



MINISTERIO
DE CULTURA

GOBIERNO
DE EL SALVADOR

MINISTERIO DE CULTURA

Dirección Administrativa

Departamento de Informática y Sistemas

PLAN OPERATIVO ANUAL DE TRABAJO AÑO 2019

Presentado por:

Ing. Ricardo Ulises Contreras Brito



San Salvador, Diciembre de 2018



ÍNDICE

I. INTRODUCCIÓN.....	3
II. OBJETIVOS.	4
III. ELABORACIÓN DE DIAGNÓSTICO	5
IV. MATRIZ DE RIESGO Y ACCIONES DE CONTINGENCIA.	8
V. VIGENCIA Y AUTORIZACIÓN	12
VI. CRONOGRAMA	13



[Handwritten signature]

I. INTRODUCCIÓN.

En cumplimiento de la razón de ser del Departamento de Informática y Sistemas, de proveer y promover el uso adecuado de tecnologías y redes de comunicación, proporcionando la infraestructura informática y administrando el personal especializado que brinde apoyo y soluciones oportunas de forma planificada para los usuarios de las distintas Direcciones y dependencias de la Institución, se presenta el Plan Anual de Trabajo para el año 2019, proponiendo resultados y acciones que contribuyan para alcanzar los objetivos estratégicos y operativos en apoyo al desarrollo de actividades del Ministerio de Cultura.

El documento comprende resultados operativos como parte fundamental del departamento y los estratégicos definidos en Plan Estratégico Institucional; de igual forma se incluye la matriz de riesgos y acciones de contingencia identificadas por el departamento, finalizando con el cronograma de acciones que se desarrollará durante el año 2019.



II. OBJETIVOS.

A. General

Establecer y definir las acciones que el Departamento de Informática y Sistemas realizará durante el año 2019 y los resultados que se obtendrán de forma estratégica y operativa en apoyo al cumplimiento de los objetivos institucionales.

B. Específicos

- Adecuar los servicios que ofrece el Ministerio de Cultura para ponerlos a disposición de la población a través de los medios informáticos con que cuenta la institución.
- Brindar el servicio de soporte técnico informático de forma adecuada y oportuna.
- Mantener la infraestructura de redes de datos sobre los cuales se proporcionan los servicios de comunicación de forma segura y continua.
- Proveer los medios de comunicación web institucionales necesarios para la promoción y difusión del quehacer artístico y cultural.
- Mejorar las aplicaciones informáticas implementadas en apoyo a las necesidades de los usuarios de las dependencias para la prestación de los servicios.
- Mantener la infraestructura del centro de datos como componente indispensable en la prestación de los servicios informáticos que se brindan a los usuarios.



R

III. ELABORACIÓN DE DIAGNÓSTICO.

FORTALEZAS	OPORTUNIDADES
<p>F1 Posee la infraestructura tecnológica de seguridad y comunicaciones necesaria para prestar servicios informáticos a los usuarios.</p>	<p>O1 Países o entidades externas que realicen donaciones de equipos y licenciamiento de software a través de convenios de cooperación.</p>
<p>F2 Mantiene un ambiente laboral con buena comunicación y relaciones interpersonales.</p>	<p>O2 Instituciones de Educación Media y Superior, que proporcionen recurso humano en áreas técnicas especializadas mediante proyectos de servicio social.</p>
<p>F3 Cuenta con personal que posee conocimientos en las diferentes áreas técnicas para brindar soporte a usuarios y capacidad de trasladar el conocimiento.</p>	<p>O3 Aprovechamiento de capacitaciones a través de la Red de Capacitación Gubernamental, Instituciones u Organizaciones que apoyen con programas o convenios para compartir conocimientos, capacitaciones técnicas y experiencias en el uso de las tecnologías informáticas.</p>
<p>F4 Posee controles administrativos y herramientas informáticas establecidas para la prestación de servicios informáticos en la institución.</p>	<p>O4 Aprovechamiento de una amplia variedad de herramientas informáticas de código abierto que están disponibles para uso gratuito.</p>
<p>F5 Posee personal con alto grado de responsabilidad y compromiso con la institución.</p>	<p>O5 Aprovechamiento de proyectos de promoción y difusión de las TIC'S.</p>
<p>F6 Dispone de conocimientos y competencias técnicas necesarias para brindar asesoramiento en proyectos de tecnología.</p>	<p>O6 Asignación de presupuesto para adquisición de materiales, repuestos y accesorios que permiten apoyar en tareas de soporte técnico a usuarios de la institución y en licencias para el funcionamiento de la infraestructura de servidores que se adapta a las necesidades crecientes.</p>
<p>F7 Mantiene buenas relaciones con otras instituciones de gobierno.</p>	<p>O7 Existencia de control y visibilidad de las aplicaciones desplegadas en el centro de datos protegidas por una capa de seguridad perimetral.</p>
<p>F8 Posee un centro de datos con los equipos que permiten el alojamiento de aplicaciones informáticas con su respectiva protección y resguardo.</p>	<p>O8 Integración de los proyectos de Tecnología dentro del Marco de la Normativa de seguridad de la información.</p>
<p>F9 Dispone de nuevo enfoque de protección, defensa preventiva, activa y pro-activa del flujo de datos generado por las aplicaciones.</p>	
<p>F10 Equipo de Infraestructura tecnológica, cuenta con software operativo actualizado en</p>	



