	1	1	1	1	1	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
LMA	4. Implementadas medidas a favor del medio ambiente y eficiencia energética						2													
LMA	4.1 Instruir al personal por medio de al menos dos memorándums al año para cumplimiento del reciclaje, basados en el Plan Institucional de Manejo Integral de los desechos sólidos en oficinas centrales		Memorándums dirigidos al personal	A101.3-01 Correspondencia (interna y externa)	Jefe de la UIS	Memorándum	2					1				1				
LMA	5. Fortalecida la educación ambiental del personal de la institución a través de capacitaciones, talleres, mensajes de sensibilización y otros.	Número de acciones medioambientales				Acción	2													
LMA	Participar en talleres de manualidades con reciclaje que se realizará con el apoyo de otras unidades del Ministerio		Invitaciones a talleres por parte de la DG ambiental	A101.3-01 Correspondencia (interna y externa)	Jefe de la UIS	Invitaciones	2						1					1		
LIE	1. Desarrolladas actividades que promueven la igualdad, equidad y erradicación de la violencia y discriminación de género con personal, en los meses de marzo, junio y noviembre 2023	Número de participaciones				Acción	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	1.1. Gestión y participación en actividades de sensibilización y capacitación relacionadas a la cultura de igualdad, equidad y no discriminación para fomento y garantía de derechos de mujeres, población LGBTIQ+, afro descendencia y pueblos indígenas.		Lista de asistencia de participación	A101.3-01 Correspondencia (interna y externa)	Jefatura y Equipo de Trabajo	Participación	3				1			1					1	

DIRECCIÓN GENERAL DE ADMINISTRACIÓN UNIDAD DE INFORMÁTICA Y SISTEMAS MINISTERIO DE CULTURA REPÚBLICA DE EL SALVADOR EN LA AMÉRICA CENTRAL GOBIERNO DE EL SALVADOR

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

VII. Autorización.

Autorizado: _____

Mariemm Pleitez
Ministra de Cultura.

Revisado: _____

Lcda. Claudia Ramírez de Iglesias
Directora General de Planificación y Desarrollo Institucional

VoBo: _____

Lic. José Napoleón Zepeda Carías
Director General de Administración

Formulado y Elaborado: _____

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

_____

Vangie Grissel Vigil León
Técnico Enlace

Fecha de Autorización: ENE 2023