GOBIERNO DE EL SALVADOR

MINISTERIO DE CULTURA

MINISTERIO DE CULTURA
DIRECCIÓN GENERAL DE ADMINISTRACIÓN

UNIDAD DE INFORMÁTICA Y SISTEMAS

PLAN OPERATIVO ANUAL
AÑO 2022

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

EL SALVADOR, 2022

INDICE

I. INTRODUCCIÓN. 3

II. OBJETIVOS DEL POA 3

III. ANÁLISIS DEL ENTORNO. 4

IV. IDENTIFICACIÓN DEL RIESGO. 7

V. GESTIÓN DEL RIESGO. 10

VI. PROGRAMACIÓN DE ACTIVIDADES. 12

VII. AUTORIZACIÓN. 17

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 2022 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 2021 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**
❖ Se cuenta con personal capacitado en: ❖ Cambio de repuestos de forma oportuna antes que falle alguna otra pieza. ❖ Limpieza de equipo informático. ❖ Impartir cursos de Microsoft Office 365. ❖ Adopción de nuevas tecnologías. ❖ Diseño y creación de sitios web. ❖ Diseño, creación y mantenimiento de redes de datos. ❖ Hardware y software. ❖ Administración y control sobre: ❖ Dispositivos conectados a la red de datos institucional. ❖ Dispositivos de Red Inalámbricas. ❖ Equipos físicos, así como de los servicios que brinda el centro de Datos a nivel virtual. ❖ Herramientas y materiales adecuados para realización de mantenimiento de redes de datos. ❖ Completa constancia en la realización de mantenimientos semestrales. ❖ Equipos de Seguridad Actualizados. Controles de Accesos Informáticos. ❖ Apoyo Financiero para Actualización de equipos de Seguridad Informática. ❖ Se dispone de herramientas de protección anti SPAM. ❖ Creación de una herramienta informática para registro y actualización de inventario de equipos. ❖ Se tiene disponible la consulta 7/24 de correos vía cliente web. ❖ Se dispone de un cliente de correo de tipo open sourse que no requiere. licenciamiento para la administración de correos.	❖ Poco personal para atender la demanda de creación y desarrollo de cursos virtuales, nuevos sistemas y sitios web. ❖ Personal con múltiples actividades asignadas reducen la cantidad de cursos y contenido a impartir en el año. ❖ Falta de capacitación al personal en nuevas tecnologías. ❖ 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 ❖ 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.

Factores Internos	
Fortalezas	**Debilidades**
❖ Disponibilidad de forma ágil y oportuna de consultar en línea la información de equipos y usuarios según inventario informático realizado. ❖ Poder contar con herramienta informática para control de entregas de accesorios a los usuarios.	

Factores Externos	
Oportunidades	**Amenazas**
❖ Gestiones de apoyo: 1. En soporte técnico con estudiantes en Servicio Social o Práctica Profesional. 2. En soporte técnico externo por parte de proveedores y fabricantes. 3. Para actividades de mantenimiento preventivo con estudiantes en Servicio Social o Práctica Profesional. ❖ Mantener conexión de redes de datos estable en oficinas centrales y dependencias del Ministerio de Cultura. ❖ Monitoreo del funcionamiento de la red de datos y de las redes para corroborar el correcto uso por parte de los usuarios que tengan dicho privilegio. ❖ 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	❖ Retraso en la cobertura de requerimientos por aumento de la demanda de servicios debido a la falta de personal de la unidad. ❖ 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. ❖ Afectación a la salud del personal por COVID. ❖ Fallas en los enlaces de datos por parte del Proveedor de Servicios de Internet afectando este a los empleados. ❖ Que personal que posea las contraseñas de acceso a las redes inalámbricas proporcionen dicho acceso a usuarios no autorizados. ❖ Hackers, usuarios internos inconformes. ❖ Constantes ataques de SPAM o virus que vulnere la seguridad del servicio de correo electrónico institucional, así como usuarios que acceden o abren correos fraudulentos que contienen SPAM, virus o Phishing.

Factores Externos	
Oportunidades	**Amenazas**
de los eventos solucionados y no solucionados en los equipos de centro de Datos. ❖ Existe material de apoyo disponible en Internet para reforzar los contenidos de los cursos impartidos. ❖ Se cuenta con apoyo de la Secretaría de Innovación para la donación de sistemas para implementar en la institución. ❖ 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.	❖ Cambios de gobierno que no apoyen la transformación digital. ❖ Resistencia al cambio por parte de Usuarios Finales. ❖ 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. ❖ Presupuesto económico limitado para compra de. ❖ Repuestos y accesorios informáticos ❖ Insumos y herramientas de limpieza de equipos. ❖ Materiales y herramientas para mantenimiento de redes de datos. ❖ Insumos para limpieza de equipos. ❖ Repuestos informáticos por alta demanda de insumos en oficinas centrales y dependencias. ❖ Materiales y herramientas para mantenimiento de redes de datos. ❖ Accesorios informáticos para suplir necesidades de usuarios en Oficinas Centrales y Dependencias. ❖ Cambio por prioridades institucionales que derivan en cambios a la planificación interna establecida. ❖ Retraso en la cobertura de requerimientos por aumento de la demanda de servicios debido a la falta de personal de la unidad.

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	❖ Retraso en la cobertura de requerimientos por aumento de la demanda de servicios debido a la falta de personal de la unidad. ❖ 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. ❖ 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			Alta Probabilidad	Muy Serio					Riesgo Extremo
RO	1.3 Actualización de Inventario de equipos informáticos	Riesgo Operacional			Alta Probabilidad	Serio					Riesgo Alto.
RO	2. Controlada la Infraestructura informática de la institución										

Códigos	Resultados y Acciones	Identificación del riesgo			Análisis del riesgo						Descripción de la calificación del riesgo
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 Tecnológico Riesgo 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
RO	2.6 Realización de mejoras a 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

Códigos	Resultados y Acciones	Identificación del riesgo			Análisis del riesgo						Descripción de la calificación del riesgo
RO	3. Realizado el Mantenimiento de Plataforma para 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.
RO	4. Proporcionados los Accesorios informáticos a usuarios										
RO	4.1 Administración de los accesorios informáticos	Riesgo Operacional	❖ Falta de asignación de presupuesto para adquisición de accesorios informáticos.	Técnico responsable de suministro de accesorios	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.										
RO	6.1 Creación y mantenimiento a sitios web institucionales	Riesgo Operacional	❖ Que se presente una alta demanda de cambio o solicitudes de nuevos sitios web institucionales y no exista personal suficiente para cubrir la demanda.	Jefatura y Coordinador de área	Alta Probabilidad	Muy Serio					Riesgo Extremo

V. Gestión del Riesgo.

N°	Riesgos	Gestión del Riesgo
1.	Retraso en la cobertura de requerimientos por aumento de la demanda de servicios debido a la falta de personal de la unidad.	❖ 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.
2.	Falta de asignaciones de transporte para visitas a dependencias.	❖ 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. ❖ Gestionar apoyo de transporte asignado para cobertura de rutas en jornadas completas para abarcar la mayor cantidad de dependencias posibles.
3.	Manipulación inadecuada de equipos informáticos por parte de los usuarios y personas ajenas a la institución.	❖ Divulgar medidas de prevención para conservación y buen uso de los recursos informáticos.
4.	Falta de políticas para asignación de equipos informáticos hacia usuarios que posee equipo desfasados.	❖ 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.
5.	Afectación a la salud del personal por COVID.	❖ Trasladar responsabilidades de soporte y redes hacia otros compañeros que se encuentren en buen estado de salud.
6.	Falla en el correcto funcionamiento de los medios de conexión inalámbricas por problemas en los equipos físicos	❖ Generar políticas de respaldo de configuraciones de los dispositivos.
7.	Fallas en los enlaces de datos por parte del Proveedor de Servicios de Internet.	❖ 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.
8.	Pérdida de configuraciones o defectuosas en su caso, producto de interrupciones de energía eléctrica.	❖ Generar políticas de respaldo de configuraciones de los dispositivos.
9.	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.
10.	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. ❖ Generar políticas de respaldo de configuraciones y servicios de los dispositivos que componen el centro de Datos.
11.	Falta de Seguimiento a Gobierno Digital	❖ Adquirir equipos de protección especializados para Sitios Web.
12.	Falla en los equipos físicos 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 renovación de los equipos del centro de Datos que ya hayan excedido su periodo de vida útil.
13.	Fallas por ataques Informáticos.	❖ Generar políticas de creación de claves de alta complejidad y de cifrado de archivos de respaldo.
14.	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.
15.	Falla en Internet o deficiencia en la velocidad y ancho de banda necesarios para realizar videoconferencias.	❖ Gestión de requerimiento de ancho de banda especial, con el área de Infraestructura previo a las sesiones de videoconferencia. ❖ Preparación de videos con clases pregrabadas para consulta de manera asíncrona por parte de los participantes de los cursos.
16.	Falta de asignación de presupuesto para adquisición de accesorios informáticos.	❖ Gestionar alternativas financieras para obtener los recursos necesarios para adquisición de accesorios informáticos.
17.	Falta de capacitación al personal en nuevas tecnologías para desarrollo de sistemas.	❖ Solicitar capacitaciones especializadas para el personal del área. ❖ Programación de capacitación interna, aprovechando la experticia de parte del nuevo personal, para replicarlo en toda el área.
18.	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	12													
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	Coordinadora	Cantidad de Usuarios atendidos	12	$12,869.00	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	Técnico	Cantidad de equipos intervenidos	12		1	1	1	1	1	1	1	1	1	1	1	1
RO	1.3 Actualización de Inventario de equipos informáticos		Informe Mensual de Atención de equipos informáticos	A101.3.1-01 Mantenimiento y soporte informático	Técnico	Cantidad de equipos intervenidos	12		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 trimestral de redes de datos atendidas	A101.3.3-01 Seguridad y accesos informáticos	Técnico	Informe	4	$4,690.00			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	2.2 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	Coordinador	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	Técnico	Informe	4				1			1			1			1
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	Coordinador y Técnico	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	Coordinador y Técnico	Informe	2							1						1
RO	2.6 Administración del servicio de correo electrónico		Informe semestral de servicio de correo electrónico institucional	A101.3.2-02 Medios de comunicación electrónica	Coordinadora	Informes	2							1						1
RO	3. Cursos gestionados en la plataforma virtual para la educación tecnológica	Número de Cursos gestionados				Cursos	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
RO	3.1 Desarrollo de Cursos de Microsoft Office 365 en nivel básico, intermedio y avanzado.		Listas de asistencia de participantes de cursos	A101.3.2-04 Educación tecnológica	Coordinadora y Técnicos	Cursos	3					1				1			1	
RO	4. Proporcionados los Accesorios informáticos a usuarios.	Accesorios informáticos proporcionados				Accesorios informaticos	12													
RO	4.1 Administración de los accesorios informáticos		Informe Mensual de Entregas de Accesorios Informáticos	A101.3.1.03 Correspondencia	Técnico	Accesorios entregados	12	$2,875.00	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 Informáticos	4													
RO	5.1 Desarrollo e Implementación de nuevos Sistemas informáticos y actualizaciones a sistemas existentes		Requerimientos	A101.3.2-01 Aplicaciones informáticas	Coordinadora y Técnicos	Sistemas	4				1			1			1			1
RO	6. Administrados los sitios web institucionales.	Número de Sitios web				Sitios Web	2													
RO	6.1 Creación y mantenimiento a sitios web institucionales		Sitio Web	A101.3.2-03 Medios de Comunicación Web	Coordinadora y Técnico	Sitio web	2							1						1
LAIP	1. Obtenido el nivel óptimo de información oficiosa actualizada y disponible.	Numero de información entregada				Información	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
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)	Técnico	Información	4		1			1			1			1		
LGDA	1. Implementado el sistema institucional de gestión documental y archivos, SIGDA.	Número de inventarios de las series documentales elaboradas.				Inventario	24													
LGDA	1.1 Elaborar inventarios de cada serie documental, contenidos en la tabla de clasificación		Inventarios de las series documentales elaboradas	A101.3-01 Correspondencia (interna y externa)	Técnico	Inventario	12		1	1	1	1	1	1	1	1	1	1	1	1
LGDA	1.2 Realizar la valoración documental por serie documental y elaborar la tabla de plazos de conservación		Formulario lleno	A101.3-05 Expedientes de procesos administrativos	Técnico	Formulario	12		1	1	1	1	1	1	1	1	1	1	1	1
LMA	1.Implementadas medidas a favor del medio ambiente y eficiencia energética.	Número de medidas implementadas				Acción	1													
LMA	1.1 Instalación de mensajes de ahorro y energía en tomas y apagadores.		Registro fotográfico impreso	A101.3-01 Correspondencia (interna y externa)	Jefe de la UIS	Acción	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
Género y Diversidad	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 de 2022	Número de participaciones				Acción	3													
Género y Diversidad	1.1 Gestión y participación en actividades relacionadas a la igualdad, equidad, no violencia y no discriminación en el ambiente laboral.		Solicitud y lista de asistencia de participación	A101.3-01 Correspondencia (interna y externa)	Jefatura y equipo técnico	Participación	3					1			1				1	

VII. Autorización.

Autorizado:

Maestra Mariemm Eunice Pleitez Quiñónez
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: MAR 2022