Resolución Ministerial No. 0107-2008-ED

Lima, 21 FEB. 2008

CONSIDERANDO:

Que, de conformidad con lo establecido en el artículo 20º del Reglamento de Organización y Funciones del Ministerio de Educación; la Oficina de Informática es responsable de establecer las políticas, normas y estándares, así como conducir el uso de recursos informáticos en el Sector Educación;

Que, de acuerdo a lo dispuesto en la citada norma, la Oficina de Informática, elaboró el documento denominado "Normas, Procedimientos y Estándares de Seguridad de la Información", a fin de que sea aprobado para su uso como instrumento de apoyo en el funcionamiento de dicha dependencia en observancia de las funciones que le corresponden;

De conformidad con lo dispuesto en el Decreto Ley Nº 25762, modificado por la Ley Nº 26510 y el Decreto Supremo Nº 006-2006-ED, modificado por el Decreto Supremo Nº 001-2008-ED, y la Ley Nº 29158;

SE RESUELVE:

Artículo Único.- Aprobar el documento denominado Normas, Procedimientos y Estándares de Seguridad de la Información del Ministerio de Educación, el mismo que forma parte de la presente Resolución.

Regístrese y comuníquese.

Ing. José Antonio Chang Escobedo
Ministro de Educación

0107 -2008-ED

Ministerio de Educación

Normas, Procedimientos y Estándares de Seguridad de la Información

Versión 1

(Versión 1.0)

Enero 2008

Ministerio de Educación

Contenido

Introducción

El presente documento contempla los documentos del Marco Normativo que respalda al sistema de gestión de seguridad realizada como parte del Servicio de Consultoría para la Implementación de las Normas y Gestión de la Seguridad de Información en el Centro de Datos del Ministerio de Educación, en adelante el Ministerio.

Objetivo

El desarrollo de la presente etapa tiene como objetivos:

- Definir y desarrollar el conjunto de Normas relacionadas con la gestión de la Seguridad de la Información.
- Definir y desarrollar el conjunto de Procedimientos relacionados con la Seguridad de la Información.
- Definir y desarrollar el conjunto de Estándares relacionados con la Seguridad de la Información y que den soporte a los procedimientos de seguridad.

El desarrollo de dichos documentos se basa en el uso de un enfoque sistemático para manejar la información sensible o confidencial de la institución de forma que se mantenga segura. Se entiende por información segura, aquella en que se preserven los atributos de confidencialidad, integridad y disponibilidad para los cuales fue generada.

Alcance

El alcance de las Políticas, Normas, Procedimientos y Estándares definidos y desarrollados para el Ministerio se circunscribe al Centro de Datos del Ministerio, acotado a los siguientes elementos que se encuentran en la actualidad en dicho Centro de Datos:

1. El hardware base
2. El software base
3. El software de aplicaciones
4. Las comunicaciones
5. Las funciones
6. Los procesos y controles
7. Los roles
8. Las responsabilidades

Roles de Seguridad de la Información

*** Oficial de Seguridad de la Información**

Es la persona designada para garantizar el desarrollo e implantación de la Seguridad de la Información en el Ministerio. En la redacción de las normas y procedimientos de este documento se le denomina como "Oficial de Seguridad".

*** Especialistas de Seguridad en las Unidades Orgánicas del Ministerio**

Deben canalizar y sensibilizar la prevención de riesgos tecnológicos en cada una de las áreas a las cuales pertenecen.

*** Responsable o Propietario de la Información**

Esta responsabilidad recae sobre el jefe o encargado de la unidad organizacional o apoyo correspondiente donde se crea o genera la información en cualquiera de sus formas.

*** Custodio de la información**

Es el usuario que tiene la responsabilidad de mantener y proteger la información a través de su procesamiento y la gestión de su almacenamiento, haciéndola accesible a los demás usuarios.

*** Usuario de la Información**

Es el conjunto de personas internas y/o externas que con la debida autorización del propietario de la información, puede consultar, ingresar, modificar o borrar la información almacenada en los sistemas informáticos u otros medios de almacenamiento

Normas de Seguridad de la Información

Se entiende como Norma, a la directiva sobre la cual se regula el total de acciones, responsabilidades y disposiciones de las entidades relacionadas en los temas de seguridad del Ministerio; se desarrolla y define para el Ministerio las Normas de Seguridad de la Información. Las mismas forman parte del presente entregable, con la siguiente codificación por documento:

Código de la Norma	Descripción
NO-001	**Norma de administración de cambios de sistemas de información**
NO-002	**Norma de administración de incidentes de seguridad**
NO-003	**Norma de clasificación y manejo de la información**
NO-004	**Norma de comprobación técnica**
NO-005	**Norma de conexión de redes externas**
NO-006	**Norma de control de acceso a las librerías de programas fuente**
NO-007	**Norma de control de acceso a los recursos de información**
NO-008	**Norma de control de acceso al centro de datos**
NO-009	**Norma de control del software en producción**
NO-010	**Norma de controles criptográficos**
NO-011	**Norma de controles de auditoría de sistemas**
NO-012	**Norma de creación de datos de prueba**
NO-013	**Norma de cumplimiento de la legislación**
NO-014	**Norma de desarrollo externo de software**
NO-015	**Norma de inclusión de requisitos de seguridad en contratos con terceros**
NO-016	**Norma de intercambio de información**
NO-017	**Norma de monitoreo continuo del desempeño de los sistemas**
NO-018	**Norma de registro de incidencias en las operaciones**
NO-019	**Norma de registro de operaciones**
NO-020	**Norma de respaldo de información**
NO-021	**Norma de seguridad de las aplicaciones del sistema**
NO-022	**Norma de seguridad de los equipos informáticos**
NO-023	**Norma de seguridad en comercio electrónico**
NO-024	**Norma de seguridad en el re-uso o eliminación de equipos y medios informáticos**
NO-025	**Norma de seguridad en la red**

Código de la Norma	Descripción
NO-026	**Norma de seguridad en los sistemas ofimáticos**
NO-027	**Norma de seguridad física y ambiental del centro de datos**
NO-028	**Norma de seguridad física**
NO-029	**Norma de servicios externos**
NO-030	**Norma de uso de correo electrónico**
NO-031	**Norma de uso de equipos móviles**
NO-032	**Norma de uso de protectores de pantalla y escritorios limpios**

Procedimientos de Seguridad de la Información

Entendiendo como Procedimientos, los documentos descriptivos que contienen en forma detallada la secuencia de acciones concatenadas entre sí y que orientadas en forma lógica permiten la ejecución de procesos para el cumplimiento de los temas de seguridad del Ministerio. Los mismos forman parte del presente entregable, con la siguiente codificación por documento:

Código del Procedimiento	Descripción
PR-01-01-01	**Evaluación del ambiente de TI**
PR-01-02-01	**Evaluación de proyectos de TI nuevos**
PR-01-03-01	**Administrar los cambios en la estrategia de TI**
PR-02-01-01	**Elaboración de políticas, normas y estándares**
PR-02-02-01	**Diseñar arquitectura de TI**
PR-02-02-02	**Evaluar arquitectura de TI**
PR-03-01-01	**Gestión del control de cambios en los sistemas de información**
PR-03-01-02	**Ejecución de la solución**
PR-03-01-03	**Validación de la solución**
PR-04-01-01	**Creación y/o modificación de accesos**
PR-04-01-02	**Eliminación de accesos**
PR-04-01-03	**Eliminación de información sensible**
PR-04-02-01	**Otorgamiento de acceso físico**
PR-04-02-02	**Control de acceso físico**
PR-04-02-03	**Autorización de un nuevo recurso de tratamiento de la información**
PR-04-03-01	**Identificación de Riesgos**
PR-04-03-02	**Evaluación de Riesgos**
PR-04-03-03	**Definición de Estrategia de Mitigación de Riesgos**
PR-04-03-04	**Monitoreo de Estrategia de Mitigación de Riesgos**
PR-04-03-05	**Clasificación de activos de la información**
PR-04-03-06	**Marcado de la información**
PR-04-04-01	**Respuesta ante incidencias de seguridad**
PR-04-04-02	**Administración de incidentes de seguridad**
PR-05-01-01	**Monitoreo de la Disponibilidad**
PR-05-01-02	**Monitoreo de la Capacidad**
PR-05-01-03	**Monitoreo de Logs de incidencias**
PR-05-02-01	**Elaboración del plan de contingencia**
PR-05-02-02	**Implementación del plan de contingencia**

Código del Procedimiento	Descripción
PR-05-02-03	**Prueba al plan de contingencia**
PR-05-03-01	**Definición de Plan de Respaldo**
PR-05-03-02	**Ejecución de Plan de Respaldo**
PR-05-03-03	**Ejecución de Plan de Restauración**
PR-05-03-04	**Custodia Externa de Respaldos**
PR-05-03-05	**Custodia Interna de Respaldos**
PR-05-03-06	**Prueba de respaldo de información**
PR-05-03-07	**Definición de Catálogo de Respaldo**
PR-05-04-01	**Administración de incidentes de operación**
PR-05-04-02	**Administración de incidentes de usuario**
PR-05-05-01	**Control de cambios sobre recursos de TI**
PR-05-05-02	**Mantenimiento preventivo/correctivo**
PR-05-05-03	**Recolección de evidencia**
PR-05-06-01	**Elaboración inventario de activos de TI**
PR-05-06-02	**Actualización inventario de activos de TI**
PR-06-01-01	**Brindar capacitación**
PR-06-02-01	**Elaboración de Encuestas Aleatorias**
PR-06-02-02	**Elaboración de Encuestas en Capacitaciones**
PR-06-03-01	**Administración de incidentes de usuario**
PR-06-04-01	**Seguimiento de Desempeño de Help Desk**
PR-07-01-01	**Elaborar Plan de Capacitación**
PR-07-01-02	**Capacitar al Personal**

Estándares de Seguridad de la Información

Se entiende como Estándares, los documentos descriptivos que contienen un modelo o referencia a seguir que están relacionados, o apoyan, a los procesos para el cumplimiento de los temas de seguridad del Ministerio. Los mismos forman parte del presente entregable, con la siguiente codificación por documento:

Código del Estándar	Descripción
DOC-001	**Acta de comité Ejecutivo de Seguridad de Información (CESI)**
DOC-002	**Acta de comité Operativo de Seguridad (COSI)**
DOC-003	**Matriz de dueños de la información**
DOC-004	**Bitácora de acceso físico al Centro de Datos**
DOC-005	**Inventario de activos de información**
DOC-006	**Bitácora de incidencias de seguridad**
DOC-007	**Bitácora de Operaciones**
DOC-008	**Bitácora de acceso usuarios**
DOC-009	**Bitácora de cuentas genéricas**
DOC-010	**Control de activos de tratamiento de información**
DOC-011	**Registro de control de requerimientos**
DOC-012	**Requerimiento de acceso de usuario**
DOC-013	**Bitácora de Respaldo y Restauración de Información**
DOC-014	**Arquitectura técnica de seguridad**
DOC-015	**Bitácora de incidencias de Operaciones**

Aprobación y Mantenimiento de las Políticas, Normas, Procedimientos y Estándares

Para asegurar que las políticas, normas, procedimientos y estándares se encuentren acorde a la realidad del Centro de Datos del Ministerio, es necesario que se lleve a cabo un proceso periódico de mantenimiento, en la cual se deben identificar los posibles cambios que se deben realizar a lo largo del tiempo, luego se deben implementar los cambios para finalmente pasen por el proceso de aprobación definido.

A continuación se detalla el estándar de documentación definido y los procedimientos de aprobación y mantenimiento de las políticas, normas, procedimientos y estándares.

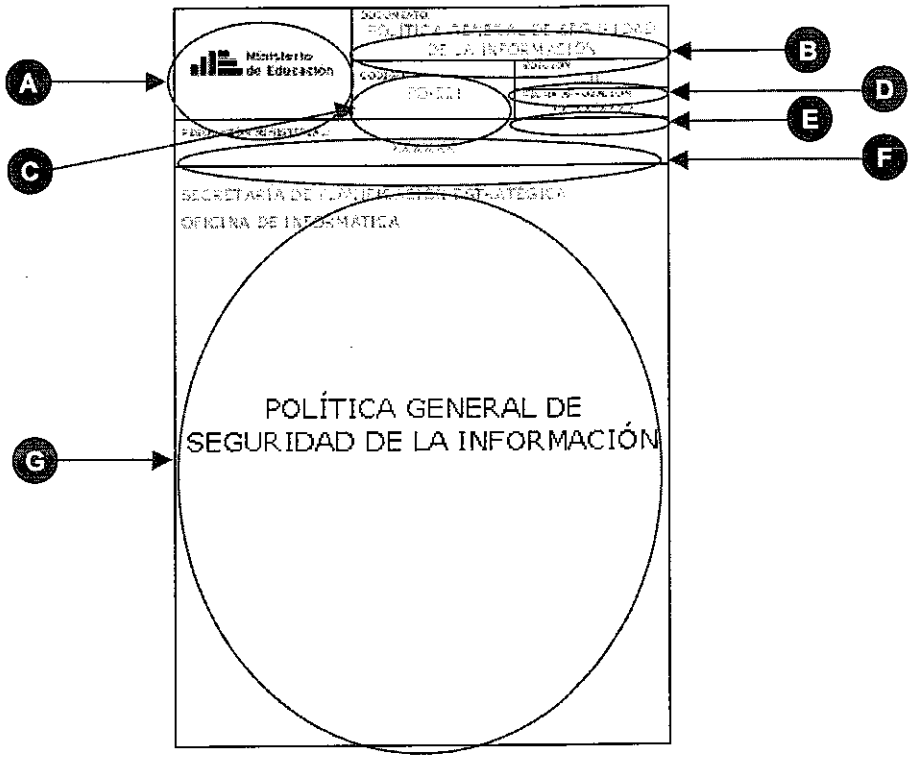
Estándares de documentación

Se entiende como Estándares, los documentos descriptivos que contienen un modelo o referencia a seguir que están relacionados, o apoyan, a los procesos para el cumplimiento de los temas de seguridad del Ministerio.

Los estándares de documentación se muestran a continuación:

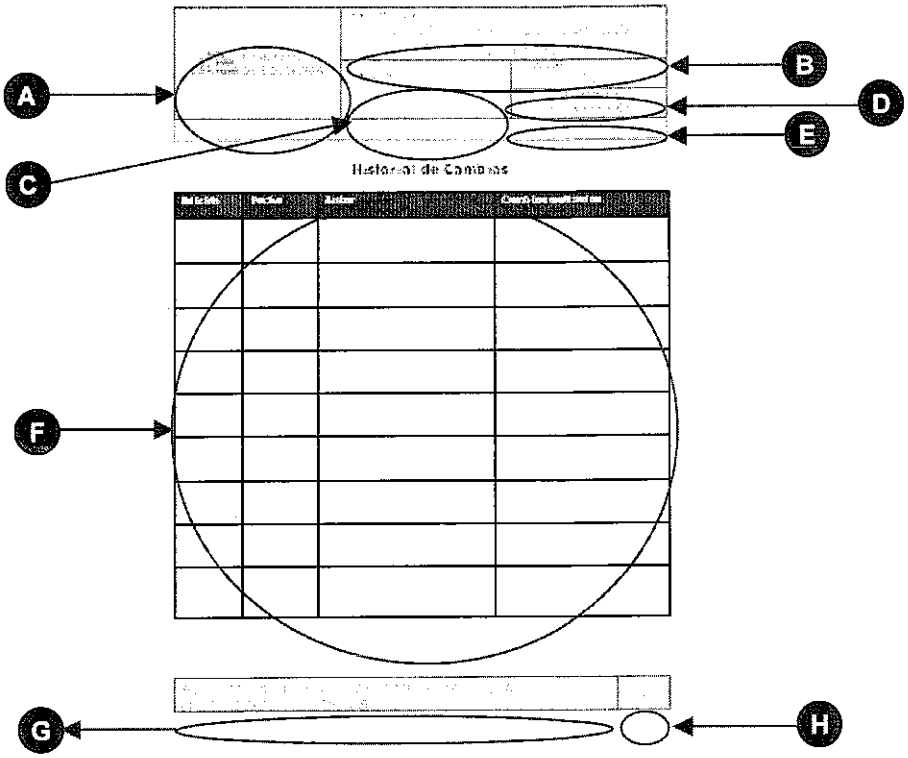
Estándares de documentación de Políticas y Normas

A continuación se muestran los estándares de documentación de Políticas y Normas:



La descripción de cada uno de los campos se muestra a continuación:

Sección	Descripción
A	**Imagen (Logotipo) del Ministerio de Educación**
B	**Nombre del documento**
C	**Código del documento**
D	**Edición del documento**
E	**Fecha de aprobación**
F	**Resolución ministerial que aprueba el presente documento**
G	**Carátula general del Documento**

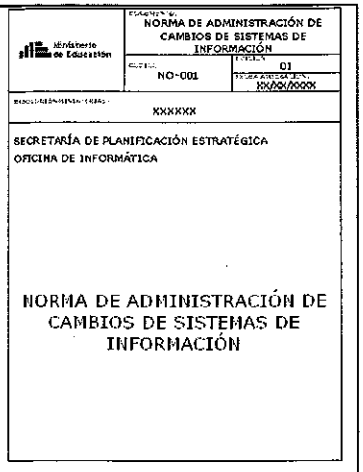
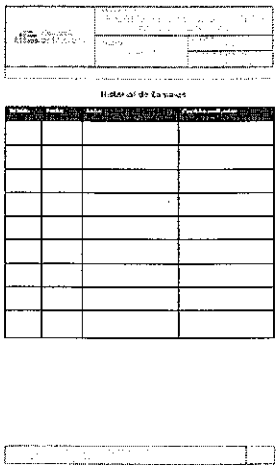
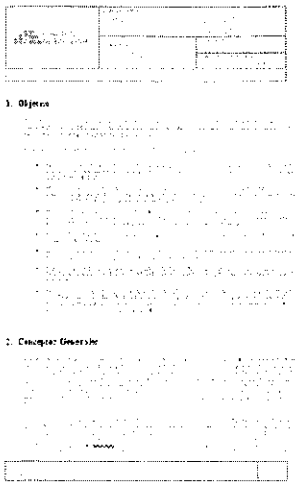


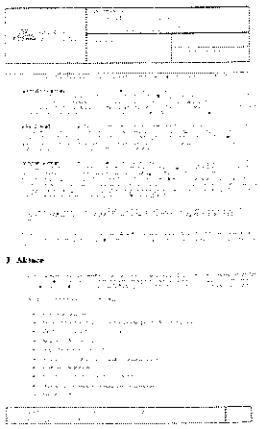
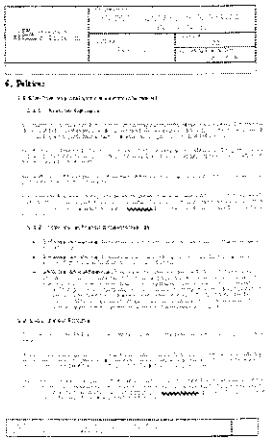
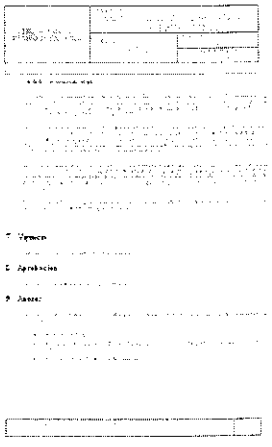
La descripción de cada uno de los campos se muestra a continuación:

Sección	Descripción
A	**Imagen (Logotipo) del Ministerio de Educación**
B	**Nombre del documento**
C	**Código del documento**
D	**Edición del documento**
E	**Fecha de aprobación**
F	**Historial de Cambios de cada una de las versiones del documento**
G	**Oficina responsable del documento**
H	**Número de página del documento**

El cuerpo de cada política y/o norma está compuesto por las siguientes secciones:

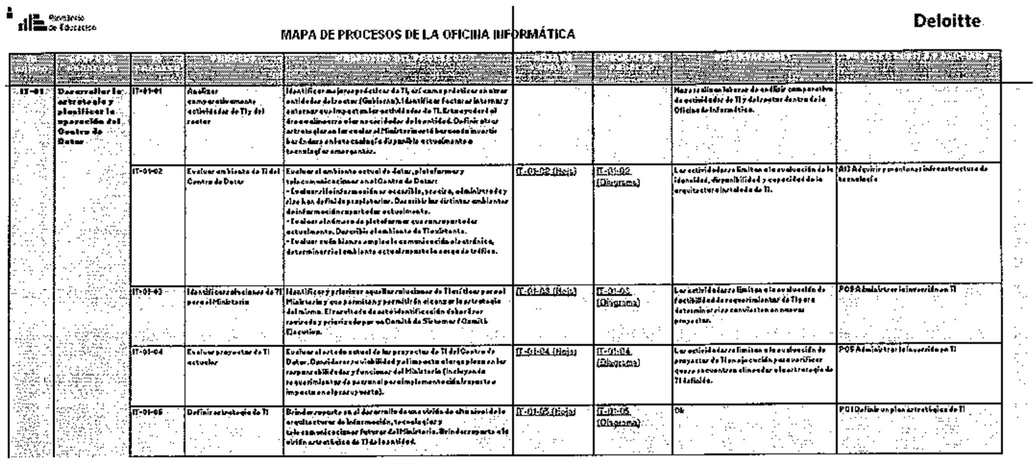
Sección	Imagen

Carátula	Presentación y Descripción general del documento.	 NORMA DE ADMINISTRACIÓN DE CAMBIOS DE SISTEMAS DE INFORMACIÓN NO-001 01 XX/XX/XXXX XXXXXX SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA OFICINA DE INFORMÁTICA NORMA DE ADMINISTRACIÓN DE CAMBIOS DE SISTEMAS DE INFORMACIÓN
Historial de Cambios	Tabla en la cual se registran todos los cambios que se hayan realizado al documento desde su concepción.	
Objetivo	Descripción del objetivo principal del documento.	
Conceptos Generales	Descripción de los principales conceptos a utilizar como parte del documento.	

Alcance	Descripción del alcance del documento.	
Secciones inherentes al documento	En estas secciones se detalla toda la información propia de la política o norma.	
Vigencia	Describe la vigencia del documento.	
Aprobación	Describe la forma por la cual se aprobó el documento.	
Anexos	**Los anexos del documento**	

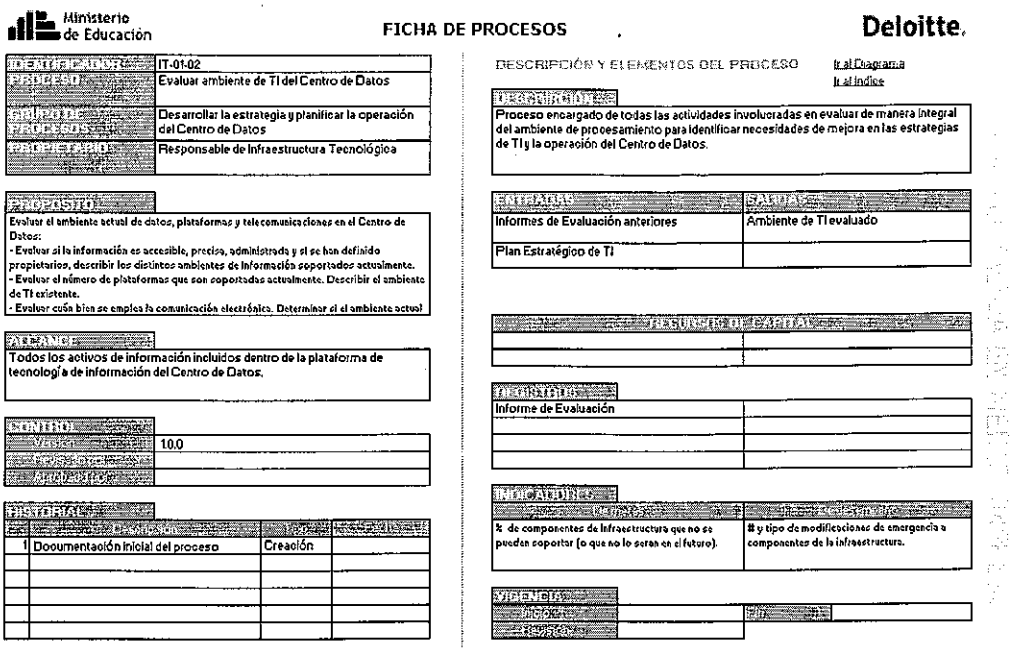
Estándares de documentación de Procedimientos

A continuación se muestran los estándares de documentación de Procedimientos:



La descripción de cada uno de los campos se muestra a continuación:

Sección	Descripción
ID GRUPO	**Código del grupo de procesos**
GRUPO DE PROCESOS	**Nombre del Grupo de Procesos en el que está incluido el proceso.**
ID PROCESO	**Código del proceso.**
PROCESO	**Nombre del proceso.**
PROPÓSITO DEL PROCESO	**Descripción del proceso.**
HOJA DE PROCES	**Relación con la hoja en la cual se describe los datos generales el proceso.**
DIAGRAMA DE PROCESO	**Relación con la hoja en la cual se desarrollan las actividades del proceso.**
OBSERVACIONES	**Información que ayuda al entendimiento del proceso.**
PROCESO COBIT 4.0 ASOCIADO	**Referencia al proceso del estándar internacional COBIT asociado.**



Ministerio de Educación

FICHA DE PROCESOS

Deloitte.

IDENTIFICADOR	IT-01-02
PROCESO	Evaluar ambiente de TI del Centro de Datos
GRUPO DE PROCESOS	Desarrollar la estrategia y planificar la operación del Centro de Datos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPÓSITO

Evaluar el ambiente actual de datos, plataformas y telecomunicaciones en el Centro de Datos:
- Evaluar si la información es accesible, precisa, administrada y si se han definido propietarios, describir los distintos ambientes de información soportados actualmente.
- Evaluar el número de plataformas que son soportadas actualmente. Describir el ambiente de TI existente.
- Evaluar cuán bien se emplea la comunicación electrónica. Determinar si el ambiente actual

ALCANCE

Todos los activos de información incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	10.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción		
1	Documentación inicial del proceso	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCESO

Ir al Diagrama
Ir al Índice

DESCRIPCIÓN

Proceso encargado de todas las actividades involucradas en evaluar de manera integral del ambiente de procesamiento para identificar necesidades de mejora en las estrategias de TI y la operación del Centro de Datos.

ENTRADAS	SALIDAS
Informes de Evaluación anteriores	Ambiente de TI evaluado
Plan Estratégico de TI	

RESPONSABILIDADES

REGISTROS

Informe de Evaluación

INDICADORES

% de componentes de infraestructura que no se pueden soportar (o que no lo serán en el futuro).	# y tipo de modificaciones de emergencia a componentes de la infraestructura.

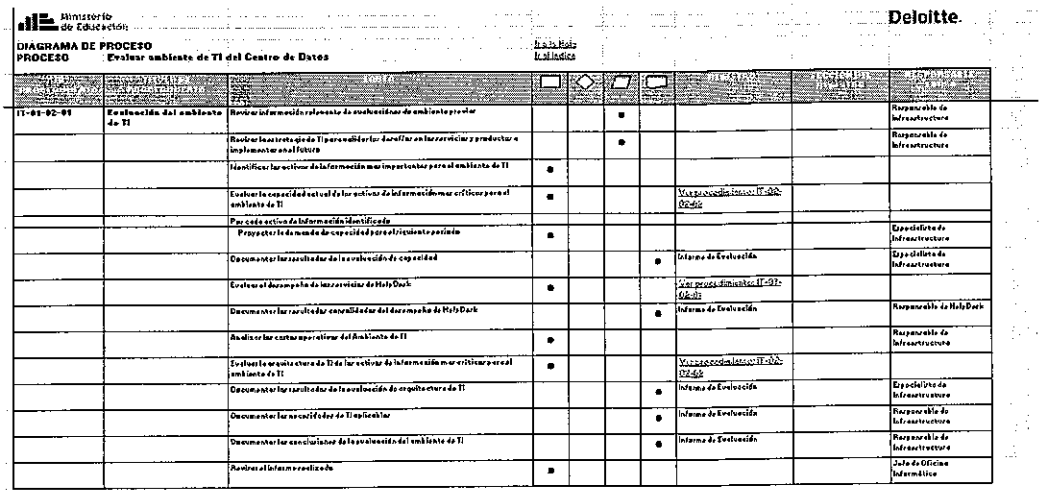
VIGENCIA

Inicio		Fin	
Frecuencia			

La descripción de cada uno de los campos se muestra a continuación:

Sección	Descripción
IDENTIFICADOR	**Código que identifica al proceso. Esta compuesto por el código identificador del Grupo de Proceso (Por ejemplo: IT-02) seguido de un numero correlativo.**
PROCESO	**Nombre del proceso.**
GRUPO DE PROCESOS	**Nombre del Grupo de Procesos en el que está incluido el proceso.**
PROPIETARIO	**Persona encargada de velar que se cumplan las actividades definidas en el proceso y que la documentación del mismo se encuentre actualizada.**
ALCANCE	**Actividades y/o recursos alcanzados por las actividades definidas en el proceso.**
CONTROL	**Sección que indica información asociada a la elaboración de la última versión de la documentación del proceso.**
Versión	**Identificador del número de versión correspondiente a la documentación actual del proceso.**
Revisado por	**Nombre de la persona que revisó, antes de su aprobación, la versión actual de la documentación del proceso.**
Aprobado por	**Nombre de la persona aprobó, antes de su difusión, la versión actual de la documentación del proceso.**
HISTORIAL	**Sección en la que se documenta el historial de cambios que ha sufrido la documentación del proceso desde su creación. Cada cambio se documenta como un renglón dentro de la tabla contenida en esta sección.**
Descripción	**Descripción del cambio realizado sobre la documentación del proceso**

	proceso.
Tipo	**Tipo de cambio realizado sobre la documentación del proceso (Elaboración, Revisión, Aprobación).**
Fecha	**Fecha en la que se realizó el cambio descrito sobre la documentación del proceso.**
DESCRIPCIÓN	**Descripción global de las actividades involucradas en el proceso.**
ENTRADAS	**Sección en la que se indican, de manera referencial, los recursos y/o actividades (pre-condiciones) requeridas por el proceso. Cada entrada se documenta como un renglón dentro de la tabla contenida en esta sección.**
SALIDAS	**Sección en la que se indican, de manera referencial, los recursos y/o actividades (post-condiciones) que se obtienen como resultado del proceso. Cada salida se documenta como un renglón dentro de la tabla contenida en esta sección.**
RECURSOS DE CAPITAL	**Sección en la que se indican los recursos adicionales al personal, los registros, las entradas y las salidas; pero que son requeridos para la ejecución de las actividades del proceso. Cada recurso de capital se documenta como un renglón dentro de la tabla contenida en esta sección.**
REGISTROS	**Sección en la que se documenta la información, sea física (documentos, informes, etc.) o electrónica (correos, sistemas, etc.), que constituye evidencia de registro de alguna de las actividades incluidas dentro del proceso, y que puede ser revisada para efectos de verificación del cumplimiento de las mismas.**



Ministerio de Educación

Deloitte.

DIAGRAMA DE PROCESO
PROCESO : Evaluar ambiente de TI del Centro de Datos

Hoja de Hoja
Actividades

IT-01-02-01	Evaluación del ambiente de TI	Revisar información relevante de evaluaciones de ambiente previas			•				Responsable de Infraestructura
		Revisar las estrategias de TI para establecer lineamientos para los servicios y productos a implementar a futuro			•				Responsable de Infraestructura
		Identificar los activos de información mas importantes para el ambiente de TI	•						
		Evaluar la capacidad actual de los activos de información mas críticos para el ambiente de TI	•				Ver proceso relacionado: IT-02-02-02		
		Procesar la información identificada							
		Proyectar la demanda de capacidad para el siguiente periodo	•						Especialistas de Infraestructura
		Documentar los resultados de la evaluación de capacidad				•	Informe de Evaluación		Especialistas de Infraestructura
		Evaluar el desempeño de los servicios de HelpDesk	•				Ver proceso relacionado: IT-07-02-03		
		Documentar los resultados de la evaluación del desempeño de HelpDesk				•	Informe de Evaluación		Responsable de HelpDesk
		Analizar los costos operativos del Ambiente de TI	•						Responsable de Infraestructura
		Evaluar la arquitectura de TI de los activos de información mas críticos para el ambiente de TI	•				Ver proceso relacionado: IT-02-02-02		
		Documentar los resultados de la evaluación de arquitectura de TI				•	Informe de Evaluación		Especialistas de Infraestructura
		Documentar las necesidades de TI aplicables				•	Informe de Evaluación		Responsable de Infraestructura
		Documentar las conclusiones de la evaluación del ambiente de TI				•	Informe de Evaluación		Responsable de Infraestructura
		Revisar el informe realizado	•						Jefe de Oficina Informática

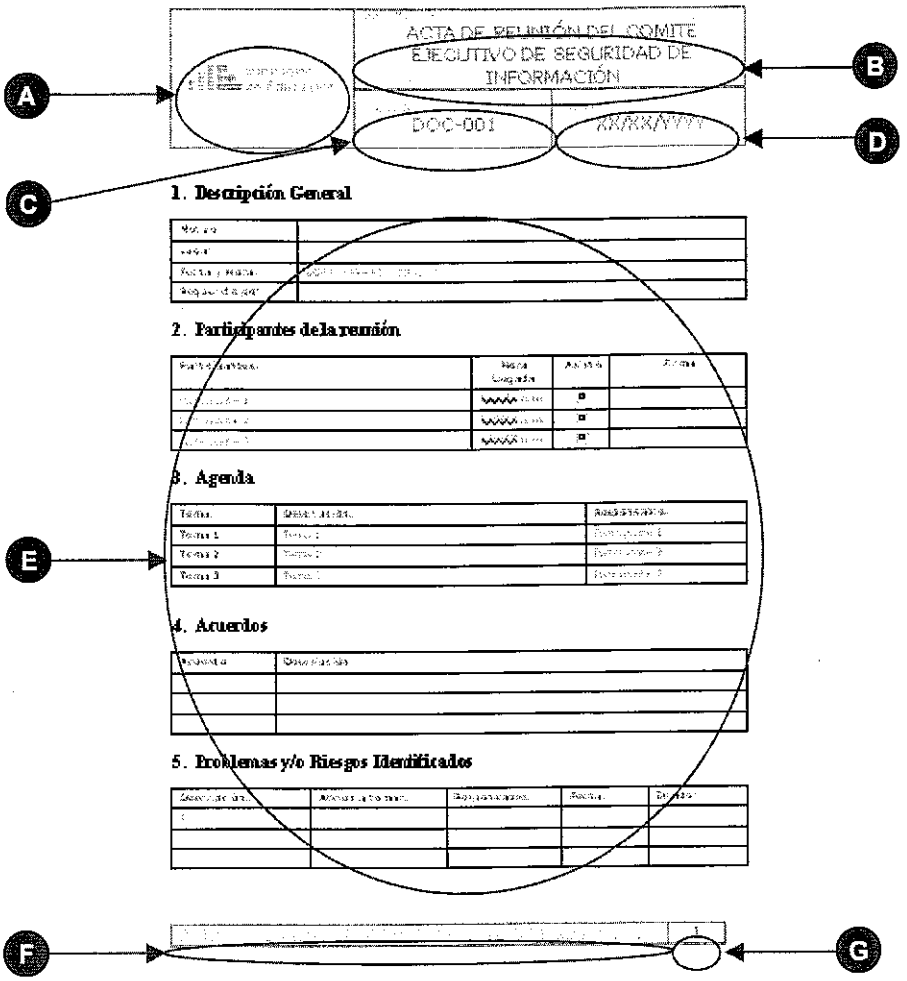
La descripción de cada uno de los campos se muestra a continuación:

Sección	Descripción
ID PROCEDIMIENTO	**Código que identifica un procedimiento (un proceso puede estar compuesto por uno o varios procedimientos). Esta compuesto por el código identificador del proceso (Por ejemplo: IT-02-01) seguido de un numero correlativo.**
TITULO DE PROCEDIMIENTO	**Nombre del procedimiento.**

TAREA	**Descripción de la actividad a realizar. Cada actividad se documenta como un renglón dentro de la tabla contenida en esta sección.**
TIPO DE TAREA	**Sección que indica información del tipo de la actividad.**
	**Actividad de procesamiento del algún tipo.**
	**Actividad de toma de decisión**
	**Actividad de análisis de entrada y/o emisión de salidas**
	**Actividad de documentación.**
REGISTRO	**Nombre del registro generado por la actividad.**
SECCIÓN DEL REGISTRO	**Sección del registro en el que se registra algun control definido por la actividad.**
RESPONSABLE TAREA	**Persona encargada de ejecutar la actividad.**

Estándares de documentación de Estándares

A continuación se muestran los estándares de documentación de Estándares:



1. Descripción General

2. Participantes de la reunión

3. Agenda

4. Acuerdos

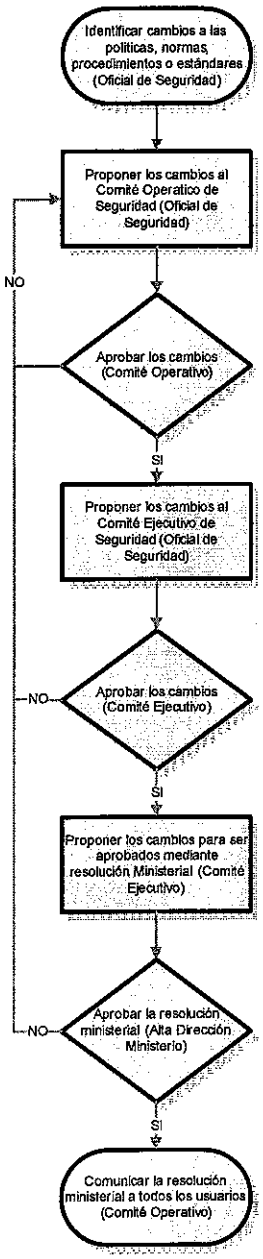
5. Problemas y/o Riesgos Identificados

La descripción de cada uno de los campos se muestra a continuación:

Sección	Descripción
A	**Imagen (Logotipo) del Ministerio de Educación**
B	**Nombre del documento**
C	**Código del documento**
D	**Fecha de emisión del documento**
E	**Cuerpo del documento**
F	**Oficina responsable del documento**
G	**Número de página del documento**

Proceso de Aprobación y Mantenimiento de Políticas, Normas, Procedimientos y Estándares

A continuación se muestra el procedimiento definido para realizar el mantenimiento y aprobación de las Políticas, Normas, Procedimientos y Estándares.


Identificar cambios a las políticas, normas, procedimientos o estándares (Oficial de Seguridad)
Proponer los cambios al Comité Operatico de Seguridad (Oficial de Seguridad)
NO
Aprobar los cambios (Comité Operativo)
SI
Proponer los cambios al Comité Ejecutivo de Seguridad (Oficial de Seguridad)
NO
Aprobar los cambios (Comité Ejecutivo)
SI
Proponer los cambios para ser aprobados mediante resolución Ministerial (Comité Ejecutivo)
NO
Aprobar la resolución ministerial (Alta Dirección Ministerio)
SI
Comunicar la resolución ministerial a todos los usuarios (Comité Operativo)

0107-2008-ED

Ministerio de Educación	**DOCUMENTO:** NORMA DE ADMINISTRACIÓN DE CAMBIOS DE SISTEMAS DE INFORMACIÓN	
	CÓDIGO: NO-001	**EDICIÓN:** 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE ADMINISTRACIÓN DE CAMBIOS DE SISTEMAS DE INFORMACIÓN

Ministerio de Educación	DOCUMENTO: NORMA DE ADMINISTRACIÓN DE CAMBIOS DE SISTEMAS DE INFORMACIÓN	
	CÓDIGO: NO-001	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE ADMINISTRACIÓN DE CAMBIOS DE SISTEMAS DE INFORMACIÓN	
	CÓDIGO: NO-001	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de posibles omisiones en el proceso de aceptación de los usuarios tras modificaciones o creación de nuevos sistemas de información del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

2.1 El Oficial de Seguridad es responsable de:

- Verificar que todos los desarrollos nuevos o modificaciones a los sistemas de información del Ministerio cumplan con lo establecido en el PR-03-01-01 - Procedimiento de Gestión del control de cambios en los sistemas de información.

3. Descripción

3.1. La administración de los cambios de los sistemas de información exige que todo cambio sea documentado como un medio de control para las actividades de desarrollo o implementación de los sistemas de información.

3.2. Todo cambio se inicia cuando es necesaria la creación de una nueva funcionalidad o la modificación en alguna funcionalidad existente dentro de los sistemas de información del ambiente de producción del Ministerio.

3.3. Las especificaciones de cambio en los sistemas de información, deben contemplar los cambios que se deben realizar a los controles de seguridad del sistema. Se debe informar del riesgo asociado a la no implantación del cambio especificado.

3.4. Se deben incluir un plan de pruebas previo al cambio, las cuales incluyen pruebas de capacidad, pruebas paralelas y pruebas de usuario. Estas pruebas deberán ser documentadas, incluyendo los atributos de la misma y resultados obtenidos.

3.5. Todo sistema de información debe contemplar mecanismos de validación y verificación de la información que se ingresa.

3.6. Se debe seguir un adecuado control de cambios de acuerdo a lo establecido en el PR-03-01-01 - Procedimiento de Gestión del control de cambios en los sistemas de información.

3.7. Se deben de realizar verificaciones y cambios en el sistema operativo de los terminales de los usuarios cuando sea requerido.

3.8. Todo cambio debe de ser aprobado por el Jefe de Desarrollo antes de proceder a ser ejecutado por el personal de producción del Ministerio.

3.9. Todo cambio o implantación realizado a los sistemas de información debe contar con el visto bueno del usuario solicitante para poder ser considerado como terminado. Así mismo, se deberá documentar el detalle del cambio realizado, incluyendo sus atributos y resultados obtenidos.

3.10. Los manuales de usuario, instructivos y/o otros documentos complementarios serán entregados al término de la implementación del sistema informático en su versión final.

DE LA AUDITORÍA Y REVISIÓN DE LA ADMINISTRACIÓN DE LOS CAMBIOS

3.11. El Oficial de Seguridad deberá verificar que todo el proceso de administración de cambios se realice de acuerdo a la presente norma y a los procedimientos asociados definidos en la misma.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD	
	CÓDIGO: NO-002	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD

Ministerio de Educación	DOCUMENTO: NORMA DE ADMINISTRACIÓN DE LOS INCIDENTES DE SEGURIDAD	
	CÓDIGO: NO-002	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE ADMINISTRACIÓN DE LOS INCIDENTES DE SEGURIDAD	
	CÓDIGO: NO-002	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Administrar y dar solución de manera efectiva a los incidentes de seguridad asociados a temas de tecnología de información informados por personal del Ministerio de Educación (en adelante el Ministerio).

2. definición de Términos

2.1. **Incidente de Seguridad**: Es un evento que puede comprometer de alguna manera la confidencialidad, integridad y disponibilidad de la información. Algunos de los incidentes de seguridad son los siguientes:

- Falla y pérdida de los servicios de los sistemas de información
- Código malicioso
- Negación de servicio
- Errores resultantes de datos incompletos o no actualizados
- Faltas a la integridad de la información

3. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

3.1. El Oficial de Seguridad es responsable de:

- Solicitar los informes de desempeño de las actividades de Help Desk para su revisión y contrastarlos con la bitácora de Help Desk disponible.
- Revisar los informes de cada una de las incidencias presentadas.

3.2. El Custodio de Información es responsable de:

- Preparar un informe por cada incidente de seguridad que se presente en la plataforma de tecnología del Ministerio.
- Preparar un informe consolidado que contenga el total de incidentes de seguridad identificados, obteniendo información del porcentaje de incidentes solucionados, la duración promedio de los incidentes, causas más recurrentes, etc.

3.3. El Encargado de Soporte Técnico (Help Desk) es responsable de:

- Registrar las solicitudes y los incidentes de seguridad que se presenten en la bitácora de Help Desk.
- Preparar un informe sobre el desempeño de las labores de Help Desk del Ministerio.

3.4. El Usuario de Información es responsable de:

- Advertir, registrar y comunicar al Oficial de Seguridad de cualquier incidente informático así como las debilidades o amenazas observadas en materia de seguridad con relación a los sistemas de información.
- Advertir, registrar y comunicar al Oficial de Seguridad de cualquier acto doloso cometido por algún empleado del Ministerio.

4. Descripción

4.1. Se debe informar a todos los empleados acerca de los procedimientos de comunicación de los diferentes tipos de incidentes (violaciones, amenazas, debilidades o anomalías en materia de seguridad) que podrían producir un impacto en la seguridad de los activos de la organización.

4.2. Todos los fallos de software que se presenten en la plataforma tecnológica del Ministerio debe quedar registrado e informado al Oficial de Seguridad de manera oportuna. Los usuarios no deberían intentar retirar el software salvo expresa autorización del Área de Sistemas de Información.

4.3. Para atender debidamente los incidentes de seguridad será necesario que el Oficial de Seguridad recolecte evidencia tan pronto como sea posible una vez ocurrido el hecho.

4.4. En caso las labores de Help Desk sean realizadas por contratistas externos se deberá asegurar que existan acuerdos de niveles de servicio que garanticen un desempeño eficaz y eficiente de su parte.

4.5. El uso de alarmas anti-coacción deberá aplicarse tras una evaluación de riesgos, en cuyo caso se proceda a la implementación de la misma, debe quedar un procedimiento definiendo responsabilidades.

DEL USO DE LA BITÁCORA DE HELP DESK

4.6. Las solicitudes y/o reportes de incidentes podrán ser cursadas por personal del Ministerio vía telefónica o por correo electrónico al Encargado de Soporte Técnico (Help Desk).

4.7. Todas las comunicaciones cursadas al Encargado de Soporte Técnico (Help Desk) deberán ser documentadas para asegurar el adecuado seguimiento de las mismas hasta su resolución. Esta documentación también permitirá la eventual identificación de problemas recurrentes que pudieran estarse presentando.

4.8. La bitácora de Help Desk deberá contener información suficiente para asegurar el adecuado seguimiento de cada registro (informante, fecha de registro, problema informado, causa del problema, solución identificada, fecha solución y estado solicitud, como mínimo). Esta información permitirá realizar un monitoreo de las incidencias que se repitan, permitiendo obtener información estadística.

DEL TRATAMIENTO DE LOS INCIDENTES DE SEGURIDAD

4.9. Se debe establecer un procedimiento formal de comunicación, junto con un procedimiento de respuesta, que establezca la acción que ha de emprenderse al recibir un informe sobre incidentes. Todos los empleados y contratistas deben estar enterados del procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto como sea posible. En este procedimiento se debe tomar en cuenta:

- Advertir y registrar los síntomas del problema y los mensajes que aparecen en la pantalla.
- La computadora debe ser aislada si es posible, deteniéndose el uso de la misma.
- Alertar de inmediato al Oficial de Seguridad.

- Si se ha de examinar el equipo, éste debe ser desconectado de las redes del Ministerio antes de ser activado nuevamente.

4.10. Personal interno y/o contratistas externos deberán advertir, registrar y comunicar las debilidades y/o amenazas de seguridad, con relación a los sistemas o servicios de la compañía.

4.11. Para los casos en los que se haya detectado una debilidad se debe informar al personal que ellos no deben, bajo ninguna circunstancia intentar probar una supuesta debilidad, dado que dicha acción puede infringir en la propia seguridad de los equipos e información, además de ser interpretado como un mal accionar en posteriores investigaciones del incidente.

4.12. Para el tratamiento de los incidentes de seguridad, además del registro en la Bitácora de Help Desk, el Encargado de Soporte Técnico (Help Desk) deberá informar cada incidente de seguridad ocurrido al Oficial de Seguridad, siendo las de mayor gravedad informadas también al Jefe de la Oficina de Informática.

4.13. El personal técnico tiene la obligación de registrar estados y actividades que se ejecutan en la resolución de problemas reportados por usuarios, así como también las acciones que arribaron la solución del caso.

4.14. El Oficial de Seguridad deberá coordinar la recolección de evidencia tan pronto como sea posible una vez ocurrido el hecho.

4.15. Según su gravedad, los incidentes relativos a seguridad deben comunicarse a las oficinas cuya información haya sido comprometida.

4.16. Se debe incurrir en la documentación específica de informes de cada incidente por parte del Custodio de Información, con el fin de identificar específicamente las causas e identificar la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros, o de tomarlos en cuenta en el proceso de revisión de la política de seguridad.

4.17. El informe de cada incidente deberá ser presentado al Oficial de Seguridad para su revisión. El Oficial de Seguridad deberá coordinar con el Custodio de Información la implantación de medidas correctivas que mitiguen el riesgo de que el incidente vuelva a repetirse.

DEL PROCESO DISCIPLINARIO

4.18. Se deben de tener definidos procesos disciplinarios que sirvan de factor disuasivo para que personal interno y/o externo al Ministerio no pase por alto los procedimientos de seguridad definidos.

4.19. Si el personal viola las políticas y procedimientos de seguridad del Ministerio, esto será considerado como un acto disciplinario; y por lo tanto deberán ser impuestas las medidas disciplinarias previstas para estos casos.

4.20. Los contratos firmados con contratistas deberán indicar las consecuencias en el caso de que violen las políticas y procedimientos de seguridad del Ministerio.

4.21. El proceso disciplinario debe garantizar un trato imparcial y correcto hacia los empleados y/o contratistas sospechosos de haber cometido violaciones graves o persistentes a la seguridad.

DE LA REVISIÓN Y AUDITORÍA DE LA ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD

4.22. El Oficial de Seguridad debe revisar periódicamente los informes de desempeño elaborados por el Encargado de Soporte Técnico (Help Desk) para verificar que las labores de seguimiento de las solicitudes se estén realizando oportunamente.

4.23. El Oficial de Seguridad debe revisar los informes de cada incidente de seguridad que se haya presentado para verificar que labores de seguimiento y medidas correctivas hayan sido implantadas.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	
	CÓDIGO: NO-003	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

Ministerio de Educación	DOCUMENTO: NORMA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	
	CÓDIGO: NO-003	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	
	CÓDIGO: NO-003	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Normar la clasificación de la información del Ministerio de Educación, en adelante el Ministerio, en base a los criterios de confidencialidad, integridad y disponibilidad de la información, estableciendo los métodos de clasificación así como el cumplimiento de dicho proceso.

2. Definición de Términos

Se deberá tener un claro entendimiento de los siguientes conceptos:

2.1. **Confidencialidad:** La información sólo debe ser conocida por el personal que la requiera para el desarrollo de sus funciones.

Este principio fundamental de seguridad busca garantizar que toda la información de los accionistas, empleados y proveedores, y sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

2.2. **Integridad:** La información no puede ser alterada ni eliminada por cambios no autorizados o accidentales.

Este principio fundamental de seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de acuerdo con los valores y expectativas del negocio, así como evitar fraudes y/o irregularidades de cualquier índole que haga que la información no corresponda a la realidad.

2.3. **Disponibilidad:** La información debe estar disponible para el personal, usuarios y entidades reguladoras de manera oportuna y acorde a sus niveles de autorización.

Este principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando esta es requerida por el proceso del negocio. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento y/o equipamiento de procesamiento.

2.4. **Información pública:** Toda aquella información cuya divulgación fuera del Ministerio no representa riesgo alguno para la empresa.

2.5. **Información de uso interno:** Toda aquella información de uso interno del Ministerio y cuyo acceso puede ser permitido a cualquier empleado de la empresa, sin embargo, que no puede ser transmitida fuera del Ministerio sin autorización escrita del propietario de la información.

2.6. **Información confidencial:** Toda aquella información restringida que debe ser accedida por personas expresamente autorizadas, en base al concepto de "necesidad-de-conocer" (need-to-know). Su divulgación requiere el consentimiento formal del responsable de la misma.

Ministerio de Educación	DOCUMENTO: NORMA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	
	CÓDIGO: NO-003	EDICIÓN: 01
		FECHA APROBACIÓN:

3. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

3.1. El Oficial de Seguridad es responsable de:

- Apoyar a los propietarios de la información en la identificación de controles que brinden una seguridad adecuada a la información de acuerdo a su clasificación.
- Coordinar con el custodio de información la implementación de los controles definidos.
- El Propietario de Información es responsable de:
- Estimar el valor y clasificar la información del Ministerio bajo su responsabilidad.
- Decidir el nivel de control necesario para la información bajo su responsabilidad.
- Autorizar el acceso a la información bajo su responsabilidad (tanto a personal interno como externo al Ministerio).

3.2. El Custodio de Información es responsable de:

- Garantizar el establecimiento y aplicación de los controles establecidos por el propietario de la información.
- Asegurar protección física a la gestión y almacenamiento de la información.

4. Descripción

4.1. Los responsables de clasificar la información del Ministerio son los propietarios de la misma, en general esta responsabilidad recaerá sobre el jefe o encargado de la unidad de negocio o apoyo correspondiente, responsable de la protección y uso de la información.

4.2. Se considera información confidencial toda información clasificada de uso interno y restringido.

4.3. La información confidencial deberá ser marcada en caso sea tratada en los siguiente tipos de tratamiento:

- Copia.
- Almacenamiento.
- Transmisión por correo físico, fax y correo electrónico.
- Transmisión oral, incluida telefonía móvil, transmisión de voz y máquinas de respuesta automática.
- Destrucción.

4.4. Los criterios que deberán tener en cuenta los propietarios de información para clasificar la misma son:

- Utilidad de la información.
- Valor de la información.
- Antigüedad de la información.
- Nivel de daño que sufriría la organización si se compromete la confidencialidad de la información.
- Nivel de daño que sufriría la organización si se compromete la integridad de la información.
- Nivel de daño que sufriría la organización si se compromete la disponibilidad de la información.
- Quién accede a la información
- Quién mantiene la información
- Dónde es almacenada la información

4.5. La información deberá ser clasificada dentro de los tres siguientes tipos:

- Información pública.
- Información de uso interno.
- Información confidencial.

4.6. Todo medio de almacenamiento que contenga información clasificada o confidencial, deberá ser rotulado para su plena identificación como confidencial.

4.7. Se debe contar con una matriz de clasificación centralizada en donde se tenga un inventario de la información utilizada por el Ministerio. Dicha matriz debe identificar la clasificación de la información y al propietario de la misma (Anexo A).

4.8. El propietario de información conjuntamente con el Oficial de Seguridad deberán identificar los controles a implementar sobre la información de acuerdo a la clasificación obtenida.

4.9. El Oficial de Seguridad conjuntamente con el Custodio de Información deberán implementar los controles identificados, de acuerdo a la clasificación de la información.

4.10. Según las características de los diferentes sistemas de información utilizados en producción, deben existir procedimientos para corrección de errores en ingreso de información. Estos procedimientos deben considerar una serie de aprobaciones y no infringir contra la característica de integridad de la información.

4.11. Toda información relacionada a los sistemas de información del Ministerio deben ser clasificada como "Confidencial" y ser tratada como tal.

DE LA AUDITORÍA Y CLASIFICACION DE LA INFORMACION

4.12. Se debe registrar toda la información clasificada utilizando la matriz de clasificación definida (Ver Anexo A – Matriz Centralizada de Clasificación de Información).

4.13. La matriz de clasificación de la información será revisada por todos los propietarios de la información de manera trimestral o cada vez que haya un cambio importante en el proceso y/o la manera como se administra la información.

4.14. Se deberá tener disponible para el Órgano de Control Institucional la matriz de clasificación para sus revisiones periódicas.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

7. Anexos

7.1. Anexo A – Matriz Centralizada de Clasificación de Información.

Proceso	Activo de Información	Tipo de Activo	Propietario de Información	Impacto Conf.	Impacto Int.	Impacto Disp.	Clasificación

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE COMPROBACIÓN TÉCNICA	
	CÓDIGO: NO-004	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE COMPROBACIÓN TÉCNICA

Ministerio de Educación	DOCUMENTO: NORMA DE COMPROBACIÓN TÉCNICA	
	CÓDIGO: NO-004	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

0107 -2008-ED

Ministerio de Educación	**DOCUMENTO:** NORMA DE COMPROBACIÓN TÉCNICA	
	CÓDIGO: NO-004	**EDICIÓN:** 01
		FECHA APROBACIÓN:

1. Objetivo

Garantizar que los controles de aplicación y de seguridad en la infraestructura tecnológica del Ministerio de Educación, en adelante el Ministerio, se encuentran operando de acuerdo a lo establecido.

2. Disposiciones Generales

El Oficial de Seguridad es responsable de verificar el cumplimiento de lo dispuesto en la presente norma.

3. Descripción

3.1. Todos mecanismos de control implantados como parte de la infraestructura tecnológica del Ministerio deben ser probados regularmente para comprobar su correcto funcionamiento.

3.2. Se debe contar con personal calificado para la realización de las comprobaciones técnicas. Las comprobaciones técnicas deben incluir pruebas de intrusión interna y/o externa, las cuales deben de ser realizadas por personal del Ministerio o por personal externo y/o consultoras especializadas.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CONEXIÓN DE REDES EXTERNAS	
	CÓDIGO: NO-005	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CONEXIÓN DE REDES EXTERNAS

Ministerio de Educación	DOCUMENTO: NORMA DE CONEXIÓN DE REDES EXTERNAS	
	CÓDIGO: NO-005	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE CONEXIÓN DE REDES EXTERNAS	
	CÓDIGO: NO-005	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Se deberá tener un claro entendimiento de los siguientes conceptos: los mecanismos necesarios al Ministerio de Educación (en adelante el Ministerio) para administrar y asegurar las conexiones que se tengan con redes externas.

2. Definición de términos

Se deberá tener un claro entendimiento de los siguientes conceptos:

Conexión externa: Una conexión externa se define como cualquier comunicación de datos establecida entre el Ministerio y una red externa, siendo independiente el origen y destino del sentido en el cual se establece la comunicación.

Registro de conexiones externas: Un registro de conexiones externas se define como una bitácora de conexiones realizadas por el Ministerio con redes externas.

3. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

3.1. El Oficial de Seguridad es responsable de:

- Definir los mecanismos de seguridad de información apropiados para las conexiones del Ministerio con redes externas.
- Aprobar el establecimiento de conexiones con redes externas y llevar un control de la habilitación / deshabilitación de las mismas en el Registro de Conexiones Externas.

3.2. El Custodio de Información es responsable de:

- Implementar los mecanismos de seguridad de información apropiados para las conexiones del Ministerio con redes externas.

3.3. El Responsable de Información es responsable de:

- Definir la importancia de la comunicación y si es requerido que el canal de comunicaciones se encuentre cifrado.

3.4. El Propietario del Proceso es responsable de:

- Definir, con apoyo del Oficial de Seguridad, los mecanismos de seguridad de información requeridos para las conexiones del Ministerio con redes externas.

4. Descripción

4.1. Para la conexión con terceros se debe establecer mecanismos de seguridad apropiados. Los responsables de definir e implementar dichos mecanismos serán el Oficial de Seguridad y el Propietario del Proceso. Eventualmente se pueden incluir especialistas en este proceso.

4.2. La conexión de las estaciones de trabajo y/o servidores del Ministerio con redes externas debe cumplir las políticas establecidas en este documento y documentos anexos.

4.3. En caso que la conexión con redes externas requiera mecanismos de seguridad y/o recursos adicionales a los existentes, el área solicitante deberá obtener las aprobaciones necesarias por parte del despacho ministerial.

4.4. No es responsabilidad del Ministerio, asegurar la protección de la información de la red externa mientras ésta se transmite o recibe.

4.5. La responsabilidad del Ministerio sobre la seguridad de la información que recibe de redes externas empieza después de recibida la información.

4.6. Toda conexión con redes externas deberá estar acorde con el modelo de conectividad con redes externas, aprobado por el Oficial de Seguridad y definido por el Propietario del Proceso y por el Custodio de Información, basándose en la arquitectura tecnológica de la compañía. Cualquier cambio o excepción solicitado al modelo, deberá ser evaluado y aprobado por el Oficial de Seguridad, el Propietario del Proceso y el Custodio de Información. El modelo de conectividad con redes externas esta detallado en el Anexo A – Modelo de conectividad con redes externas de la presente norma.

4.7. Toda conexión con redes externas debe contar con un convenio o acuerdo formal, en el cual se definan las características de la conexión, tales como tipo de conexión, horario de conexión, responsabilidades, medios de protección a utilizar, entre otros.

4.8. Las empresas que tengan conectada su red a la del Ministerio o aquellas empresas que mantengan equipos conectados a la red del mismo, deberán contar con un acuerdo formal o contrato en el cual se estipule una cláusula de cumplimiento de las políticas de seguridad del Ministerio.

4.9. Adicionalmente se debe considerar una cláusula de confidencialidad de la información manejada o accedida por el personal de la empresa externa. Esta cláusula de confidencialidad debe ser firmada por dichas personas y por el representante legal de su empresa.

4.10. Se debe contar con mecanismos de autenticación que permitan mantener un control de los accesos desde y hacia las conexiones de redes externas del Ministerio. Estos controles pueden incluir uso de contraseñas de autenticación asimétrica, tarjetas tokens y cifrado RSA.

DE LA SOLICITUD DE APROBACION DE CONEXIÓN CON REDES EXTERNAS

4.11. La solicitud de conexión con redes externas debe ser formal y registrarse por escrito. La solicitud debe ser emitida por la Jefatura de la cual depende la Oficina que necesita establecer la conexión y dirigida al despacho ministerial para evaluar la viabilidad del proyecto.

4.12. La información entregada en la solicitud debe incluir:

- Objetivo de conexión.
- Servicios y/o aplicativos que se requiere habilitar.
- Contacto técnico con la empresa externa.
- Características técnicas de la conexión, protocolo, velocidad, tipo de enlace.
- Período durante el cual debe estar habilitada la conexión.

Para los aspectos técnicos, el apoyo será entregado por el Custodio de Información del Ministerio. Eventualmente se puede incluir el apoyo de especialistas para estas actividades.

4.13. Siempre que la comunicación sea con externos, se debe tener en cuenta que el Responsable de la Información junto con el Oficial de Seguridad, el Propietario del Proceso y el Custodio de Información debe decidir, dependiendo de la importancia de la comunicación, si esta debe estar cifrada o no.

4.14. El Propietario del Proceso, el Oficial de Seguridad y la Alta Dirección deberán aprobar la conexión con una red externa, dicha aprobación se dará previo estudio del impacto en seguridad que generaría la conexión solicitada.

4.15. En caso que la conexión solicitada no cumpla con el modelo de conectividad con redes externas, se deberá contar adicionalmente con la aprobación del Comité Operativo de Seguridad de Información para el establecimiento de la conexión.

4.16. Sólo se podrá realizar las actividades que permitan establecer la comunicación con una red externa una vez otorgadas las aprobaciones establecidas en esta norma.

4.17. Una vez establecida la conexión, ésta se deberá registrar en el Registro de Conexiones Externas. Los responsables de mantener este registro son el Custodio de Información y el Oficial de Seguridad.

DE LA DESHABILITACIÓN DE CONEXIONES CON REDES EXTERNAS

4.18. Una conexión con redes externas podrá deshabilitarse toda vez que se detecte que está siendo utilizada para acceder a servicios no otorgados o que se está efectuando un mal uso de la misma.

4.19. Una conexión con redes externas que se determine como no necesaria, deberá ser deshabilitada en forma inmediata. El área solicitante de la conexión tendrá la responsabilidad de avisar formalmente al Oficial de Seguridad que ya no está haciendo uso de dicha conexión para que coordine su retiro.

4.20. El Custodio de Información realizará la desconexión con la autorización del Oficial de Seguridad y del Propietario del Proceso. Una vez deshabilitada la conexión se deberá actualizar el Registro de Conexiones Externas.

DE LA AUDITORÍA Y REVISIÓN DE CONEXIONES CON REDES EXTERNAS

4.21. Se debe registrar toda actividad que corresponda a una conexión con redes externas al Ministerio utilizando para ello el archivo de registros de auditoria del dispositivo de seguridad o comunicación que controla dicho enlace, o los aplicativos asociados a este control.

4.22. El monitoreo de dichas conexiones se hará de acuerdo a lo definido en la Norma de Control de Acceso a los Recursos de Red (NO-007)

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

7. Anexos

7.1. Anexo A – Modelo de Conectividad con redes externas.

Ministerio de Educación	DOCUMENTO: NORMA DE CONEXIÓN DE REDES EXTERNAS	
	CÓDIGO: NO-005	EDICIÓN: 01
		FECHA APROBACIÓN:

Este modelo busca establecer las exigencias y condiciones que deben ser consideradas al momento de concretar una conexión con redes externas.

A. Conectividad

1. Cualquier conexión con redes externas, independiente de su modo de conexión, debe acceder al Ministerio a través de algún firewall o router, con listas de acceso. Estos dispositivos deben ser administrados por el Custodio de Información o por la persona a quien el Ministerio entregue esta responsabilidad. Ningún acceso a cualquier servicio, podrá realizarse en forma directa.
2. Debe privilegiarse la utilización de un canal único de comunicación para toda conexión desde o hacia el exterior de la red corporativa del Ministerio.
3. En caso de no ser una conexión TCP/IP o punto a punto, se deberá efectuar un control a nivel aplicativo.
4. En caso que equipos externos se conecten a la red del Ministerio, deberá privilegiarse el acceso de éstos a través de un dominio definido para estos efectos y conectados físicamente con dispositivos de comunicaciones dedicados para este tipo de conexiones haciendo una segregación física y lógica desde la red.

B. Tipo de Conexión

1. Las conexiones con terceros sólo podrán ser de alguno de los siguientes tipos, cualquier excepción debe ser aprobada por la Oficina de Informática:
   - Enlace dedicado.
   - Enlace Internet.
   - Enlace satelital.
2. No se considera válida la conexión de módems internos a redes externas. En caso que sea necesario para la función del negocio, se deberá habilitar mecanismos de seguridad de control de acceso a las estaciones de trabajo conectadas, como son firewalls personales, IDS personales, u otros.
3. En caso que se tenga una estación de trabajo del Ministerio conectada físicamente a una red de una institución externa, y se requiera que dicha PC se conecte a servicios internos del Ministerio, esta conexión sólo podrá ser efectuada a través de redes privadas virtuales (VPN), u otro mecanismo que permita alcanzar los mismos niveles de confidencialidad e integridad. Esta PC deberá tener adicionalmente mecanismos de protección y filtro para impedir el acceso a esta máquina desde la red externa a la que se conecta.
4. Se deberá configurar correctamente a los equipos de comunicación para la utilización de técnicas de NAT para la conversión de conexiones de red

C. Servicios Ofrecidos

1. Los servicios ofrecidos en la conexión con redes externas estarán limitados sólo a los necesarios y sólo en los dispositivos que se requiera, por lo tanto la especificación técnica debe ser lo más exacta posible.
2. No se permite asignar acceso ilimitado a cualquier usuario. Por defecto, cualquier acceso estará negado y en la medida de los requerimientos alcanzados al Oficial de Seguridad se habilitará los servicios específicos según lo indicado en la norma NO-007 - Control de Acceso a los Recursos de Información.

0107-2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO A LAS LIBRERÍAS DE PROGRAMAS FUENTE	
	CÓDIGO: NO-006	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CONTROL DE ACCESO A LAS LIBRERÍAS DE PROGRAMAS FUENTE

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO A LAS LIBRERÍAS DE PROGRAMAS FUENTE	
	CÓDIGO: NO-006	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	**DOCUMENTO:** NORMA DE CONTROL DE ACCESO A LAS LIBRERÍAS DE PROGRAMAS FUENTE	
	CÓDIGO: NO-006	**EDICIÓN:** 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de corrupción en los sistemas de aplicación debido a accesos no autorizados del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

El Oficial de Seguridad es responsable de:

2.1. El personal del Área de Infraestructura Tecnológica es el único autorizado de acceder al ambiente de producción del Ministerio.

2.2. El Oficial de Seguridad es responsable de verificar que los accesos al ambiente de producción se encuentra restringido y limitado a las personas autorizadas.

3. Descripción

3.1. Los archivos ejecutables, con sus respectivas librerías, deben de limitarse a los mínimos necesarios para que los sistemas de aplicación funcionen de manera adecuada.

3.2. En la medida de lo posible, los archivos fuente de los sistemas de aplicación del Ministerio no deben de almacenarse ni acompañar a los archivos ejecutables en el ambiente de producción.

3.3. Toda labor que se realice en el ambiente de producción, que involucre la actualización de los ejecutables y/o librerías de los sistemas de aplicación, debe cumplir con lo establecido en la Norma Administración de Cambios de Sistemas de Información (NO-001) y en la Norma de Respaldo de Información (NO-020).

3.4. Todo cambio que se efectúe en el ambiente de producción del Ministerio, debe quedar registrado en una bitácora, la cual como mínimo debe indicar lo siguiente:

- Fecha y Hora del cambio
- Personal que realiza el cambio
- Aplicaciones afectadas

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO A LOS RECURSOS DE INFORMACIÓN	
	CÓDIGO: NO-007	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CONTROL DE ACCESO A LOS RECURSOS DE INFORMACIÓN

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO A LOS RECURSOS DE INFORMACIÓN	
	CÓDIGO: NO-007	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO A LOS RECURSOS DE INFORMACIÓN	
	CÓDIGO: NO-007	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Establecer el control y seguimiento de los accesos a los recursos de información que conforman la infraestructura tecnológica del Ministerio de Educación, en adelante el Ministerio, con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información minimizando los riesgos e incidentes de seguridad en la misma.

2. Definición de términos

Se deberá tener un claro entendimiento de los siguientes conceptos:

2.1. **Recurso de Información:** Toda información que tiene valor para la organización.

Todo recurso de información puede ser accedido por sistemas de aplicación, motores de bases de datos, carpetas compartidas o cualquier otro mecanismo que permita la consulta, creación, modificación, eliminación o actualización de los recursos de información.

2.2. **Controles de acceso:** Mecanismos que permiten restringir el acceso a los recursos de información. Un ejemplo de controles de acceso puede ser un directorio activo, listas de control de acceso, entre otros.

2.3. **Directorio Activo**: Servicio LDAP que permite a los administradores de red establecer políticas a nivel de empresa, desplegar programas en muchas computadoras y aplicar actualizaciones críticas a una organización entera. Un Directorio Activo almacena información de una organización en una base de datos central, organizada y accesible.

2.4. **Usuario de Dominio:** Cuenta registrada en el directorio activo de la organización y asignada a un único trabajador del Ministerio.

3. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

3.1. El oficial de Seguridad es responsable de:

- Definir los mecanismos de seguridad de información apropiados para verificación del adecuado uso y asignación de accesos a los recursos de información de la institución.
- Realizar un muestreo trimestral de todos los accesos otorgados en el periodo con la finalidad de verificar el cumplimiento de la presente norma.

3.2. La Oficina de Informática es responsable de:

- Creación y asignación de accesos a los recursos de información a los trabajadores del Ministerio que necesiten de los mismos para realizar sus labores.

4. Descripción

4.1. Los recursos de tratamiento y comunicaciones de la información del Ministerio permiten el normal desempeño de las actividades parar las que son destinadas. Por tal motivo su acceso físico y/o electrónico comprende:

- Las áreas y el entorno en donde se encuentran. Estas son áreas seguras y los entornos están protegidos por perímetros de seguridad definidos, con barreras de seguridad, controles de entrada y acceso apropiados.
- La seguridad de los equipos. Evitar perdidas, daños o comprometer la actividad y continuidad de los mismos.
- Controles Generales. Prevenir la exposición a riesgo o robos de información y de recursos de tratamiento de información.
- Control de acceso. Controlar el acceso a la información en base a los requisitos de seguridad y requerimientos de función.
- Gestión de accesos de usuarios. Evitar accesos no autorizados a los recursos de información. Esto contempla la supervisión de accesos.
- Control de acceso a la red. Controlar el acceso a los servicios, así como las redes internas y externas. El acceso a la red y servicios no comprometen la seguridad de los mismos.
- Control de acceso al Sistema Operativo. Evitar accesos no autorizados a los computadores.
- Control en la Identificación y autenticación de usuario. Identificador único para uso personal y exclusivo, a fin de manifestarse y auditarse las actividades de cada responsable particular.

4.2. El usuario se responsabiliza en el mantenimiento de la eficacia de las medidas de control de acceso, para ello debe de seguir las pautas de seguridad sobre el material puesto a su disposición.

DEL CONTROL DE ACCESO A LOS RECURSOS DE INFORMACIÓN

4.3. Para la creación de una cuenta de acceso a la red para el personal del Ministerio que por sus funciones así lo requiera, la Jefatura a la cual pertenece la Oficina responsable deberá solicitar la creación y activación de la cuenta de acceso a la Oficina de Informática a través de un Oficio.

4.4. Toda solicitud de acceso a los recursos de información deberá ser aprobada de acuerdo a lo establecido en la Matriz de Propietarios de Información.

4.5. Los accesos a los recursos de información deben encontrarse debidamente segmentados por las personas responsables a cargo. Por ejemplo, los accesos a los recursos de red no deberán ser otorgados por los responsables de accesos a sistemas de aplicación.

4.6. La incorporación de cada usuario de dominio a la red del Ministerio, involucra la asignación de una cuenta de usuario, la misma que representa la identificación digital, a través de la cual el usuario podrá hacer uso de los diferentes recursos de información. Esta cuenta de dominio está conformada por un nombre de usuario y una contraseña.

4.7. La identificación digital de cada empleado es única e intransferible. Es responsabilidad del trabajador conservar esta identificación digital en secreto y en uso personal exclusivo, asimismo

deberá seguir las políticas de contraseñas, seguridad y uso de la red detallada en presente documento.

4.8. Para los sistemas de aplicación, todo usuario deberá contar con una cuenta de usuario que le permite acceder únicamente a la información requerida por él para realizar sus funciones. El acceso a los sistemas de aplicación debe también ser solicitado mediante un oficio a la Oficina de Informática remitido por el Jefe inmediato superior del usuario.

4.9. Todos los sistemas de aplicación deben contar con un sistema de gestión de contraseñas de modo que se cumpla con lo estipulado en la presente norma.

4.10. Queda totalmente prohibido intentar burlar las restricciones de la cuenta de usuario de dominio asignada. Asimismo, de ocurrir algún incidente de violación de la seguridad, tratando de usar una cuenta de usuario que no le pertenezca y/o haya sido obtenida con cualquier medio y no haya sido autorizado por el mismo, el empleado asociado a dicha cuenta será el responsable directo de dicho acto, el mismo deberá tomar las medidas necesarias para garantizar la inviolabilidad y uso personal de su cuenta de usuario.

4.11. Cualquier trabajador que a través de su cuenta de usuario de dominio haga un mal uso de los recursos de información, o que haga un uso indebido de técnicas de rompimiento y/o hacking será sometido a la auditoria de su computador, función a cargo de la Oficina de Informática y que mediante un informe comunicará los hechos, con copia a la Unidad de Personal para su evaluación y sanción correspondiente.

4.12. Las cuentas de usuario del directorio activo tienen un formato específico de etiqueta: Primera letra del nombre seguido del apellido paterno. En caso de ya existir en el directorio activo una cuenta coincidente con este formato, se añadirán consecutivamente las letras del primer nombre hasta que no haya coincidencia.

4.13. El formato y sintaxis de cada contraseña deberá cumplir como mínimo con lo establecido en los siguientes lineamientos de formato, tamaño, número de caracteres y tiempo de vida:

- Longitud mínima de 6 caracteres
- Combinación mínima obligatoria de letras mayúsculas, letras minúsculas y números.
- Vigencia de 42 días, al término de los cuales se forzará el cambio de contraseña, no pudiendo repetir las tres (03) últimas.

4.14. Al crearse cada cuenta, se establece una contraseña por defecto, la cual es forzada a cambiarse por el sistema luego del primer inicio de sesión. El usuario elige la contraseña con el formato y sintaxis indicados y asume la responsabilidad sobre la inviolabilidad de su contraseña desde ese momento y cada vez que la renueve.

4.15. Se debe establecer un mecanismo adecuado que brinde confidencialidad e integridad a la entrega de las credenciales de acceso a los recursos de información.

4.16. Se deberán establecer políticas de restricción de acceso por perfiles restringiendo la instalación de software no autorizado y de acceso a panel de control y otras opciones de configuración de los computadores. Siempre que se requiera para el normal cumplimiento de sus funciones, se podrán solicitar excepciones temporales de dichas restricciones, las que serán dirigidas por el Jefe Inmediato Superior del usuario mediante correo electrónico firmado digitalmente a la Oficina de Informática. El personal de la Oficina de Informática, por la naturaleza propia de su desempeño y sus funciones están exceptuados de estas restricciones, así como los Jefes.

4.17. El acceso a los servicios y privilegios (correo electrónico, Internet, mensajería instantánea, etc) deberá ser solicitado mediante correo electrónico firmado digitalmente al Jefe de la Oficina de Informática con copia al Jefe del área de Sistemas de Información por el Jefe Inmediato Superior del usuario, contando con la aprobación de la Secretaría a la que pertenece.

4.18. Durante el proceso de autenticación ante el sistema de red, el usuario tendrá tres intentos para ingresar su contraseña correcta. Si en los 3 intentos ingresa una contraseña incorrecta, la cuenta se bloqueará automáticamente. Para volver a activar dicha cuenta deberá ponerse en contacto con el Administrador de la Red o el personal responsable del sistema que administra dicha cuenta.

4.19. Los registros de eventos de auditoría son realizados de acuerdo a niveles de clasificación en importancia, los niveles que se contempla son:

- ALTA, se almacenan hasta por un periodo de 6 meses.
- MEDIA, se almacenan hasta por un periodo de 3 meses.
- BAJA, se almacenan hasta por un periodo de 1 mes.

Se podrán registrar los siguientes parámetros:

- Identificación del usuario.
- Fecha y hora de conexión y desconexión.
- Identificación del Terminal o el lugar si es posible.
- Registro de los intentos aceptados y rechazados de acceso al sistema.
- Registro de los intentos aceptados y rechazados de acceso a datos y otros recursos.

4.20. Los dispositivos o recursos de telecomunicaciones en el tratamiento de la información tienen configuradas rutas forzosas y dominio lógicos de acceso de acceso al sistema, los cuales están segmentados y divididos tomando como premisa el control de acceso a los recursos de información, políticas y normas de la institución.

4.21. Se aplican medidas de protección para los dispositivos de la red LAN para la protección y acceso de los mismos y para evitar que usuarios no autorizados puedan modificar las configuraciones establecidas.

4.22. Los principales servidores de aplicaciones deberán utilizar certificados digitales para proteger las posibles intercepciones internas y garantizar la confidencialidad de la información de las comunicaciones electrónicas.

4.23. En caso que un tercero haya sido contratado por el Ministerio, y para ejercer sus labores necesite una cuenta para acceder a los servicios y a la red, se deben cumplir todos los puntos anteriormente mencionados. Así mismo, si es que el tercero hará uso de su propio computador para conectarse a la red, el Área de Sistemas de Información deberá revisar dicho equipo con la finalidad de verificar el cumplimiento del estándar de seguridad mínimo establecido, y debe emitir un informe para poder proceder a la creación de la cuenta de acceso.

4.24. Toda creación, modificación o eliminación de accesos a los recursos de información deberá ser documentada en una bitácora de controles de acceso.

DEL CONTROL DE ACCESO AL SISTEMA OPERATIVO

4.25. Se deberá tener control de la descripción y ubicación física de cada usuario de los recursos de información, en la cual se especifique la dirección lógica o IP asociada.

4.26. Para el control y registro de intentos de acceso mal intencionados se debe contar con soluciones de Detección de Intrusos dentro de la red y fuera de ella (IDS interno e IDS externo).

4.27. Todo usuario autorizado deberá tener una cuenta que lo identifica, con su correspondiente contraseña. La excepción corresponde a equipos utilizados masivamente en la parte operativa, para los que se definen cuentas genéricas que identifican la función (ejemplo: ingresos, aprobaciones, etc.) y que asocia cada cuenta a un único perfil de usuario. Cada perfil mostrará en el escritorio del computador solamente los iconos de las aplicaciones requeridas para cada función. Estas cuentas de dominio no tiene asociadas direcciones de correo electrónico, pues para ello se requieren usuarios específicos. La existencia de cuentas genéricas deberá ser soportada por documentación que indique el o los responsables de dichas cuentas, así como también el tiempo por el cual dicha cuenta permanecerá activa.

4.28. La conexión es válida sólo si el usuario ha ingresado todos los datos solicitados: usuario y contraseña, y se registra en el visor de eventos de los Controladores de Dominio su intento de ingreso (sea éste exitoso o no exitoso).

DE LA DESACTIVACIÓN DEL ACCESO

4.29. Cuando se da de baja a un usuario a quien se otorgó una cuenta con acceso a los recursos de información del Ministerio, la Jefatura responsable deberá solicitar la eliminación de su cuenta y privilegios otorgados a la Oficina de Informática a través de un Oficio, en lo posible el mismo día del cese de funciones del usuario.

4.30. El Oficial de Seguridad deberá incorporar en sus actividades la revisión selectiva del inventario de equipos asignados a usuarios, verificando en forma aleatoria la asignación efectuada y su respectivo uso.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO AL CENTRO DE DATOS	
	CÓDIGO: NO-008	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CONTROL DE ACCESO AL CENTRO DE DATOS

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO AL CENTRO DE DATOS	
	CÓDIGO: NO-008	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO AL CENTRO DE DATOS	
	CÓDIGO: NO-008	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Normar el acceso al ambiente del centro de datos del Ministerio de Educación, en adelante el Ministerio, con el fin de asegurar la disponibilidad, confidencialidad e integridad de la información almacenada en los equipos informáticos.

2. Definición de términos

2.1. **Centro de datos:** Ambiente físico donde se encuentran los servidores de producción y equipos principales del Ministerio que están bajo la supervisión del Custodio de Información.

3. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

3.1. El Oficial de Seguridad es responsable de:

- Verificar rutinariamente el adecuado funcionamiento de los controles de accesos físico instalados en el Centro de Datos.

3.2. El Custodio de Información es responsable de:

- Verificar rutinariamente el adecuado funcionamiento de los controles de accesos físico instalados en el Centro de Datos.

4. Descripción

DE LAS RESTRICCIONES FÍSICAS DE ACCESO AL Centro de Datos

4.1. Las puerta de acceso al Centro de Datos debe permanecer cerrada constantemente y sólo debe ser abierta cuando sea necesario el ingreso y/o salida de personal autorizado.

4.2. Todos los equipos que contengan datos de producción deberán estar en el interior del Centro de Datos del Ministerio.

4.3. La puerta de acceso debe contar con un equipo "cierra puertas" y un dispositivo automático de control de acceso (Ejemplos: tarjeta de proximidad, biometría, códigos de acceso, etc.).

4.4. El Centro de Datos no debe contar con ventanas que expongan dicha área con el exterior u otras áreas. Debe procurarse utilizar una única puerta de acceso, contando las demás con dispositivos de alarma.

4.5. Queda prohibido el ingreso al Centro de Datos con bebidas, comidas, armas, y material inflamable (se exceptúa el papel necesario para ser usado en impresiones, el cual debe ser ingresado antes de la impresión y retirado inmediatamente después de terminada la misma).

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO AL CENTRO DE DATOS	
	CÓDIGO: NO-008	EDICIÓN: 01
		FECHA APROBACIÓN:

DE LAS MEDIDAS DE CONTROL DE ACCESO

4.6. El acceso al Centro de Datos del Ministerio debe estar físicamente restringido. Únicamente tendrá acceso permanente a esta área, el Custodio de Información, el Oficial de Seguridad y el operador que se encuentre de turno.

4.7. El ingreso al Centro de Datos debe ser informado previamente por medio del envió de un Correo Electrónico firmado digitalmente, dirigido al Jefe de la Oficina de Informática con copia al Jefe del Área de Infraestructura Tecnológica indicando lo siguiente:

- Unidad Orgánica a la que pertenece(n) el(los) usuario(s) o procedencia del(los) terceros.
- Nombre de el(los) usuario(s) o del(los) tercero(s).
- Motivo de la visita
- En caso de mantenimiento de equipos y/o servicios por un tercero se debe señalar la duración estimada de la visita. Asimismo, los visitantes deben ser asistidos y supervisados por el personal de las unidades orgánicas involucradas.

4.8. Los accesos del personal al Centro de Datos se clasifican en tres tipos de acuerdo a lo siguiente:

- **Acceso Directo**: es el que se otorga al personal que por naturaleza de sus funciones tiene acceso permanente a las instalaciones del Centro de Datos y no requiere autorización expresa. (Ver Anexo B – Formato: Relación de personal con acceso directo al centro de datos)

- **Acceso Autorizado**: es el que se otorga al personal que requiere ingresar al Centro de Datos eventualmente. Este personal debe figurar en una lista autorizada (Ver Anexo C – Formato: Relación de personal autorizado de ingreso al centro de datos) y debe registrar su ingreso en la Bitácora de Control de Acceso al Centro de Datos (Ver Anexo A – Formato: Bitácora de Control de acceso al centro de datos).

- **Acceso Especial**: es el que se otorga excepcionalmente a personal diverso y por lo tanto requiere autorización expresa del responsable del Centro de Datos. A su vez debe registrar su ingreso en la Bitácora de Control de Acceso al Centro de Datos (Ver Anexo A – Formato: Bitácora de Control de acceso al centro de datos).

4.9. El Operador del Centro de Datos es el encargado de registrar y asistir al visitante. En él recae la responsabilidad del actuar del visitante dentro del área en mención.

4.10. El personal de limpieza o de seguridad física deberán acceder al Centro de Datos bajo la supervisión del operador de turno.

4.11. Los ingresos y salidas al Centro de Datos debe ser registrados en todos los casos en la bitácora de Control de Acceso al Centro de Datos.

- En el caso de personal autorizado este registro debe efectuarse utilizando el mecanismo de control de acceso implementado.
- Estos registros deben ser custodiados y respaldados en forma adecuada.
- El acceso de personal ajeno al Centro de Datos deberá ser registrado en una bitácora o registro de acceso. Se deberá registrar en esta bitácora: fecha, hora de ingreso, motivo de ingreso, hora de salida y quien autorizó dicho ingreso. (Ver Anexo A)

4.12. Todo personal del Ministerio debe alertar y/o cuestionar la presencia de desconocidos dentro de los Centro de Datos.

4.13. A menos que se autorice expresamente, no debe permitirse el ingreso de equipos fotográficos, de vídeo, audio u otro tipo de equipamiento que registre información.

4.14. El personal sólo debe tener conocimiento de la existencia de un Centro de Datos o de las actividades que se llevan a cabo dentro de éste, según el criterio de necesidad de conocer.

4.15. No debe permitirse el acceso de ningún equipo que no esté plenamente identificado, debiéndose registrar su procedencia, utilización, número de serie y partes. Al salir este equipo del Centro de Datos debe ser revisado y los datos corroborados.

4.16. Debe existir un plan de evacuación preestablecido, conocido y evaluado. Se debe procurar contar con una salida de emergencia.

4.17. Todos los usuarios autorizados a entrar al Centro de Datos, deben hacerlo utilizando sus propias identificaciones. Está prohibido que los usuarios autorizados o no, entren aprovechando la entrada de otro usuario autorizado.

DE LA AUDITORÍA Y REVISIÓN DEL CONTROL DE ACCESO AL Centro de Datos

4.18. El Oficial de Seguridad revisará mensualmente el log del dispositivo de control de acceso para identificar los usuarios autorizados y la frecuencia de acceso al Centro de Datos.

4.19. El Oficial de Seguridad revisará mensualmente el correcto uso de la bitácora de acceso al Centro de Datos para el personal externo.

4.20. Se deberá tener disponible para el área de auditoría y los auditores externos los logs de acceso al Centro de Datos y las bitácoras de acceso para el personal externo.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DE ACCESO AL CENTRO DE DATOS	
	CÓDIGO: NO-008	EDICIÓN: 01
		FECHA APROBACIÓN:

7. Anexos

7.1. Anexo A – Formato: Bitácora de control de acceso al centro de datos

Fecha	Persona	Hora de Ingreso	Hora de Salida	Autoriza	Motivo de Ingreso

7.2. Anexo B – Formato: Relación de personal con acceso directo al centro de datos

Personal con acceso directo al Centro de Datos

Nombres	Apellidos	Persona que autoriza	Área

7.3. Anexo C– Formato: Relación de personal autorizado de ingreso al centro de datos

Personal autorizado de ingreso al centro de datos

Fecha	Persona	Hora de Ingreso	Hora de Salida	Autoriza	Motivo de Ingreso

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DEL SOFTWARE EN PRODUCCIÓN	
	CÓDIGO: NO-009	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CONTROL DEL SOFTWARE EN PRODUCCIÓN

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DEL SOFTWARE EN PRODUCCIÓN	
	CÓDIGO: NO-009	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROL DEL SOFTWARE EN PRODUCCIÓN	
	CÓDIGO: NO-009	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de existencia de software no autorizado en el ambiente de producción del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

2.1. El personal del Área de Infraestructura Tecnológica es el único autorizado de acceder al ambiente de producción del Ministerio.

2.2. El Oficial de Seguridad es responsable de verificar que los accesos al ambiente de producción se encuentra restringido y limitado a las personas autorizadas.

3. Descripción

3.1. Los archivos ejecutables, con sus respectivas librerías, deben de limitarse a los mínimos necesarios para que los sistemas de aplicación funcionen de manera adecuada.

3.2. En la medida de lo posible, los archivos fuente de los sistemas de aplicación del Ministerio no deben de almacenarse ni acompañar a los archivos ejecutables en el ambiente de producción.

3.3. Toda labor que se realice en el ambiente de producción, que involucre la actualización de los ejecutables y/o librerías de los sistemas de aplicación, debe cumplir con lo establecido en la NO-001 - Norma Administración de Cambios de Sistemas de Información y en la NO-020 - Norma de Respaldo de Información.

3.4. Todo cambio que se efectúe en el ambiente de producción del Ministerio, debe quedar registrado en una bitácora, la cual como mínimo debe indicar lo siguiente:

- Fecha y hora del cambio.
- Personal que realiza el cambio.
- Aplicaciones afectadas.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROLES CRIPTOGRÁFICOS	
	CÓDIGO: NO-010	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CONTROLES CRIPTOGRÁFICOS

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROLES CRIPTOGRÁFICOS	
	CÓDIGO: NO-010	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROLES CRIPTOGRÁFICOS	
	CÓDIGO: NO-010	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Definir la gestión de controles criptográficos para el envío/recepción de información en medios magnéticos/ópticos del Ministerio de Educación, en adelante el Ministerio.

2. Definición de términos

Se deberá tener un claro entendimiento de los siguientes conceptos:

2.1. **Métodos criptográficos:** Los métodos criptográficos están basados en algoritmos matemáticos (funciones) tales que aplicados sobre ciertos datos (información) más un argumento variable (clave) producen un determinado resultado no legible (texto cifrado).

Los algoritmos matemáticos usados en criptografía cumplen con ciertas condiciones, entre ellas, la fundamental, que es sencillo computarla en un sentido, y prácticamente imposible en sentido inverso, sin conocer algún dato.

2.2. **Autenticación**: es la función para el establecimiento de la validez de la supuesta identidad de un usuario, dispositivo u otra entidad en un sistema de información o comunicaciones.

2.3. **Disponibilidad**: la propiedad de que los datos, la información y los sistemas de información y comunicaciones sean accesibles y utilizables oportunamente y en la forma precisa

2.4. **Confidencialidad**: es la propiedad de que los datos o la información no sean disponibles, ni se revele, a personas, entidades o procesos no autorizados.

2.5. **Criptografía**: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

2.6. **Clave criptográfica**: es un parámetro que se utiliza junto con un algoritmo criptográfico para transformar, validar, autenticar, cifrar o descifrar datos.

2.7. **Datos**: es la presentación de información de una forma adecuada para su comunicación, interpretación, almacenamiento, o tratamiento.

2.8. **Cifrado**: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (datos cifrados) y asegurar su confidencialidad.

2.9. **Descifrado**: es la función inversa al cifrado.

2.10. **Integridad de los datos**: es la propiedad de que los datos o la información no hayan sido modificados o alterados de forma no autorizada.

2.11. **Sistema de gestión de claves**: es un sistema para la generación, almacenamiento, distribución, revocación, eliminación, archivo, certificación o aplicación de claves criptográficas.

2.12. **Depositario de la clave**: es una persona o entidad que está en posesión o tiene el control de las claves criptográficas. El depositario de la clave no es necesariamente el usuario de la misma.

2.13. **No repudio**: es una propiedad que se consigue a través de medios criptográficos, que impide a una persona o entidad negar haber realizado una acción en particular relativa a datos (como los

mecanismos de no rechazo de autoría (origen); como demostración de obligación, intención o compromiso; o como demostración de propiedad).

2.14. **Datos personales**: es cualquier información referente a una persona identificada o identificable.

3. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

3.1. La Oficina de Informática es responsable de:

- Resguardar las claves públicas de los usuarios, y de tenerlas disponibles de forma permanente para las distintas áreas de negocio.
- Mantener actualizada esta norma, como así también los procedimientos asociados, y la capacitación de las áreas internas involucradas.

4. Descripción

DE LA CONFIANZA EN LOS MÉTODOS CRIPTOGRÁFICOS

4.1. Los métodos criptográficos deben ser fiables, para generar confianza en el uso de los sistemas de información y comunicaciones.

4.2. Aunque los estándares internacionales deberían bastarse para lograr confianza en los sistemas fiables, los reglamentos gubernamentales, las licencias, y el uso de los métodos criptográficos deben asimismo fomentar la confianza del usuario. La evaluación de los métodos criptográficos, especialmente en comparación con criterios ya aceptados por el mercado, también podría generar confianza por parte del usuario.

4.3. En interés de la confianza del usuario, cualquier contrato referente al uso de un sistema de gestión de claves debería indicar la jurisdicción cuyas leyes se aplican a dicho sistema.

4.4. El uso de controles de acceso o criptográficos puede incluir la adquisición de hardware y/o software para cumplir con los requerimientos criptográficos del Ministerio.

DE LA ELECCIÓN DE MÉTODOS CRIPTOGRÁFICOS

4.5. Los usuarios deben disponer de acceso a una criptografía que responda a sus necesidades, de modo que puedan confiar en la seguridad de los sistemas de información y comunicaciones, y en la confidencialidad e integridad de los datos que manejan estos sistemas. La definición del método criptográfico a implementar para atender las necesidades del usuario, será responsabilidad de los órganos de seguridad competentes.

Las personas o entidades que posean, controlen, accedan, utilicen o almacenen datos pueden tener la responsabilidad de proteger la confidencialidad e integridad de dichos datos, y pueden por tanto ser responsables de utilizar los métodos criptográficos adecuados. Es posible que sean necesarios varios métodos criptográficos para cumplir los diferentes requisitos de seguridad de los datos.

Los responsables de la seguridad deben tener la libertad, dentro de la legalidad vigente, de determinar el tipo y nivel necesarios de seguridad de los datos, así como de seleccionar y aplicar los métodos criptográficos adecuados, incluyendo un sistema de gestión de claves que se adecue a sus necesidades.

DE LAS NORMAS PARA MÉTODOS CRIPTOGRÁFICOS

4.6. Las normas técnicas, criterios y protocolos para el uso de determinados métodos criptográficos deben haber sido desarrolladas y promulgadas a nivel nacional.

4.7. Las normas nacionales para los métodos criptográficos, en caso de existir, deben ser conformes con las normas internacionales para facilitar la interoperabilidad, adaptabilidad y movilidad global.

4.8. Se deberá implementar el uso de una técnica criptográfica para la transmisión de información confidencial a través de la red del Mnisterio.

4.9. Se deberá incluir el uso de firmas digitales en las transmisiones electrónicas realizadas por los usuarios del Ministerio.

4.10. Se deberá configurar adecuadamente el registro de pistas de auditoría sobre los controles criptográficos utilizados, con el fin de evitar situaciones de repudio de transacciones.

4.11. El Ministerio es el responsable de proteger los distintos tipos de claves que utilice para el cifrado de información. Se deberá implementar un sistema de gestión de claves para dar soporte a usuarios de claves públicas y privadas, protegiéndolas de su modificación o destrucción.

DE LA PROTECCIÓN DE LA INFORMACIÓN CRÍTICA DE LA INSTITUCIÓN

4.12. Los métodos criptográficos pueden ser una valiosa herramienta para la protección de la intimidad, incluyendo tanto la confidencialidad de los datos y comunicaciones como la protección de la identidad de las personas.

Sin embargo, la aplicación de métodos criptográficos dentro del Ministerio se encuentra destinada a mantener la seguridad de la información crítica de la institución con respecto a su confidencialidad, integridad y disponibilidad. No es responsabilidad del Ministerio proteger la información personal de los usuarios a través de la aplicación de métodos criptográficos.

DEL ACCESO LEGAL

4.13. Las políticas criptográficas nacionales pueden permitir un acceso legal a texto claro o a claves criptográficas, de los datos cifrados. Estas políticas deben respetar el resto de los principios que forman parte de las directrices, en la mayor medida posible.

4.14. Cuando se consideren las políticas sobre métodos criptográficos que faciliten el acceso legal, las entidades deben sopesar cuidadosamente los beneficios, incluyendo los beneficios para el orden público, la aplicación de la ley y la seguridad nacional, así como los riesgos de un mal uso, los gastos adicionales de cualquier infraestructura de apoyo, las perspectivas de fallos técnicos, y otros costes.

4.15. En el caso de que se solicite el acceso al texto en claro, o a las claves criptográficas de los datos cifrados, dentro de un proceso legal, la persona o entidad que solicite dicho acceso debe tener un derecho legal a la posesión del texto en claro, y una vez obtenido, los datos deben utilizarse sólo para fines legítimos. El proceso a través del cual se obtiene el acceso legal debe quedar registrado, de forma que se pueda auditar o revisar la revelación de las claves criptográficas de los datos, de acuerdo con el derecho nacional. Cuando se solicite y se obtenga el acceso legal, dicho acceso debe concederse dentro de unos límites de tiempo fijados, de forma adecuada a las circunstancias. Las condiciones del acceso legal deben indicarse claramente y hacerse públicas de una forma que

sean fácilmente disponibles para los usuarios, depositarios de las claves y proveedores de métodos criptográficos.

4.16. Los sistemas de gestión de claves proporcionan una base para una posible solución que podría equilibrar el interés de los usuarios y autoridades encargadas de la aplicación de la ley; estas técnicas también se podrán para recuperar datos, en caso de pérdida de las claves. Los procesos de acceso legal a las claves criptográficas deben reconocer la distinción entre las claves que se utilizan para proteger la confidencialidad y las claves que se utilizan únicamente con otros fines. No debe proporcionarse una clave criptográfica que proporcione sólo identidad o integridad sin el consentimiento de la persona o entidad que tiene la propiedad legítima de dicha clave.

DE LA RESPONSABILIDAD

4.17. Cuando así lo establezcan un contrato o la legislación, la responsabilidad de personas y entidades que ofrecen servicios criptográficos o son depositarios o acceden a las claves criptográficas, deberá exponerse claramente.

4.18. La responsabilidad de cualquier persona o entidad, incluyendo un organismo gubernamental, que ofrece servicios criptográficos o posee o tiene acceso a claves criptográficas, debe quedar claramente establecida, mediante contrato o, en los casos pertinentes, a través de la legislación nacional e internacional. Asimismo, debe indicarse claramente la responsabilidad de los usuarios por un mal uso de sus propias claves. A un depositario de clave no pueden exigírsele responsabilidades por proporcionar claves criptográficas o texto en claro de datos cifrados, si se ha realizado de forma acorde con un acceso legal. La parte que consiga un acceso legal debe ser responsable del mal uso de las claves criptográficas o del texto en claro que haya obtenido.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROLES DE AUDITORÍAS DE SISTEMAS	
	CÓDIGO: NO-011	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CONTROLES DE AUDITORÍAS DE SISTEMAS

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROLES DE AUDITORÍAS DE SISTEMAS	
	CÓDIGO: NO-011	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE CONTROLES DE AUDITORÍAS DE SISTEMAS	
	CÓDIGO: NO-011	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Garantizar la disponibilidad de información que permitan una adecuada realización de una Auditoría de Sistemas de la plataforma tecnológica del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

El Oficial de Seguridad es responsable verificar el cumplimiento de lo dispuesto en la presente norma.

3. Descripción

3.1. Se deben planificar y acordar distintas actividades de auditoría que impliquen comprobaciones a los sistemas operativos.

3.2. Todos los accesos deben ser registrados y supervisados.

3.3. Se debe tener toda la documentación de procedimientos, políticas y normas actualizadas.

3.4. Se deben de realizar auditorías de sistemas internas a cargo del Órgano de Control Institucional.

3.5. El acceso a las distintas herramientas de auditoría implementadas debe ser restringido. Deben de encontrar en ambientes distintos al de producción y/o desarrollo.

3.6. Los respaldos de información de las pista de auditoría no debe ser almacenado en lugares públicos.

3.7. Se debe definir una revisión de auditoría a la Oficina de Informática donde se incluya la revisión de sus operaciones, acompañada de una auditoría a la infraestructura de sistemas implementada. Esta revisión deberá realizarse por lo menos una vez al año.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CREACIÓN DE DATOS DE PRUEBA	
	CÓDIGO: NO-012	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CREACIÓN DE DATOS DE PRUEBA

0107 -2008-ED

Ministerio de Educación	**DOCUMENTO:** NORMA DE CREACIÓN DE DATOS DE PRUEBA	
	CÓDIGO: NO-012	**EDICIÓN:** 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CREACIÓN DE DATOS DE PRUEBA	
	CÓDIGO: NO-012	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de existencia de información real y confidencial cuando se utiliza como base información existente en las bases de datos de producción para los ambientes de desarrollo y/o pruebas del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

2.1. El Oficial de Seguridad es responsable de verificar que la información usada en los ambientes de desarrollo y/o pruebas del Ministerio no contenga datos reales de la base de datos de producción.

3. Descripción

3.1. La información utilizada en los ambientes de desarrollo y/o pruebas del Ministerio debe ser simulada no conteniendo información real de la base de datos de producción del Ministerio.

3.2. En los casos que la información utilizada en los ambientes de desarrollo y/o pruebas se base en lo almacenado en las bases de datos de producción, ésta última debe ser alterada de modo que se garantice la confidencialidad de la información real.

3.3. Todos aquellos controles de acceso utilizados en los ambientes de producción, deben de utilizarse también en los ambientes de desarrollo y/o pruebas del Ministerio con la finalidad de tener un ambiente lo más parecido al real.

3.4. Toda copia de información de los ambientes de producción del Ministerio, deben quedar registrados en una bitácora de modo que permita realizar un seguimiento en caso de ser requerido.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE CUMPLIMIENTO DE LA LEGISLACIÓN	
	CÓDIGO: NO-013	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE CUMPLIMIENTO DE LA LEGISLACIÓN

Ministerio de Educación	DOCUMENTO: NORMA DE CUMPLIMIENTO DE LA LEGISLACIÓN	
	CÓDIGO: NO-013	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE CUMPLIMIENTO DE LA LEGISLACIÓN	
	CÓDIGO: NO-013	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el impacto proveniente de la no documentación y/o actualización de los documentos legales, regulatorios y contractuales relacionados a los sistemas de información del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

El Oficial de Seguridad es responsable verificar el cumplimiento de lo dispuesto en la presente norma.

3. Descripción

3.1. Todos los requisitos legales, regulatorios y/o contractuales deben encontrarse obligatoriamente documentados en su totalidad para cada uno de los sistemas de información del Ministerio.

3.2. Se debe de cumplir con todas restricciones legales sobre el uso del material protegido por derecho de propiedad intelectual, como: derechos de autor, derechos de diseño o marcas registradas.

3.3. Se debe incluir todos los requisitos legales, regulatorios y/o contractuales en los contratos firmados entre terceros para desarrollo de software.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE DESARROLLO EXTERNO DE SOFTWARE	
	CÓDIGO: NO-014	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE DESARROLLO EXTERNO SOFTWARE

Ministerio de Educación	DOCUMENTO: NORMA DE DESARROLLO EXTERNO DE SOFTWARE	
	CÓDIGO: NO-014	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE DESARROLLO EXTERNO DE SOFTWARE	
	CÓDIGO: NO-014	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de no tomarse en cuenta aspectos cruciales inherentes de la tercerización de desarrollo de software por parte del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

El Oficial de Seguridad es responsable verificar el cumplimiento de lo dispuesto en la presente norma.

3. Descripción

3.1. Se debe cumplir con toda la legislación relacionada a acuerdos de licencias, derechos de autor, propiedad del código, y cualquier ley, norma o regulación que afecte el desarrollo y funcionamiento del software.

3.2. Es imprescindible la presentación de una certificación de calidad y exactitud del trabajo por parte del ente externo a quien haya sido delegado el desarrollo de software por parte del Ministerio.

3.3. Revisar el código del desarrollo en busca de posibles brechas de seguridad y código malicioso.

3.4. Se debe contar con cláusulas que contractuales que confirmen la calidad del código desarrollado por el ente externo.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE INCLUSIÓN DE REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS	
	CÓDIGO: NO-015	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE INCLUSIÓN DE REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS

Ministerio de Educación	DOCUMENTO: NORMA DE INCLUSIÓN DE REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS	
	CÓDIGO: NO-015	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE INCLUSIÓN DE REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS	
	CÓDIGO: NO-015	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Reducir el riesgo de posibles incidentes de seguridad relacionados con el acceso de terceros a recursos de tratamiento de información de el Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

2.1. El Oficial de Seguridad es responsable de:

- Verificar el cumplimiento de las medidas de protección de información a través de revisiones periódicas.

2.2. La Unidad de Abastecimiento es responsable de:

- Incluir dentro de los contratos que se realicen entre el Ministerio y cualquier organización externa, cláusulas que se refieran a todos los requisitos de seguridad de acuerdo a las Políticas y Normas del Ministerio.

3. Descripción

3.1. La adopción de una norma de inclusión de requisitos de seguridad en contratos con terceros, reduce el riesgo de posibles incidentes de seguridad con el acceso de terceros a recursos de tratamiento de información del Ministerio.

3.2. Todo acceso a terceros a los recursos de red del Ministerio, debe cumplir con la norma NO-007 – Norma de Control de Acceso a los Recursos de Información.

DE LA PROTECCION DE LA INFORMACIÓN

3.3. La Oficina General de Administración, a través de su Unidad de Abastecimiento, es la encargada de incluir dentro de todos los contratos con terceros, que vayan a tener acceso a recursos de información del Ministerio, cláusulas que indiquen el cumplimiento por parte de los terceros de todas las políticas y normas de seguridad establecidas por el Ministerio, además de las responsabilidades que asumirán en caso se haga caso omiso a dichas disposiciones.

3.4. La Oficina General de Administración, a través de su Unidad de Abastecimiento, deberá incluir dentro de los contratos con terceros, cláusulas que indiquen las limitaciones de acceso físico de los terceros a los recursos de información, de acuerdo a lo indicado en la NO-008 - Norma de control de acceso al centro de datos.

DE LA AUDITORIA Y REVISION DEL CUMPLIMIENTO DE LA PROTECCION DE LA INFORMACIÓN

3.5. El Oficial de Seguridad deberá realizar trimestralmente una revisión aleatoria de los contratos firmados con terceros para verificar el cumplimiento de la presente norma. Las no conformidades de cumplimiento de la presente norma deben quedar documentadas.

3.6. El Comité Operativo de Seguridad de Información debe analizar todos aquellos casos en donde se encuentre no cumplimiento de la presente norma.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE INTERCAMBIO DE INFORMACIÓN	
	CÓDIGO: NO-016	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE INTERCAMBIO DE INFORMACIÓN

Ministerio de Educación	DOCUMENTO: NORMA DE INTERCAMBIO DE INFORMACIÓN	
	CÓDIGO: NO-016	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE INTERCAMBIO DE INFORMACIÓN	
	CÓDIGO: NO-016	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de exposición de información sensible a través de distintos medios de comunicación de voz, facsímil y video que formen parte de la infraestructura tecnológica del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

El Oficial de Seguridad es responsable verificar el cumplimiento de lo dispuesto en la presente norma.

3. Descripción

3.1. Se deben de tomar las precauciones necesarias para que el personal del Ministerio no revele información sensible vía telefónica debido a que estas líneas pueden estar siendo interceptadas.

3.2. Se deberán definir las responsabilidades de las partes involucradas en el intercambio de información, así como los riesgos asociados a la misma.

3.3. No se deben tener conversaciones confidenciales en lugares públicos.

3.4. Se debe tener especial cuidado con el uso de máquinas de fax y con la información que es almacenada en las bandejas de los mismos una vez recibida una transmisión.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE MONITOREO CONTÍNUO DEL DESEMPEÑO DE LOS SISTEMAS	
	CÓDIGO: NO-017	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE MONITOREO CONTÍNUO DEL DESEMPEÑO DE LOS SISTEMAS

Ministerio de Educación	DOCUMENTO: NORMA DE MONITOREO CONTÍNUO DEL DESEMPEÑO DE LOS SISTEMAS	
	CÓDIGO: NO-017	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE MONITOREO CONTÍNUO DEL DESEMPEÑO DE LOS SISTEMAS	
	CÓDIGO: NO-017	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de fallas en los sistemas de información del Ministerio de Educación, en adelante el Ministerio, mediante el monitoreo de la capacidad de los mismos y su correcto funcionamiento.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

2.1 El Oficial de Seguridad es responsable de:

- Revisar el desempeño del ambiente de procesamiento con el fin de garantizar la disponibilidad y el cumplimiento de los niveles de servicio definidos con los proveedores, según lo indicado por la NO-029 - Norma de Servicios Externos.

2.2 El Custodio de Información es responsable de:

- Establecer los mecanismos que permitan medir y evaluar el desempeño de los sistemas de información.
- Plantear las acciones correctivas a seguir para solucionar los problemas de capacidad que se puedan identificar.
- Presentar mensualmente un informe con los resultados de las labores de monitoreo de desempeño y capacidad de los sistemas de información.

3. Descripción

3.1 El desempeño de una plataforma de tecnología se monitorea generalmente mediante la medición del tiempo que le lleva al sistema realizar tareas y ejecutar programas.

3.2 La medición del uso de la capacidad generalmente incluye la comparación del uso de un recurso con el límite superior que pudiera haber utilizado.

3.3 En los recursos informáticos a monitorear, se deberá incluir a los servidores, sistemas de aplicación, servicios y sistemas de comunicación críticos y cualquier activo de información adicional que la Oficina de Informática considere.

3.4 Adicionalmente a estos monitoreos se deben realizar proyecciones para futuros requerimientos de capacidad con el fin de reducir el riesgo de sobrecarga del sistema. De la misma manera se deben establecer, documentar y probar los requerimientos operativos de nuevos sistemas antes de su aprobación y uso.

3.5 A menudo existe una relación entre la capacidad y el desempeño, dado que a medida que disminuye la capacidad restante disminuyen los niveles de desempeño. Esto por lo general se traduce en una degradación lenta que se agudiza a medida que se aproxima la capacidad máxima.

3.6 Es recomendable que se lleven a cabo revisiones regulares de la utilización de la capacidad del desempeño para asegurarse de que los problemas progresivos de capacidad se manejen antes de que tengan un efecto material en el desempeño.

3.7 Un mal desempeño se puede deber a una deficiente fragmentación de información o un mal diseño de aplicación. Cuando el desempeño sea deficiente y aparentemente la capacidad no sea la causa, se deberá investigar otras áreas para establecer el origen del problema.

3.8 Sin un adecuado monitoreo de la capacidad y el desempeño, los problemas podrían no ser fácilmente corregidos y podrían causar que el sistema falle.

3.9 La solución y rastreo inadecuado de problemas pueden afectar de manera adversa la disponibilidad, integridad y confiabilidad general de los sistemas de información. Esto puede a su vez, afectar la calidad de las decisiones de negocios que dependen de los sistemas de información.

DEL MONITOREO DEL DESEMPEÑO

3.10 El Custodio de Información deberá monitorear el desempeño de los sistemas con el fin de garantizar un diagnóstico oportuno de los problemas potenciales que afectan los niveles de servicio.

3.11 El monitoreo del desempeño debe incluir por lo menos la revisión de las siguientes variables dentro de la plataforma tecnológica del Ministerio:

- La capacidad utilizada del disco.
- Disponibilidad y tráfico de red.
- Utilización del procesador.
- Utilización de memoria.
- Conexiones simultáneas a un sistema.
- Velocidad de respuesta del servicio (performance del servicio).

3.12 Debe considerarse para un monitoreo efectivo lo siguiente:

- Técnicas para identificar problemas.
- Definición de las tendencias y estadísticas de problemas.
- Evaluación del impacto comercial de los problemas.
- Directrices para enfocarse en la corrección de las causas y no en solucionar parcialmente basándose en las consecuencias del problema.
- Análisis e implantación de soluciones.

3.13 El Custodio de Información deberá preparar un informe mensual donde se presente la evolución histórica de cada una de estás variables, así como la resolución y seguimiento realizado sobre cualquier incidente que se haya presentado.

3.14 Se debe contar con distintos mecanismos que permitan verificar que los recursos tecnológicos provistos por el Ministerio a sus usuarios, se encuentran siendo utilizados para los fines adecuados.

DE LA PLANEACIÓN DE LA CAPACIDAD

3.15 El Custodio de Información deberá monitorear demandas de capacidad y realizar proyecciones de sus futuros requerimientos, a fin de garantizar la disponibilidad del procesamiento. Estas proyecciones deben tomar en cuenta los nuevos requerimientos del negocios y sistemas, además de las tendencias actuales y/o proyectadas en el procesamiento de información del Ministerio.

3.16 El Custodio de Información debe utilizar esta información para identificar y evitar potenciales cuellos de botella que podrían plantear una amenaza a la seguridad del sistema o a los servicios del usuario, y planificar una adecuada acción correctiva.

3.17 El Custodio de Información deberá incluir en el informe mensual los requerimientos de expansión de capacidad que sean requeridos en función de las actividades de planeación de la capacidad realizadas.

DE LA AUDITORÍA Y REVISIÓN DEL MONITOREO DE DESEMPEÑO Y CAPACIDAD

3.18 El Oficial de Seguridad deberá revisar los informes mensuales de desempeño elaborados por el Custodio de Información verificando que el desempeño y la capacidad de la plataforma de tecnología esté dentro de los parámetros adecuados.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE REGISTRO DE INCIDENCIAS EN LAS OPERACIONES	
	CÓDIGO: NO-018	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE REGISTRO DE INCIDENCIAS EN LAS OPERACIONES

Ministerio de Educación	DOCUMENTO: NORMA DE REGISTRO DE INCIDENCIAS EN LAS OPERACIONES	
	CÓDIGO: NO-018	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE REGISTRO DE INCIDENCIAS EN LAS OPERACIONES	
	CÓDIGO: NO-018	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Administrar y dar solución de manera efectiva a los incidentes de operaciones asociados a temas de tecnología de información informados por personal del Ministerio de Educación, en adelante el Ministerio.

2. Definición de términos

2.1. **Incidente de Operación**: Es un evento que puede comprometer de alguna manera el funcionamiento correcto y continuo de la infraestructura tecnológica del Ministerio.

3. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

3.1. El Oficial de Seguridad es responsable de:

- Solicitar los informes de desempeño de las actividades de Operaciones para su revisión y contrastarlos con la bitácora de Operaciones disponible.
- Revisar los informes de cada una de las incidencias presentadas.

3.2. El Encargado de Operaciones es responsable de:

- Registrar las solicitudes y los incidentes de operaciones que se presenten en la bitácora de Operaciones.
- Preparar un informe sobre el desempeño de las labores de Operaciones del Ministerio.

3.3. El Usuario de Información es responsable de:

- Advertir, registrar y comunicar al Encargado de Operaciones de cualquier incidente de operación que se presente.

4. Descripción

4.1. Se debe de informar al encargado de Operaciones de cualquier incidente que se haya presentado o que pueda causar una posible interrupción o falla a cualquier punto de la infraestructura tecnológica del Ministerio.

4.2. Se debe informar a todos los empleados acerca de los medios por los cuales se pueden informar las distintas incidencias que ocurriesen y puedan tener un impacto en la continuidad de las operaciones del Ministerio.

4.3. Para atender debidamente los incidentes se debe contar con procedimientos que especifiquen las actividades a desarrollar para corregir las fallas y asegurar la disponibilidad e integridad de todos aquellos equipos y demás que formen la Infraestructura Tecnológica del Ministerio.

4.4. En caso las labores de Operaciones sean realizadas por contratistas externos se deberá asegurar que existan acuerdos de niveles de servicio que garanticen un desempeño eficaz y eficiente de su parte.

DEL USO DE LA BITÁCORA DE OPERACIONES

4.5. Todas las comunicaciones cursadas al Encargado de Operaciones deberán ser documentadas para asegurar el adecuado seguimiento de las mismas hasta su resolución. Esta documentación también permitirá la eventual identificación de problemas recurrentes que pudieran estarse presentando.

4.6. La bitácora de Operaciones deberá contener información suficiente para asegurar el adecuado seguimiento de cada registro (informante, fecha de registro, problema informado, causa del problema, solución identificada, fecha solución y estado del problema, etc.).

4.7. La bitácora de Operaciones debe ser incluida dentro de la estrategia de Respaldos de Información con la finalidad de asegurar la disponibilidad de información en caso ocurriese un desastre.

4.8. Todas aquellas aplicaciones o dispositivos que conformen la plataforma tecnológica del Ministerio, que se encuentren configurados para generar un listado de eventos de auditoria, también deben ser incluidos dentro de la estrategia de Respaldos de Información.

DE LA REVISIÓN Y AUDITORÍA

4.9. El Oficial de Seguridad debe revisar periódicamente los informes de desempeño elaborados por el Encargado de Operaciones para verificar que las labores de seguimiento de las solicitudes se estén realizando oportunamente.

4.10. El Oficial de Seguridad debe revisar los informes de cada incidente que haya sido categorizado como incidente de seguridad para verificar que labores de seguimiento y medidas correctivas fueron implantadas.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE REGISTRO DE OPERACIONES	
	CÓDIGO: NO-019	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE REGISTRO DE OPERACIONES

Ministerio de Educación	DOCUMENTO: NORMA DE REGISTRO DE OPERACIONES	
	CÓDIGO: NO-019	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE REGISTRO DE OPERACIONES	
	CÓDIGO: NO-019	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de no registrar las labores de los Operadores del Centro de Datos del Ministerio de educación, en adelante el Ministerio.

2. Disposiciones Generales

El Oficial de Seguridad es responsable de verificar el cumplimiento del registro de las operaciones de los operadores del Centro de Datos.

3. Descripción

DE LA REGLAMENTACIÓN

3.1 Todas las labores, sin excepción, que realicen los operadores del Centro de Datos durante su jornada laboral debe quedar registrada en una Bitácora de Operaciones.

3.2 La Bitácora de Operaciones deberá ser entregada por el operador del Centro de Datos al jefe de la Oficina de Informática al final de su jornada de trabajo.

DE LA AUDITORÍA Y REVISIÓN

3.3 El Oficial de Seguridad será el encargado de verificar el cumplimiento de la presente norma.

3.4 El Comité de Sistemas de Información debe proponer revisiones periódicas a las Bitácoras de Operaciones.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE RESPALDO DE INFORMACIÓN	
	CÓDIGO: NO-020	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE RESPALDO DE INFORMACIÓN

Ministerio de Educación	DOCUMENTO: NORMA DE RESPALDO DE INFORMACIÓN	
	CÓDIGO: NO-020	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE RESPALDO DE INFORMACIÓN	
	CÓDIGO: NO-020	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de no poder asegurar la recuperación de información tras un desastre o falla de los medios que mantienen la información del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

3.1 El Custodio de Información es responsable de:

- Administrar la ejecución, prueba y adecuado almacenamiento de los respaldos de información.

3.2 El Oficial de Seguridad es responsable de:

- Verificar el cumplimiento del plan de respaldo de información definido por parte del Custodio de Información.

3. Descripción

DE LA REGLAMENTACIÓN

3.1 Todos los directorios de datos de los usuarios, programas, archivos de configuración y administración del sistema operativo de los servidores deberán ser respaldados.

3.2 Antes y después de poner en operación un nuevo servidor o en cada nueva versión de alguna aplicación o sistema operativo, es necesario realizar un respaldo completo.

3.3 La información generada en los sistemas y la información almacenada en los servidores de archivos centrales deberán ser respaldadas en medios de almacenamiento externos de manera diaria.

3.4 Los medios de respaldo deberán ser debidamente etiquetados y almacenados de manera segura tanto dentro como fuera del Ministerio.

3.5 Deben mantenerse dos juegos de los respaldos, uno dentro del Ministerio para recuperación de desastres menores y otro fuera del Ministerio para escenarios de desastres mayores.

3.6 El proveedor de almacenamiento externo, debe cumplir con los estándares ambientales recomendados por el fabricante para la conservación de los medios de almacenamiento externos. Así mismo, debe contar con medidas de seguridad estrictas en cuanto al acceso al lugar de custodia de los medios de almacenamiento externos.

DEL RESPALDO DE LOS SISTEMAS DE INFORMACIÓN PARA RECUPERACIÓN DE DESASTRES

3.7 Ante la puesta en producción de un nuevo sistema o una nueva versión del mismo se deberá realizar un respaldo completo de la información. Esto dará una imagen inicial de todos los sistemas y servidores como un punto de partida para el proceso periódico de respaldo de información.

3.8 Se debe efectuar respaldos diarios completos. Dicho respaldo deberá incluir los datos de usuarios, librerías y configuraciones en general.

3.9 Una vez que se cumpla una semana de respaldar información se deberá realizar nuevamente un respaldo total, que incluya todos los elementos del sistema (sistema operativo, actualizaciones, librerías, base de datos, información de usuarios, etc.), y se deberá seguir con la rutina antes descrita. Una copia de este respaldo deberá almacenarse fuera del Ministerio en un ambiente seguro y controlado.

3.10 Se deberá contar adicionalmente con cintas disponibles para los casos en que un respaldo de información ocupe más de una cinta, o esta presente fallas.

DEL RESPALDO DE LOS SISTEMAS DE INFORMACIÓN

3.11 Todos los sistemas en producción del Ministerio deben tener como parte de su diseño un esquema de respaldo de información histórica, en el cual se defina la frecuencia de respaldo, información a almacenar, información histórica a conservar, plan de destrucción de información y plan de pruebas de respaldo.

3.12 La información histórica debe ser información sensible a auditorias internas o externas y debe ser mantenida por al menos un periodo de cinco (5) años.

3.13 Una copia de los respaldos históricos al igual que los respaldos de recuperación de desastres, deben ser almacenados fuera de las instalaciones del Ministerio

DE LA RESPUESTA A FALLAS DEL RESPALDO

3.14 Si un respaldo falla, éste deberá ser re-ejecutado siempre y cuando la tarea de respaldo no interfiera con las operaciones del negocio.

DE LAS PRUEBAS A LAS CINTAS DE RESPALDO

3.15 Las pruebas periódicas de las cintas de respaldo son esenciales para asegurar que las copias de seguridad se encuentren disponibles y puedan ser utilizadas en cualquier momento.

3.16 Se debe seleccionar un respaldo cada dos meses para la pruebas de recuperación de las cintas.

3.17 Se deberá documentar todas las pruebas de respaldo realizadas, incluyendo los atributos y resultados de la misma.

3.18 De detectarse algún problema durante las pruebas, se deberán tomar acciones para aislar y responder a dicho problema.

DEL RESPALDO DE LA INFORMACIÓN DE USUARIOS

3.19 Se deberá crear un espacio para los datos de cada área del Ministerio dentro de los servidores de la red local; estableciendo límites de capacidad para su almacenamiento en función de las necesidades de cada área y del espacio disponible en el servidor.

DE LA SEGURIDAD FÍSICA DE LOS MEDIOS DE ALMACENAMIENTO

3.20 Los ambientes donde se depositan los medios de almacenamiento de la información contarán con adecuadas condiciones de temperatura, humedad, entre otras. Estos ambientes dispondrán de medidas de seguridad complementarias, como por ejemplo, cámaras de vídeo, puertas con dispositivos de acceso, de acuerdo a la disponibilidad presupuestal del Ministerio.

3.21 Los ambientes donde se encuentran los medios de almacenamiento serán de acceso restringido, sólo estará autorizado el ingreso al personal responsable de la Seguridad de la Información.

DE LA AUDITORÍA Y REVISIÓN DE LOS PROCESOS DE RESPALDO

3.22 El Oficial de Seguridad será el encargado de auditar el cumplimiento de la presente norma.

3.23 Se deberá coordinar con el Custodio de Información la realización de pruebas periódicas a las cintas de respaldo de manera aleatoria e independientemente de las pruebas programadas y descritas en la presente norma.

3.24 Se realizarán revisiones periódicas de los registros de los sistemas de respaldo con el motivo de asegurar que los procesos de copias de seguridad se realicen como han sido programados y que culminen correctamente.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD DE LAS APLICACIONES DEL SISTEMA	
	CÓDIGO: NO-021	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SEGURIDAD DE LAS APLICACIONES DEL SISTEMA

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD DE LAS APLICACIONES DEL SISTEMA	
	CÓDIGO: NO-021	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD DE LAS APLICACIONES DEL SISTEMA	
	CÓDIGO: NO-021	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo de no tomar en cuenta aspectos cruciales inherentes de la tercerización de desarrollo de software por parte del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

El Oficial de Seguridad es el encargado de verificar el cumplimiento de esta norma. Así mismo deberá de realizar revisiones a todos los sistemas de aplicación del Ministerio.

3. Descripción

3.1. Se deben validar los datos de entrada a los sistemas de información mediante la implementación de controles, que permitan validar entradas duplicadas, caracteres inválidos, datos fuera de rango, datos incompletos, entre otros.

3.2. Se debe tener procedimientos que permitan actuar ante los errores de validación que se presenten. Así mismo los procedimientos deben incluir la comprobación de la integridad de los datos de entrada.

3.3. Se deberá tener la relación del personal involucrado en todo el proceso de ingreso de datos. La relación de personal debe incluir sus respectivas responsabilidades en el proceso.

3.4. Se deberá implementar planes de prueba periódicos, los cuales incluyan pruebas de conectividad, pruebas paralelas con el fin de garantizar la integridad de datos y comprobar que los programas de las aplicaciones se ejecutan en el momento adecuado.

3.5. El desarrollo de los sistemas de aplicación debe contemplar que tras la ocurrencia de un error, el funcionamiento del aplicativo no se vea alterado así como tampoco la información procesada.

3.6. Todos los sistemas de aplicación deben contar con controles de verificación, por ejemplo la verificación tras la ejecución de una transacción o de algún proceso en lote, cálculos generados manual y/o automáticamente, entre otros.

3.7. Se debe considerar el implementar técnicas de autenticación de mensajes con la finalidad de verificar que el mensaje transmitido entre aplicaciones, estaciones o cualquier dispositivo que forme parte de la infraestructura tecnológica del Ministerio, no haya sido alterado en el camino. La autenticación de mensajes puede darse a través del uso de hardware y/o software.

3.8. Los datos de salida de los sistemas de aplicación deben de ser validados con la finalidad de brindar confianza en los mismos. Se recomienda que también se incluya información visual suficiente con la finalidad de poder determinar la exactitud del resultado.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS	
	CÓDIGO: NO-022	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS	
	CÓDIGO: NO-022	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS	
	CÓDIGO: NO-022	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Definir las medidas de uso y resguardo que debe tener un usuario del Ministerio de Ecuación, en adelante el Ministerio, con respecto a los recursos tecnológicos que le son asignados para el desarrollo de su trabajo.

2. Definición de términos

2.1. **Software base:** El software base o software de sistemas puede definirse como programas de cómputo y/o rutinas relacionadas que manejan y apoyan el procesamiento de sistemas de aplicación y hardware de cómputo. Esto incluye el sistema operativo, así como compiladores, sistemas de manejo de cinta y el software que se requiere para monitorear y sintonizar el sistema operativo.

2.2. **Licencia de Software:** Autorización o permiso concedido por el titular del derecho de autor, en cualquier forma contractual, al usuario de un programa informático, para utilizar éste en una forma determinada y de conformidad con unas condiciones convenidas.

3. Disposiciones generales

Se tienen definidas las siguientes responsabilidades:

3.1. El Oficial de Seguridad es responsable de:

- Aprobar el estándar de software antivirus a utilizar por el Ministerio y velar por la adecuada administración y actualización del mismo.
- Revisar los reportes de inventarios de software de los servidores y las estaciones de trabajo en conjunto con el Custodio de Información.

3.2. El Custodio de Información es responsable de:

- Asegurar que el software instalado en los servidores este de acuerdo a las licencias adquiridas por el Ministerio.
- Elaborar los reportes de inventarios de software de los servidores.

3.3. El Encargado de Soporte Técnico (HelpDesk) es responsable de:

- Asegurar que el software instalado en las estaciones de trabajo este de acuerdo a las licencias adquiridas por el Ministerio.
- Elaborar los reportes de inventarios de software de los estaciones de trabajo.

3.4. Los usuarios son responsables de:

- Transferir de manera periódica la información crítica para sus labores a las carpetas designadas por el Encargado de Soporte Técnico (Help Desk), en los equipos de procesamiento centralizados.

4. Descripción

4.1. A fin de garantizar el correcto funcionamiento de los equipos, el Oficial de Seguridad debe asegurarse que el área de Sistemas de Información cuente con un plan de mantenimiento preventivo/correctivo de la infraestructura tecnológica del Ministerio, así como los mecanismos de seguridad más adecuados para su protección.

4.2. La Oficina de Informática debe proveer los mecanismos adecuados para que se respeten permanentemente las instrucciones del fabricante, por ejemplo: protección por exposición a campos electromagnéticos fuertes, uso de corriente estabilizada y otros.

4.3. Los equipos informáticos son entregados por el Ministerio para que su personal pueda cumplir las labores que se le ha encomendado.

4.4. Los equipos informáticos no serán utilizados para desarrollar labores personales de los usuarios, ni de terceros bajo ninguna circunstancia.

4.5. Es deber de todos los usuarios velar por el buen uso y cuidado de los equipos entregados por el Ministerio.

4.6. Todos los usuarios son responsables por la información que es almacenada en los equipos que se les han asignado. Es responsabilidad de los usuarios alertar al Oficial de Seguridad de cualquier riesgo potencial a los que puedan estar expuestos tanto los equipos como la información.

4.7. Los accidentes ocasionados a los equipos entregados por el Ministerio causados por descuidos del personal serán responsabilidad del usuario al que se asignó el equipo.

4.8. El personal deberá informar a:

- Encargado de Soporte Técnico (Help Desk) por cualquier daño que pudiera haberse producido sobre el equipo.
- Personal de seguridad y vigilancia en caso de robo.

4.9. Los usuarios son responsables de reportar cualquier acto que atente contra los equipos del Ministerio o cualquier acto sospechoso.

4.10. Por ningún motivo se prestará a terceros el computador personal, computador portátil, etc. que contenga información confidencial.

4.11. Los usuarios no están autorizados a transportar equipos asignados por el Ministerio, salvo sean estos equipos portátiles. En caso que un equipo portátil sea requerido, se necesitará una autorización por escrito del área usuaria.

4.12. Los equipos deberán ser ubicados en áreas que permitan proveer la seguridad que requiera el equipo en base a la confidencialidad de la información almacenada.

4.13. Todos los equipos informáticos que forman parte de la infraestructura tecnológica del Ministerio, y que deban ser ubicados fuera de las instalaciones del Ministerio, deben cumplir con lo dispuesto en la presente norma.

4.14. En caso que el usuario tenga asignado un equipo portátil este deberá ser resguardado según se indica en la NO-031 – Norma de uso de equipos móviles.

DE LA INFORMACIÓN EN LOS EQUIPOS

4.15. Toda la información almacenada en los equipos entregados, se considera información del Ministerio.

4.16. El Ministerio podrá en cualquier momento hacer revisiones de la información almacenada en los equipos con el objeto de asegurar que los mismos se estén usando en cumplimiento con las funciones para las que fueron asignados.

4.17. Los usuarios no deben modificar la configuración del software base.

4.18. Los usuarios están prohibidos de instalar cualquier tipo de software en los equipos asignados por el Ministerio. El Encargado de Soporte Técnico (Help Desk) es el único autorizado para realizar instalaciones en los equipos del Ministerio.

4.19. El software "freeware" o "shareware" adquirido por correo o por cualquier otro servicio de Internet no es permitido, salvo que sea evaluado por el Encargado de Soporte Técnico (Help Desk) y aprobado por el Oficial de Seguridad.

4.20. El Encargado de Soporte Técnico (Help Desk) es responsable de asignar a todos los usuarios del Ministerio un espacio donde puedan almacenar información a ser respaldada según los mecanismos estándares. La Oficina de Seguridad es responsable de velar por que la información de los usuarios esté incluida en las estrategias de respaldo del Ministerio y que los usuarios estén almacenando la información crítica en los espacios asignados.

4.21. El usuario será responsable de mantener depurado el espacio asignado en el servidor central.

4.22. La información que no sea almacenada en las ubicaciones asignadas por el Encargado de Soporte Técnico (Help Desk) no será incluida en las estrategias de respaldo del Ministerio, en consecuencia es responsabilidad del usuario respaldar esta información.

4.23. Debe evitarse conservar información restringida y/o confidencial en los discos duros de las estaciones de trabajo, la misma deberá conservarse en los equipos de procesamiento centralizados en la medida que la plataforma tecnológica lo soporte. El usuario es responsable por la seguridad que brinda a la información conservada en su estación y, en especial, por la que está expuesta para consulta o acceso de otros usuarios por vía de los recursos compartidos, ya sea que tengan o no contraseñas de acceso.

4.24. Si la información residente en una estación de trabajo está cifrada para evitar la manipulación no autorizada, la llave de encriptación y el material utilizado para la generación de ésta, no deben estar almacenadas en el mismo medio en donde reside la información cifrada.

4.25. La información sensible o confidencial, una vez impresa, debe ser retirada de la impresora inmediatamente.

4.26. Los empleados no deben navegar por las computadoras o redes del Ministerio, a menos que sea una función de su cargo, y que esto tenga un propósito demostrable y justificado.

4.27. El usuario responsable del computador personal debe de bloquear el mismo cuando por causa laboral o extra laboral está en necesidad imperiosa de ausentarse de su lugar de trabajo (Ctrl-Alt-Sup y bloquear sesión). Esto impide tanto el acceso no autorizado al sistema, como a las aplicaciones. El usuario que no deje bloqueado su computador al ausentarse, será responsable por el uso no autorizado del equipo, de la red o de las aplicaciones instaladas.

4.28. Todos los equipos de cómputo deben contar con un protector de pantalla institucional o uno autorizado por el Encargado de Soporte Técnico (Help Desk) y el Oficial de Seguridad que exija el ingreso de una contraseña para permitir utilizar los recursos e información contenida en el equipo.

4.29. Todos los equipos de cómputo deben tener contraseñas de inicio de sesión y contraseña de BIOS. La administración de las contraseñas de BIOS debe encontrarse a cargo del personal de Soporte Técnico.

DE LA ASIGNACIÓN DE LOS EQUIPOS

4.30. El Encargado de Soporte Técnico (Help Desk) en el momento de asignar un equipo a un usuario o cambiar alguna de las partes del equipo asignado, debe registrar un inventario del equipo y partes asignadas, obteniendo la firma del usuario como conformidad de la recepción o la modificación.

DE LA AUDITORÍA Y REVISIÓN DEL USO DE LOS EQUIPOS Y ESTACIONES DE TRABAJO

4.31. El Encargado de Soporte Técnico (Help Desk) deberá:

- Elaborar trimestralmente un inventario total del software instalado en las estaciones de trabajo emitiendo un informe dirigido a la Oficina de Seguridad en el que se indique las estaciones que tienen instalado software no autorizado y de que tipo es éste, dicho informe deberá ser analizado para tomar las medidas que correspondan.

- Verificar aleatoriamente o sobre la base de los registros de auditoría o eventos de seguridad, si el usuario ha modificado la configuración del software base o hardware de su equipo, notificando de este hecho al usuario, a su jefe directo y al Oficial de Seguridad.

4.32. La Oficina de Seguridad deberá incorporar en sus actividades la revisión selectiva del inventario de equipos asignados a usuarios, verificando en forma aleatoria la asignación efectuada y el uso.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN COMERCIO ELECTRÓNICO	
	CÓDIGO: NO-023	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SEGURIDAD EN COMERCIO ELECTRÓNICO

Ministerio de Educación	**DOCUMENTO:** NORMA DE SEGURIDAD EN COMERCIO ELECTRÓNICO	
	CÓDIGO: NO-023	**EDICIÓN:** 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN COMERCIO ELECTRÓNICO	
	CÓDIGO: NO-023	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Asegurar que los riesgos inherentes a transacciones financieras realizadas electrónicamente con otras instituciones sean debidamente mitigados por el Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

1.1 El Oficial de Seguridad es responsable de:

- Verificar el cumplimiento de las medidas de protección a las transacciones electrónicas a través de revisiones periódicas.

3. Descripción

3.1. Todas las transacciones que realice el Ministerio a través de medios electrónicos debe ser controlada y protegida considerando como mínimo los siguientes puntos.

- **Servicios de autenticación de doble factor**: la entidad externa debe proporcionar, para verificar su identidad, dos pruebas de información que validen su identidad.
- **Autorizaciones previas:** la entidad externa deberá contar con la autorización expresa del Ministerio para las actividades de comercio electrónico.
- **Procesos de oferta y contratación:** el Ministerio deberá seleccionar a las entidades con las que realizará comercio electrónico, mediante los mismos términos de evaluación de proyectos, definidos en el procedimiento PR-01-02-01 – Evaluación de proyectos de TI.
- **Servicios de cifrado de la información:** una vez verificada la identidad de la entidad externa, toda la información intercambiada con el Ministerio deberá ser cifrada antes de su transmisión, asegurando que se encuentre protegida desde el punto de inicio de la transmisión hasta el punto destino.
- **Servicios de no repudio:** toda transacción cuyo inicio sea solicitado por otra institución deberá ser realizada a través de un sistema confiable que ratifique que dicha institución ha solicitado la transacción, lo que asegura que la institución externa reconoce su responsabilidad por la transacción.
- **Acuerdo entre las partes:** la entidad y el ministerio deberán cumplir con los acuerdos definidos en la norma NO-029 – Norma de servicios externos, además del acuerdo de confidencialidad a firmar por la entidad, definido en la política PO-001 – Política General de Seguridad de la Información.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107-2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN EL RE-USO O ELIMINACIÓN DE EQUIPOS Y MEDIOS INFORMÁTICOS	
	CÓDIGO: NO-024	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SEGURIDAD EN EL RE-USO O ELIMINACIÓN DE EQUIPOS Y MEDIOS INFORMÁTICOS

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN EL RE-USO O ELIMINACIÓN DE EQUIPOS Y MEDIOS INFORMÁTICOS	
	CÓDIGO: NO-024	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	**DOCUMENTO:** NORMA DE SEGURIDAD EN EL RE-USO O ELIMINACIÓN DE EQUIPOS Y MEDIOS INFORMÁTICOS	
	CÓDIGO: NO-024	**EDICIÓN:** 01
		FECHA APROBACIÓN:

1. Objetivo

Reducir el riesgo de exposición de información si es que no se realiza un adecuado re-uso o eliminación de los equipos y/o medios informáticos de el Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

2.1. El Oficial de Seguridad es responsable de:

- Verificar el cumplimiento de las medidas de eliminación de equipos y medios informáticos.

2.2. Los Usuarios son responsables de:

- Eliminar o re-usar adecuadamente todos aquellos equipos y medios informáticos de acuerdo a lo establecido en la presente norma.

3. Descripción

3.1. La adopción de una norma de seguridad en el re-uso y eliminación de equipos y medios informáticos, reduce el riesgo de exposición de información del Ministerio a personas no autorizadas.

3.2. Todo equipo y medio informático que contenga información clasificada como "Confidencial" o de "Privada" y vaya a ser reutilizado, debe haber sido previamente borrado por algún medio magnético con la finalidad de evitar una posible recuperación no autorizada de la información. Los equipos y medios informáticos que contengan información clasificada como "pública" pueden ser sometidos a eliminación física de la información antes de ser re-usados.

3.3. La clasificación de información se estipula en la NO-003 - Norma de Clasificación y Manejo de la Información.

3.4. Los discos flexibles defectuosos o dañados que contengan información clasificada como "Confidencial", deben destruirse usando tijeras u otros métodos autorizados por el Área de Infraestructura Tecnológica.

3.5. Todo re-uso o eliminación de equipos y medios informáticos que contenga información clasificada como "confidencial" debe quedar registrado en una bitácora que será llevada por el Área de Infraestructura Tecnológica.

3.6. La bitácora de eliminación o re-uso de equipos y medios informáticos debe indicar la información que ha sido eliminada, el medio afectado, persona que realizó la labor, fecha y hora de la eliminación como mínimo.

3.7. Todas copias en papel que contengan información clasificada como "confidencial" se debe desechar mediante máquinas trituradoras autorizadas para tal fin.

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN EL RE-USO O ELIMINACIÓN DE EQUIPOS Y MEDIOS INFORMÁTICOS	
	CÓDIGO: NO-024	EDICIÓN: 01
		FECHA APROBACIÓN:

DE LA AUDITORIA Y REVISION DEL CUMPLIMIENTO DE LA PRESENTE NORMA

3.8. El Oficial de Seguridad deberá realizar mensualmente una revisión a la bitácora de re-uso y eliminación de equipos y medios informáticos para verificar su correcto uso. El no cumplimiento de esta norma debe quedar documentado.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN LA RED	
	CÓDIGO: NO-025	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SEGURIDAD EN LA RED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN LA RED	
	CÓDIGO: NO-025	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN LA RED	
	CÓDIGO: NO-025	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar el riesgo del uso no apropiado de la red, servicios y recursos de red del Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

El Oficial de Seguridad es responsable verificar el cumplimiento de lo dispuesto en la presente norma.

3. Descripción

3.1. Se deben implementar controles de acceso para todos los servicios de red que conformen la infraestructura tecnológica del Ministerio.

3.2. Todos los usuarios de la red del Ministerio deben contar con accesos únicamente a los servicios para los que fueron autorizados de alguna forma específica.

3.3. La gestión de accesos a la red, se debe dar de acuerdo a especificado en el PR-04-01-01 - Procedimiento de Creación y/o Modificación de Accesos y en el PR-04-01-02 - Procedimiento de Eliminación de Accesos.

3.4. Se debe limitar el acceso hacia la red por parte de los usuarios. Se deben implementar mecanismos como: dominios lógicos separados, implementación de VLANs, evitar recorridos cíclicos ilimitados en la red, puertas de enlace predeterminadas, entre otros. Así mismo se deberían implantar mecanismos de detección de intentos de intrusión tanto desde la red interna como externa.

3.5. Todo dispositivo que se conecte a la red del Ministerio debe de tener un identificador único con la finalidad de poder identificar los recursos accesados desde él. Se debe contar con controles en los terminales de modo que no se pueda alterar el identificar único por personal no autorizado. Estos controles deben ser implementados para que operen tanto para conexiones internas o externas.

3.6. Se debe de segmentar la red con la finalidad de limitar el acceso a los recursos de la red por parte de los usuarios. Una correcta segmentación permitirá reducir el riesgo de posibles intentos de intrusión hacia los servicios más importantes del Ministerio.

3.7. Se debe tener una descripción detallada de aquellos servicios de red que no pertenecen al Ministerio pero que son usados por el mismo como parte de su infraestructura tecnológica.

3.8. La conexión entre terminales y servidores debe de realizarse a través de una conexión segura con la finalidad de evitar que la información pueda ser alterada o vista por usuarios no autorizados. La información no segura que puede viajar a través de la red debe ser la mínima necesaria para realizar la conexión segura.

3.9. Todos los usuarios que necesiten tener acceso a la red, deben contar con un identificador único. El identificador único no puede ni debe dar a conocer información relacionada a cargos, ubicación o demás datos que podrían dar a conocer datos confidenciales a usuarios no autorizados.

3.10. En caso de existir sistemas de aplicación o software comprado que tenga herramientas que puedan servir para evadir los controles implementados en la red, se debe de restringir su uso. En caso de ser requeridas para funciones propias del negocio, éstas deben contar con autorización de la Oficina de Informática.

3.11. Se debe establecer un umbral de tiempo tras el cual, un equipo desatendido, debe de bloquearse con la finalidad que evitar que éste sea usado por otro usuario. Además se deberá establecer un umbral máximo de conexión para los usuarios, de acuerdo a la criticidad y demanda del servidor.

3.12. Se debe de restringir el horario habilitado para aceptar nuevas conexiones de usuarios a la red, por ejemplo: únicamente durante horario de oficina.

3.13. Todo sistema de aplicación y/o recurso de red que sea considerado sensible debe, de preferencia, ser aislado de la red con la finalidad de restringir su acceso únicamente a los usuarios autorizados. Las aplicaciones sensibles requieren de autorizaciones respectivas para el ingreso al sistema y manipulación de información. Así mismo, el propietario de la información y la sensibilidad de la misma debe quedar documentado.

3.14. Los servidores críticos no deberían incluir ningún tipo de descripción a modo de banner al establecerse la conexión. Además, se deberá restringir el uso de mensajes de error que puedan brindar información sobre la descripción y características del equipo.

3.15. Los servidores deberán limitar la cantidad consecutiva de intentos errados de conexión, además de llevar internamente en el sistema un registro de dichos eventos.

3.16. Se deberá configurar internamente en los servidores críticos el registro de pistas de auditoría de eventos correspondientes a:

- Accesos exitosos.
- Intentos de conexión fallidos.
- Operaciones críticas.
- Revisión de pistas de auditoría.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN LOS SISTEMAS OFIMÁTICOS	
	CÓDIGO: NO-026	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SEGURIDAD EN LOS SISTEMAS OFIMÁTICOS

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN LOS SISTEMAS OFIMÁTICOS	
	CÓDIGO: NO-026	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN LOS SISTEMAS OFIMÁTICOS	
	CÓDIGO: NO-026	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar los riesgos asociados al uso sistemas ofimáticos existentes dentro de la plataforma tecnológica del Ministerio de Educación, en adelante el Ministerio.

2. Definición de términos

2.1. **Sistema Ofimático:** Sistema de información que proporciona la oportunidad de difundir y compartir más rápido la información del negocio usando una combinación de documentos, estaciones de trabajo, computadores portátiles y comunicaciones móviles, correos escritos y de voz, comunicaciones de voz en general, multimedia, servicios y recursos postales y máquinas de fax, entre otros.

3. Disposiciones Generales

El Oficial de Seguridad es responsable verificar el cumplimiento de lo dispuesto en la presente norma.

4. Descripción

4.1. Toda información transmitida o almacenada en algún sistema ofimático debe encontrarse clasificada de acuerdo a lo especificado en la NO-003 - Norma de Clasificación y Manejo de la Información.

4.2. Si se utilizan equipos tipo fax o impresoras de documentos, éstos deben ser monitoreados de modo que personal ajeno no tenga acceso a ellos sin ser autorizado. Así mismo todo documento debe ser retirado de los faxes o impresoras una vez terminada la impresión de los mismos.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD FÍSICA Y AMBIENTAL DEL CENTRO DE DATOS	
	CÓDIGO: NO-027	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SEGURIDAD FÍSICA Y AMBIENTAL DEL CENTRO DE DATOS

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD FÍSICA Y AMBIENTAL DEL CENTRO DE DATOS	
	CÓDIGO: NO-027	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD FÍSICA Y AMBIENTAL DEL CENTRO DE DATOS	
	CÓDIGO: NO-027	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Normar las condiciones físicas y ambientales que debe tener el ambiente del Centro de Datos, en el que se encuentren los equipos que conforman la plataforma de tecnología del Ministerio de Educación, en adelante el Ministerio, con el fin de asegurar la disponibilidad, confidencialidad e integridad de la información almacenada en ellos.

2. Definición de términos

2.1. **Centro de datos:** Ambiente físico donde se encuentran los servidores de producción y equipos principales de la compañía que están bajo la supervisión del Custodio de Información.

3. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

3.1. El Oficial de Seguridad es responsable de:

- Brindar la asesoría y apoyo necesario para mantener niveles aceptables de seguridad ambiental y control de estos ambientes.
- Verificar periódicamente que se realice un monitoreo de la temperatura y la humedad relativa del ambiente del Centro de Datos, y que los mismos queden documentados.

3.2. El Custodio de Información es responsable de:

- Verificar rutinariamente el adecuado funcionamiento de los sensores ambientales, las instalaciones eléctricas y el sistema de detección/supresión de incendio instalado en el Centro de Datos.

3.3. Todos los equipos que se encuentren dentro del Centro de Datos del Ministerio deben formar parte de un plan de mantenimiento que asegure su correcto funcionar, asegurando así la disponibilidad del mismo y detectar posibles fallas en los mismos.

4. Descripción

DE LA SEGURIDAD FÍSICA EN EL CENTRO DE DATOS

4.1. El perímetro de seguridad debería estar claramente definido.

4.2. Las puertas de acceso al Centro de Datos debe ser de material resistente al fuego, sabotaje e intentos de ingreso a la fuerza.

4.3. Se deben tener implementados mecanismos que restrinjan el acceso al Centro de Datos tales como dispositivos biométricos, tarjetas de proximidad u otros. El acceso debe ser otorgado únicamente al personal mínimo necesario y debe ser de conocimiento del Área de Infraestructura Tecnológica.

4.4. Todas las puertas para incendios del perímetro de seguridad deberían tener alarma y cierre automático.

4.5. Se debería instalar un área de recepción manual, un área de carga y descarga de equipos u otros medios de control del acceso físico al edificio o lugar. Dicho acceso se debería restringir sólo al personal autorizado.

4.6. Los recursos críticos, tales como servidores, dispositivos de almacenamiento, entre otros, deben encontrarse aislados. Así mismo el acceso a la sala donde se encuentren debe requerir algún dispositivo de control de acceso.

4.7. En caso alguna persona ajena al Ministerio deba acceder al Centro de Datos, durante toda su visita, ésta debe encontrarse acompañada por alguna persona del Área de Infraestructura Tecnológica.

DE LOS CONTROLES AMBIENTALES EN EL CENTRO DE DATOS

4.8. Los recursos de tratamiento y comunicaciones se encuentran en el Centro de Datos, el cual deberá contar con medidas de seguridad establecidas y definidas como Clave de acceso, servicio de alimentación de energía ininterrumpida, flujo de alimentación estabilizada, sistema de refrigeración, así como el ingreso solo a personal autorizado.

4.9. Se deben mantener las medidas de higiene y condiciones ambientales básicas para evitar que se produzcan hechos que afecten el ambiente donde residen los recursos informáticos.

4.10. Dichas medidas deben comprender, entre otras cosas: efectuar la limpieza habitual controlada, disponer la remoción inmediata de materiales que no se utilicen, evitar la concentración de elementos inflamables innecesarios, implementar un piso adecuado y mantener una temperatura de ambiente y humedad de acuerdo a los requerimientos específicos del equipamiento.

4.11. Los materiales inflamables deben ser almacenados en lugares seguros a una distancia prudencial del Centro de Datos. Los suministros a granel, como los útiles de escritorio y cintas, no deben ser almacenados en el Centro de Datos hasta que sean requeridos.

4.12. No ubicar dentro del Centro de Datos, los recursos de uso habitual por parte del personal (como son impresoras, fotocopiadoras, máquinas de fax y/o suministros adicionales). En el caso de impresoras solo se permitirán para cumplir las tareas de impresión de reportes de los lotes procesados en el Centro de Datos. En el caso de grabadoras de CD solo se permitirán para cumplir las tareas de remisión de archivos actualizadores a provincia.

4.13. El Centro de Datos deberá contar con mecanismos contra incendios e inundaciones.

4.14. Se debe procurar que el Centro de Datos cuente con un sistema automático de detección y supresión de incendios del tipo FM-200 (Waterless Fire Protection System), de tal manera que esta labor no quede supeditada a un recurso humano. En caso no se pueda costear un sistema de este tipo se debe contar con detectores de humo y extintores suficientes para aplacar un incendio.

4.15. El Centro de Datos debe contar con un termómetro y medidor de humedad que permitan mantener control ambiental dentro de los límites recomendados por el fabricante.

4.16. Los conductos usados para calefacción, ventilación, aire acondicionado y otros deben ser a prueba de fuego.

4.17. Todos los equipos de control de condiciones ambientales deben estar protegidos contra la manipulación indebida.

DE LAS INSTALACIONES ELÉCTRICAS EN EL CENTRO DE DATOS

4.18. EL Centro de Datos debe contar con una instalación eléctrica segura, independiente y de uso exclusivo; ésta debe ser revisada periódicamente por personal calificado. Los accesos a los paneles de control de las instalaciones eléctricas deben estar adecuadamente restringidos. El centro de datos además debería contar con mecanismos de recuperación en caso se tengan caídas de fluido eléctrico, tales como: utilización de baterías, utilización de equipos UPS, utilización de grupos electrógenos; así como la correcta configuración de los mismos para que se activen de manera automática.

4.19. El Centro de Datos tendrá que contar con unidades de suministro continuo de energía, estabilizadores y de ser posible, grupos electrógenos fijos y/o móviles.

4.20. Los equipos de suministro ininterrumpido de energía (UPS) u otros implementos de respaldo de energía deben ser inspeccionados periódicamente para asegurar que soportan la capacidad requerida y se deben probar de conformidad con las recomendaciones del fabricante o proveedor. Se debe tener contratos de mantenimiento preventivo y reactivo con niveles de servicio adecuados.

4.21. El cableado de transmisión de datos se deben encontrar canalizados y estructurados de acuerdo a los estándares y normas de cableado actuales.

4.22. El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño. Se debe tener en cuenta los siguientes controles:

- Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones del Centro de Datos deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa.
- El cableado de red debe estar protegido contra interceptación no autorizada o daño, por ejemplo mediante el uso de conductos o evitando, en la medida de lo posible, trayectos que atraviesen áreas públicas.
- Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.
- Inspeccionar en forma periódica el cableado, así como las cajas de conexión y los paneles de distribución de electricidad, los cuales deben estar bajo llave.

4.23. Se debe procurar contar con al menos un botón de pánico (EPO – Emergency Power Off) que, en caso de emergencia, corte el suministro de energía de toda la sala de equipos que debería estar ubicado en la entrada principal. Este botón debe estar protegido de una activación casual.

4.24. Todos los equipos deben tener adecuadas conexiones a tierra, estas conexiones deben verificarse periódicamente.

4.25. El Centro de Datos debe contar con instrumentos de supervisión de las variables eléctricas, como son amperímetros, voltímetros, etc.

4.26. Todas las conexiones eléctricas de los equipos deben estar de acuerdo a las especificaciones de sus respectivos fabricantes.

DE LA AUDITORÍA Y REVISIÓN DE LOS CONTROLES AMBIENTALES

4.27. El Oficial de Seguridad deberá:

- Revisar semanalmente los informes de monitoreo de condiciones ambientales preparados por el Custodio de Información.

4.28. El Custodio de Información deberá:

- Velar por el adecuado funcionamiento y el monitoreo de las condiciones ambientales del Centro de Datos.
- Registrar diariamente las condiciones ambientales del Centro de Datos.

4.29. El Órgano de Control Institucional deberá:

- Incluir dentro de su plan anual una revisión completa de los controles del Centro de Datos, con el fin de asegurar que esta norma sea respetada.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD FÍSICA	
	CