



Departamento de Informática

DI-PO-01-2014
Política Gestión de soporte técnico

Fecha de envío:
Enero, 2014

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	2 de 11

Política sobre gestión de soporte técnico	3
1. Objetivo	3
2. Alcance	3
3. Definiciones	3
4. Responsabilidad.....	3
5. Descripción	4
6. Fecha de creación, y entrada en vigencia de la Política	4
7. Lista de distribución.....	4
8. Referencia a otros documentos y Anexos	4
9. Sobre la administración de cambios.....	4
Áreas objeto de control de cambios	4
10. Sobre la administración de problemas.....	6
Áreas objeto de la administración de problemas	6
11. Sobre la administración de configuraciones	6
Áreas objeto de control en la gestión de configuraciones.....	6
12. Mantenimiento	7
Mantenimiento preventivo y correctivo	7
Mantenimiento adecuado	7
Bitácora de fallas y de mantenimiento	7
Instalación y mantenimiento del cableado	7
Revisión del cableado.....	7
Procedimientos de mantenimiento de equipos.....	7
13. Del registro de actividades de mantenimiento del personal operativo.....	8
Bitácoras de las actividades de mantenimiento del personal operativo.....	8
14. Del registro de fallas.....	8
Registro de fallas	8
De la obligación de establecer parámetros claros y procedimientos para el registro de fallas	9
De la obligación de establecer parámetros claros y procedimientos para el manejo de fallas	9
Responsabilidad de la Auditoría Interna en la revisión del manejo y corrección de fallas ..	9
Tratamiento de la falla cuando ésta corresponda a un incidente de seguridad	9
De la obligación de reportar fallas en los equipos, software y sistemas del Ministerio	9
De la obligación de soporte técnico de llevar bitácoras de manejo y solución de fallas	9
15. Mesa de Servicios como apoyo al esquema de soporte técnico.....	9
Mesa de Servicios.....	9
Disposiciones finales	10

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
-------------------------	------------------------------------	--	--

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	3 de 11

Política sobre gestión de soporte técnico

1. Objetivo

La presente política tiene como objeto establecer los lineamientos y responsabilidades para recibir, catalogar y resolver solicitudes de cambios o modificaciones a los procesos existentes, asimismo pretende dar las directrices para la administración de configuración de los recursos tecnológicos y guiar en la resolución de los problemas relacionados con la tecnología, detectados en el Ministerio de Cultura y Juventud.

2. Alcance

Estas políticas son aplicables al personal encargado de brindar soporte técnico, así como las diferentes dependencias del Ministerio encargadas de la administración de problemas, configuraciones y cambios en los sistemas de información.

3. Definiciones

- ❖ **Problema:** causa subyacente desconocida de uno o más incidentes.
- ❖ **Incidente:** cualquier tipo de evento (o grupo de eventos) adverso, que no sea parte de la operación estándar, inesperado o no deseado, que tenga una alta probabilidad de amenazar, poner en riesgo o comprometer, o que efectivamente comprometa, interrumpa o cause una reducción en la calidad del servicio.

4. Responsabilidad

- ❖ **Comité Gerencial Informático:** ente encargado de velar por la Gestión del Gobierno de Tecnología, de tal forma que se garantice el alineamiento de los proyectos de tecnología con el cumplimiento de los objetivos institucionales del Ministerio.
- ❖ **Jefe del Departamento de Informática:** tiene la responsabilidad de:
 - a. Mejorar progresivamente la calidad del servicio ofrecido, su rentabilidad, y la satisfacción de los clientes y usuarios;
 - b. Evaluar la gestión de tecnología de la información en lo que corresponde a seguridad, integridad, disponibilidad y confidencialidad de los datos; y
 - c. Identificar, evaluar y controlar los riesgos presentes en el proceso de gestión de soporte técnico.
- ❖ **Auditoría Interna:** Evaluar los controles asignados a los riesgos de la gestión de soporte técnico en relación al diseño, implementación y la eficacia operativa de los mismos.

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
--------------------------------	---	---	---

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	4 de 11

5. Descripción

El Ministerio de Cultura y Juventud se encuentra en la obligación de gestionar adecuadamente el soporte técnico a/en sus sistemas y/o Recursos Informáticos. Para ello, debe dotarse de una normativa que le permita no sólo prevenir, solventar y monitorear los servicios de soporte a su plataforma tecnológica, sino también prevenir, detectar y registrar posibles violaciones a la misma y tomar las acciones correspondientes.

6. Fecha de creación, y entrada en vigencia de la Política

El presente documento fue creado en Enero de 2014, y se encuentra en plena vigencia desde Febrero 2014.

7. Lista de distribución

Las presentes políticas se distribuirán al personal directamente involucrado con su cumplimiento, únicamente en lo que a cada uno corresponda.

8. Referencia a otros documentos y Anexos

- Estándar en materia de Seguridad de la Información ISO/IEC 27002:2013;
- Estándar para la implementación de Sistemas de Administración de la Seguridad Informática ISO /IEC 27001:2013;
- Legislación costarricense aplicable a la materia (incluyendo la Ley General de Control Interno -No. 8292 de 31 de julio de 2002-, y Las Normas Técnicas para la Gestión y Control de las Tecnologías de la Información –No. R-CO-26-2007 del 7 de junio, 2007, entre otras);
- COBIT v. 4.1. en lo referente a seguridad de la información.
- Normas Técnicas para la Gestión y Control de las Tecnologías de Información (N-2-2007-CO-DFOE) Publicado en el Diario Oficial La Gaceta Nro. 119 del 21 de junio de 2007, conforme a resolución R-CO-26-2007

9. Sobre la administración de cambios

Áreas objeto de control de cambios

Se debe al menos controlar lo siguiente:

- Deben existir procedimientos formales, para cada una de las actividades involucradas en un cambio de hardware o software.
- Todos los cambios al ambiente de producción deben estar debidamente probados por quién corresponda en cada caso, y certificados por el área certificadora, que debe tomar las medidas que considere necesarias para aprobar el traspaso a producción. El área certificadora debe dar su visto bueno previo a cualquier cambio al ambiente de producción normal.

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
-------------------------	------------------------------------	--	--

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	5 de 11

- c) Todos los cambios deben estar debidamente documentados.
- d) Deben existir procedimientos establecidos que definan roles y responsabilidades en el proceso de desarrollo, mantenimiento e integración de hardware y software al ambiente de producción. Estos procedimientos deben considerar los controles necesarios para evitar traspasos no autorizados de componentes de hardware o software, al ambiente de producción.
- e) Se deben aplicar controles especiales para cambios efectuados en la infraestructura tecnológica (servidores, redes, entre otros) debido al impacto potencial que éstos implican y a la dificultad de ejercer control directo sobre terceros ajenos al Ministerio que participen en a dichas áreas.
- f) Los cambios de emergencia deben aplicar, en la medida de lo posible, los procesos de escalamiento y autorizaciones aprobados por el Ministerio para casos de normalidad. Sin embargo, si ello no fuera posible en el momento de éstos producirse, deberá tratar de ajustarse a lo planeado, una vez que se retorne a la normalidad después de realizado el cambio y basado en el procedimiento DI-PR-04 Gestión de Cambios.
- g) Los datos de entrada a las aplicaciones deben ser validados, de manera que se asegure sean correctos y adecuados.
- h) Se deben incorporar instancias de control en las aplicaciones, a fin de detectar cualquier corrupción de información debido a errores de procesamiento o actos deliberados.
- i) Deben existir controles que aseguren que los datos de salida fueron generados de acuerdo a lo requerido.
- j) Se debe restringir el acceso al código fuente de programas.
- k) Cada vez que se efectúen cambios a nivel de sistema operativo, las aplicaciones críticas deben ser revisadas y probadas de manera que se garantice que no habrá un impacto adverso en la operación o en la seguridad.
- l) El desarrollo de software por proveedores externos de la organización, debe ser supervisado y monitoreado.
- m) Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados y tomar las medidas apropiadas para tratar los riesgos asociados.
- n) No deben utilizarse datos de producción considerados sensibles, en ambientes de desarrollo o certificación.
- o) Deben ser seleccionados cuidadosamente los datos de prueba y ser protegidos y controlados según su naturaleza.
- p) Se deben establecer los planes de continuidad, de forma tal que se mitigue cualquier situación anómala a la hora de implementar algún cambio.
- q) Todos los cambios en aplicaciones deben ser desarrollados en un ambiente de prueba y validados o acreditados antes de entrar a regir en el ambiente de producción.

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
--------------------------------	---	---	---

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	6 de 11

- r) Los usuarios únicamente podrán tener permiso de lectura y ejecución sobre el ambiente de producción (ejecutables). El Departamento de Informática será, con exclusividad, el que tenga el control total del ambiente de producción (fuentes y ejecutables).

10. Sobre la administración de problemas

Áreas objeto de la administración de problemas

Se debe al menos controlar lo siguiente

- Es responsabilidad del personal del Departamento de Informática, en general, detectar problemas de manera proactiva y reactiva, adicionalmente, se debe clasificar el problema de acuerdo a su naturaleza (software, infraestructura, recurso humano y proveedores).
- Es responsabilidad del personal del Departamento de Informática, documentar e investigar el problema hasta llegar a la causa y definir la posible solución.
- Se deben realizar estudios de costo-beneficio para la implementación de la resolución de problemas.
- Debe existir una solicitud de cambio, que establezca la descripción de las características del nuevo requerimiento que dará solución al problema. Es responsabilidad del personal del Departamento de Informática y la jefatura de área involucrada, realizar estudios de costo-beneficio de la implementación de estas soluciones.
- Se debe ejecutar un cierre del problema bien sea cuando el costo y el esfuerzo no justifique el beneficio de resolución del mismo o cuando se ha resuelto definitivamente el problema de raíz y se ha validado con el usuario o áreas afectadas.
- Es responsabilidad del personal de Informática, comunicar al funcionario interno o área afectada, los cambios inherentes a la solución del problema, si es necesario, debe indicar igualmente, la documentación que se ha modificado.

11. Sobre la administración de configuraciones

Áreas objeto de control en la gestión de configuraciones

Se debe al menos controlar lo siguiente

- Se debe establecer una herramienta de apoyo y un repositorio central, que contenga la información pertinente sobre los elementos de configuración.
- Se deben establecer procedimientos de configuración para apoyar la gestión y registro de los cambios en el repositorio de configuración.
- Se deben realizar revisiones y verificaciones periódicas de la información que se considera para el proceso de gestión de configuración.

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
-------------------------	------------------------------------	--	--

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	7 de 11

12. Mantenimiento

Mantenimiento preventivo y correctivo

Los responsables de velar por el buen estado de la infraestructura del edificio y de que se le preste el oportuno y cuidadoso mantenimiento preventivo a los equipos de cómputo y de comunicaciones, así como de que se realicen las pruebas de funcionalidad, deben hacerlo es estricta conformidad con los procedimientos formalmente establecidos por la Departamento de Informática.

Mantenimiento adecuado

Los Recursos Informáticos deberán mantenerse en forma adecuada para asegurar que su disponibilidad e integridad sean permanentes.

Los Equipos Informáticos deberán mantenerse de acuerdo a los intervalos de servicio y especificaciones recomendados por el proveedor y en resguardo de las provisiones establecidas por las pólizas de seguro que les cubren. El mantenimiento deberá ser brindado únicamente por personal de mantenimiento autorizado.

Bitácora de fallas y de mantenimiento

Se debe llevar una bitácora de fallas (supuestas y reales) de los equipos del Ministerio, así como del mantenimiento preventivo o correctivo que se les ha brindado a los mismos.

Instalación y mantenimiento del cableado

La instalación y mantenimiento del cableado debe asignársele a por personal calificado y debidamente capacitado para los efectos, a fin de garantizar la seguridad e integridad del mismo.

Revisión del cableado

La seguridad del sistema de cableado del Ministerio debe ser revisada, cada vez que se produzca una actualización en el hardware y/o cada vez que haya cambios en las distintas áreas del Ministerio.

Procedimientos de mantenimiento de equipos

Cada dependencia del Ministerio debe asignar un responsable de velar por el buen estado de la infraestructura del edificio y porque se le preste el oportuno y cuidadoso mantenimiento preventivo y correctivo a los equipos de cómputo y de comunicaciones, así como por que se realicen las pruebas de funcionalidad que correspondan.

Deben crearse y aprobarse procedimientos de mantenimiento preventivo y correctivo que:

- Garanticen éstos sean llevados a cabo únicamente por personal autorizado;
- Garanticen la aplicación de los controles necesarios para proteger la información contenida en los equipos que son objeto de ellos;

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
-------------------------	------------------------------------	--	--

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	8 de 11

- c) Procuren los equipos se conserven en buen estado durante toda su vida útil;
- d) Cumplan con lo estipulado por el fabricante de los equipos (en término de intervalos de servicio y especificaciones) de manera que se conserven las garantías que le son inherentes, mientras éstas se encuentren vigentes;
- e) Estén orientados a garantizar la integridad y la disponibilidad de los equipos en todo momento; y
- f) Garanticen que se cumpla con lo requerido por las pólizas de seguro respectivas.

Todo evento de mantenimiento que se realice, debe quedar registrado en la bitácora correspondiente con indicación de qué y quién lo realizó. Se deben llevar bitácoras de fallas (supuestas y reales), así como de mantenimiento preventivo y correctivo.

La ejecución del mantenimiento será responsabilidad del esquema del esquema de soporte técnico instaurado, con base en los procedimientos que al efecto determine la Departamento de Informática.

13. Del registro de actividades de mantenimiento del personal operativo

Bitácoras de las actividades de mantenimiento del personal operativo

Debe exigírsele a todo el personal operativo que mantenga un registro de sus actividades de mantenimiento, debidamente documentado y actualizado, por medio de bitácoras. Estos registros deben incluir, según corresponda:

- a) Tiempos de inicio y cierre del sistema;
- b) Errores del sistema y medidas correctivas tomadas;
- c) Confirmación del manejo correcto de archivos y salidas; y
- d) Los datos de la persona que lleva a cabo la actualización del registro, incluyendo su nombre completo, número de cédula y firma, además de la fecha y hora en que la misma fue llevada a cabo.

Estos registros deben estar sujetos a revisiones periódicas, independientes de las revisiones de los propios procedimientos operacionales. Los registros serán revisados por las respectivas jefaturas.

14. Del registro de fallas

Registro de fallas

De todas las fallas de equipo, software y sistemas del Ministerio, deben llevarse registros actualizados que serán suficientemente documentados mediante bitácoras. Será responsabilidad de la Administración Superior, velar porque efectivamente se efectúen dichos registros y se tomen las medidas correctivas correspondientes.

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
-------------------------	------------------------------------	--	--

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	9 de 11

De la obligación de establecer parámetros claros y procedimientos para el registro de fallas

Corresponderá al Encargado de Seguridad definir los parámetros y procedimientos para la estandarización de los registros de fallas, y a la Comisión de Seguridad, aprobar dichos parámetros y procedimientos.

De la obligación de establecer parámetros claros y procedimientos para el manejo de fallas

Corresponderá al Encargado de Seguridad definir los parámetros y procedimientos generales para el manejo de fallas, teniendo como objetivo principal, el que las mismas sean resueltas satisfactoriamente utilizando medidas autorizadas, sin que en el proceso se violenten los controles de seguridad establecidos y aprobados por el Ministerio. Estos parámetros y procedimientos deben ser aprobados por la Comisión de Seguridad.

Responsabilidad de la Auditoría Interna en la revisión del manejo y corrección de fallas

Será responsabilidad de la Auditoría Interna del Ministerio, el revisar que en el manejo y corrección de fallas, no fueron comprometidos controles de seguridad aprobados por el Ministerio y que las medidas empleadas fueron debidamente autorizadas.

Tratamiento de la falla cuando ésta corresponda a un incidente de seguridad

Cuando se detecte que una falla corresponde a un incidente de seguridad, debe tratarse la misma como tal y ejercerse las acciones previstas para el manejo de este tipo de incidentes.

De la obligación de reportar fallas en los equipos, software y sistemas del Ministerio

Sin excepción todo usuario tendrá la obligación inexcusable de reportar, con la mayor prontitud, las fallas de/en los equipos, software y sistemas del Ministerio ante el esquema de soporte técnico instaurado, por los medios provistos por la Institución para tales efectos.

De la obligación de soporte técnico de llevar bitácoras de manejo y solución de fallas

El esquema de soporte técnico instaurado tendrá la obligación de llevar registros actualizados documentados mediante bitácoras, de todas las fallas que le son reportadas y de las medidas que se tomen para corregirlas. Estos registros serán debidamente documentados, según los parámetros y procedimientos aprobados por el Ministerio, para tales efectos.

15. Mesa de Servicios como apoyo al esquema de soporte técnico

Mesa de Servicios

El Ministerio de Cultura deberá implementar un sistema de Mesa de Servicios que le permita centralizar y agilizar los servicios de soporte técnico, (cuyo objeto son recursos esenciales de software y hardware), a fin de prestar un servicio más eficiente y apoyar a su vez, la gestión en seguridad de la información.

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
-------------------------	------------------------------------	--	--

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	10 de 11

Los servicios de la Mesa de Servicios podrán ser utilizados para:

- Llevar cuenta de las solicitudes de servicio y el estado de los procesos de soporte que aún no han sido solventados;
- Llevar cuenta de las áreas del Ministerio con mayores incidencia de problemas;
- Llevar a cabo inventarios de software y hardware; bitácoras de administración; retiro; adquisición; instalación; movimientos; adiciones; cambios; planeación y diseño; mantenimiento preventivo y correctivo; evaluación de productos; soporte a aplicaciones; integración de sistemas y actualizaciones de programas, entre otros.

Disposiciones finales

Reserva de derechos del Ministerio

El Ministerio se reserva el derecho de hacer cualquier tipo de modificación a estas políticas sin que ello implique responsabilidad de su parte, incluso sin previo aviso. Asimismo, la Institución se reserva el derecho de ampararse en una plataforma legal de apoyo a sus políticas, que habrán de suscribir los usuarios que pretendan tener acceso a los Recursos Informáticos.

Fiscalización de cumplimiento

El Ministerio se abroga el derecho de controlar estrictamente el debido cumplimiento de estas políticas, así como de tomar cualquier acción, de cualesquier naturaleza, sea ésta civil, penal, laboral y/o administrativa que le sea permitida por el ordenamiento jurídico, con el fin de castigar la violación a las mismas, para lo cual deberá respetar el debido proceso.

Usos ilícitos y/o no permitidos

El Ministerio facilita sus Recursos Informáticos únicamente para usos permitidos y legales. Por ende, quien haga uso de los mismos para fines ilegales y/o no permitidos, deberá asumir todas y cada una de las consecuencias que de su actuar u omisión deriven.

Políticas como una guía básica

Las Políticas incluidas en el presente documento pretenden ser una guía básica, no una lista exhaustiva. Por ende, de tener el usuario alguna duda que las Políticas no puedan aclarar, deberá consultarla, según corresponda, ya sea con el Jefe del área a que pertenece; con el supervisor del proyecto de que se trate; y/o con quien dirige el Departamento de Informática.

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
-------------------------	------------------------------------	--	--

	Política Gestión de Soporte Técnico	Código:	DI-PO-01
		Versión:	1
		Página:	11 de 11

Tolerancia

El que el Ministerio por cualesquier razón decida no tomar acciones en un determinado momento para exigir responsabilidades o sancionar algún comportamiento, no impide que pueda hacerlo en cualquier momento posterior. Deberá tenerse presente que el Ministerio estará siempre en potestad de actuar, según se lo permita el ordenamiento jurídico aplicable.

Política Integral de Seguridad de la Información

Las presentes políticas son complemento de las Políticas Integrales de Seguridad de la Información aprobadas por el Ministerio y por ende, la rigen los mismos principios rectores.

Así, los conceptos básicos que se infieren de las Políticas Integrales de Seguridad de la Información, se mantienen inalterados (e.g. seguridad de la información como factor prioritario; confidencialidad de la información del Ministerio y/o los Administrados; intereses del Ministerio y/o los Administrados por sobre intereses Personales; legalidad de toda actuación y respeto irrestricto a la legislación aplicable; respeto irrestricto a los Derechos de Autor y de Propiedad Intelectual; balance seguridad-productividad; prevalencia del interés público, entre otros).

De haber contraposición entre las Políticas Integrales de Seguridad de la Información y las presentes políticas, prevalecerán las que sean más específicas para el usuario con respecto al desempeño de sus responsabilidades para con la Institución.

Proceso: Operaciones	Fecha de aprobación: 20/01/2014	Fecha de última actualización: 20/01/2014	Aprobado por: Nombre: Catalina Cabezas Cargo: Jefe
-------------------------	------------------------------------	--	--