sus últimas versiones (software libre).	
F11 Disposición de la administración para responder a cambios tecnológicos y realización de proyectos.	
DEBILIDADES	AMENAZAS
<p>D1 Insuficiente personal técnico informático para cubrir los puestos de trabajo que las coordinaciones requieren.</p> <p>D2 Sobrecarga de trabajo para el personal de las coordinaciones.</p> <p>D3 El personal presenta un alto grado de reincidencia en problemas de salud derivados del estrés</p> <p>D4 Prolongados tiempos de atención a fallas de los requerimientos informáticos de los usuarios de la institución.</p> <p>D5 Carencia de licencias de programas especializados para implementación de control de usuarios y limitado servicio de correo electrónico.</p> <p>D6 Falta de recursos económicos para adquirir licencias de programas de ofimática actualizados, de diseño gráfico y multimedia como apoyo a la realización de actividades laborales.</p> <p>D7 Centro de Datos central que opera en condiciones mínimas, pero no cumple los estándares de acceso a instalaciones, condiciones físicas, eléctricas y de contingencia.</p> <p>D8 No se tiene acceso a capacitaciones técnicas informáticas, lo cual limita el aprovechamiento eficiente de los recursos tecnológicos actuales.</p> <p>D9 Carencia de programa para actualización de licencias de sistemas operativos y ofimática de equipos institucionales por falta de presupuesto para su implementación.</p> <p>D10 Limitado apoyo del servicio de transporte institucional para desplazamiento a dependencias de usuarios que demandan asistencia informática presencial.</p>	<p>A1 Insuficiente asignación presupuestaria a proyectos de fortalecimiento de infraestructura tecnológica.</p> <p>A2 Falla en los equipos de acondicionamiento ambiental para el funcionamiento adecuado del centro de datos central.</p> <p>A3 Usuarios sin adiestramiento en el uso de tecnologías y servicios brindados.</p> <p>A4 Fallas en los enlaces de comunicaciones de la institución.</p> <p>A5 Fallas inminentes de los equipos informáticos que en su mayoría cumplieron su vida útil.</p> <p>A6 Posibilidad de ataques contra la seguridad de la infraestructura de comunicaciones.</p> <p>A7 Catástrofes naturales.</p> <p>A8 Falta de apoyo sistemático por parte de instituciones educativas en proporcionar estudiantes para realizar actividades en áreas técnicas informáticas.</p> <p>A9 Insuficiente asignación presupuestaria a proyectos de fortalecimiento de infraestructura tecnológica.</p> <p>A10 Altos costos de la tecnología.</p>



D11 Alta resistencia al cambio por parte de los usuarios con las herramientas o programas con licenciamiento libre.

D12 Documentación deficiente o desactualizada

D13 Falta de trabajo en equipo de las áreas usuarias con el Área de Sistemas.

D14 Monitoreo insuficiente de procesos, dispositivos y equipos.

D15 Carencia de un espacio y equipo adecuado para brindar capacitaciones a los usuarios de la institución en temáticas de tecnología y ofimática.

A11 Redes de comunicaciones externas inestables.

A12 Ataques a la infraestructura informática

A13 Limitados recursos de infraestructura para la implementación de nuevas aplicaciones que demanden capacidad de almacenamiento y velocidad de procesamiento.



IV. MATRIZ DE RIESGO Y ACCIONES DE CONTINGENCIA.

Riesgos	Probabilidad de amenaza	Magnitud de daño	Resultado
Falta de disponibilidad presupuestaria para ejecución de actividades y proyectos de funcionamiento de la infraestructura informática bajo responsabilidad del departamento.	4	4	16
Afectación en la continuidad de la prestación de los servicios informáticos debido a catástrofes naturales, incendios, siniestros y fallas en el suministro eléctrico.	4	4	16
Fallas en el sistema de enfriamiento del centro de datos.	4	4	16
Falta de presupuesto asignada para el mantenimiento de la infraestructura tecnológica.	4	4	16
Fallas en funcionamiento o nuevas necesidades de mejora en las aplicaciones informáticas implementadas y sitios web institucionales.	4	4	16
Imposibilidad de apoyar nuevos proyectos de desarrollo por la falta de personal y los problemas de salud recurrentes en el personal existente además de la sobrecarga de trabajo.	4	4	16
Retraso en la cobertura de requerimientos por aumento de la demanda de servicios debido a la falta de personal del departamento.	4	4	16
Fallas en los servicios informáticos debido a ataques de seguridad en los equipos de la infraestructura tecnológica del centro de datos.	3	4	12
No proporcionar licencias de software para solventar necesidades laborales de los usuarios de equipos informáticos institucionales.	3	4	12
Retraso en la prestación del servicio de soporte técnico a usuarios, por falta de apoyo oportuno del transporte institucional para desplazamiento hacia las dependencias.	4	3	12
No contar con un espacio o plataforma informática para brindar capacitaciones técnicas al personal de la institución en el uso de herramientas de ofimática para el desarrollo de sus actividades.	3	3	9



Falta de comunicación de las redes de datos de las dependencias debido a fallas en los enlaces de comunicación del proveedor de Internet	2	4	8

La matriz se basa en el método de análisis de riesgo, usando la fórmula del riesgo:

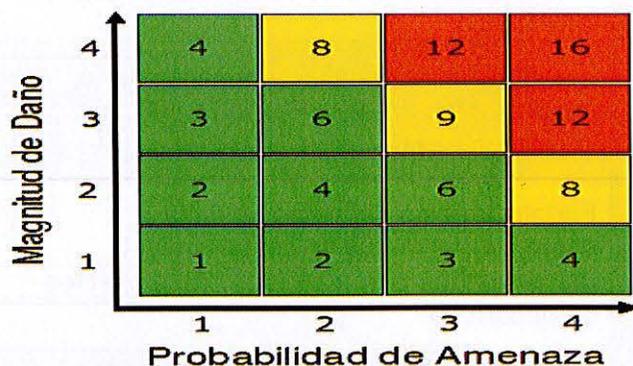
Riesgo = Probabilidad de amenaza X magnitud de daño

La matriz toma valores como los siguientes:

- 1 = Insignificante. 2 = Baja.
- 3 = Mediana. 4 = Alta.

El riesgo es el producto, de la multiplicación de la probabilidad de amenaza por la magnitud de daño se encuentra en tres rangos de diferentes colores:

- Bajo riesgo = 1 al 6 **color verde**.
- Mediano riesgo = del 8 al 9, **color amarillo**.
- Alto riesgo = de 12 al 16, **color rojo**.



ACCIONES DE CONTINGENCIA

Riesgos	Acciones contingenciales
Falta de disponibilidad presupuestaria para ejecución de actividades y proyectos de funcionamiento de la infraestructura informática bajo responsabilidad del departamento.	Gestionar alternativas financieras para obtener los recursos informáticos necesarios en la ejecución de actividades y proyectos institucionales.





<p>Afectación en la continuidad de la prestación de los servicios informáticos debido a catástrofes naturales, incendios, siniestros y fallas en el suministro eléctrico.</p>	<p>Divulgar medidas de prevención para buen uso y conservación de los recursos informáticos, así como también la construcción de redes de datos y ubicación de equipos de comunicación en lugares aislados del ambiente que pueda perjudicar el buen funcionamiento de los mismos. Gestionar el establecimiento de infraestructura virtual para la contingencia en caso de daños en la infraestructura tecnológica del centro de datos. Gestionar planes de contingencia para el restablecimiento de los servicios informáticos, en coordinación con la Coordinación de Infraestructura Informática.</p>
<p>Fallas en el sistema de enfriamiento del centro de datos.</p>	<p>Implementar un sistema alterativo para garantizar la disponibilidad de la infraestructura informática y evitar la pérdida de información y daño de equipos informático.</p>
<p>Falta de presupuesto asignada para el mantenimiento de la infraestructura tecnológica.</p>	<p>Gestionar con las autoridades asignación de presupuesto para asegurar y garantizar el funcionamiento óptimo de la infraestructura informática.</p>
<p>Fallas en funcionamiento o nuevas necesidades de mejora en las aplicaciones informáticas implementadas y sitios web institucionales.</p>	<p>Elaboración de planificación para realizar mejoras a las aplicaciones informáticas implementadas.</p>
<p>Imposibilidad de apoyar nuevos proyectos de desarrollo por la falta de personal y los problemas de salud recurrentes en el personal existente además de la sobrecarga de trabajo.</p>	<p>Fortalecimiento del personal de la coordinación mediante convenios con universidades para desarrollo de proyectos de desarrollo.</p>
<p>Retraso en la cobertura de requerimientos por aumento de la demanda de servicios debido a la falta de personal del departamento.</p>	<p>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 para que apoyen en actividades técnicas de la Coordinación de Redes y Soporte Informático.</p>
<p>Fallas en los servicios informáticos debido a ataques de seguridad en los equipos de la infraestructura tecnológica del centro de datos.</p>	<p>Implementar nuevas tecnologías de seguridad de accesos para proteger la infraestructura tecnológica del centro de datos. Oportunidad de implementar</p>



Handwritten signature





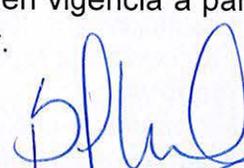
	infraestructura virtual para ampliar alcance de la protección de la infraestructura tecnológica de la institución
No proporcionar licencias de software para solventar necesidades laborales de los usuarios de equipos informáticos institucionales.	Recomendar el gestionar donación de licencias de software especializado para uso en equipos informáticos institucionales que lo requieran. Proponer el uso de programas alternativos para paliar las necesidades de licencias de software.
Retraso en la prestación del servicio de soporte técnico a usuarios, por falta de apoyo oportuno del transporte institucional para desplazamiento hacia las dependencias.	Brindar atención de requerimientos de forma remota para los casos en que sea factible apoyar a los usuarios de forma no presencial. Gestionar apoyo de transporte asignado para cobertura de rutas en jornadas completas para abarcar la mayor cantidad de dependencias posibles.
No contar con un espacio o plataforma informática para brindar capacitaciones técnicas al personal de la institución en el uso de herramientas de ofimática para el desarrollo de sus actividades.	Realizar gestiones para la implementación de la plataforma virtual, además de realizar medidas alternativas para el traslado del conocimiento a los usuarios.
Falta de comunicación de las redes de datos de las dependencias debido a fallas en los enlaces de comunicación del proveedor de Internet	Gestionar con las autoridades asignación de presupuesto para asegurar y garantizar el funcionamiento óptimo de la infraestructura informática. Brindar un mantenimiento periódico a las redes de comunicación de datos en las dependencias de la institución. Gestionar mejoras en las especificaciones técnicas en la contratación del servicio de enlaces de comunicaciones con los proveedores. Concientizar a las autoridades sobre la importancia de contar con un sitio de contingencia y mantener un plan de respaldo sistemático para las aplicaciones en funcionamiento.



V. VIGENCIA Y AUTORIZACIÓN.

El presente plan, entrará en vigencia a partir de la autorización de la Ministra de Cultura de El Salvador.

Autorizado:


Maestra Silvia Elena Regalado
Ministra de Cultura.

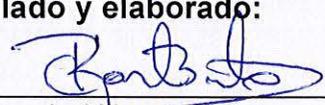
Vo.Bo.:


Lic. José Manuel Rivas Zacatares
Director Administrativo.

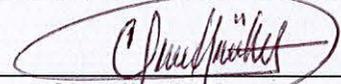
Revisado:

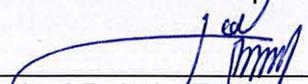

Licda. Claudia Ramírez de Iglesias
Jefe del Unidad de Planificación y Desarrollo Institucional

Formulado y elaborado:


Ing. Ricardo Ulises Contreras Brito
Jefe del Departamento de Informática y Sistemas


Ing. Angela Merino de Barahona
Jefe de Sección de Redes y Soporte Técnico


Ing. Claudia de Campos
Jefe de Sección de Aplicaciones y Medios Informáticos


Ing. Joel Beltrán Zaldrán
Jefe de Sección de Infraestructura Informática

Fecha de autorización:



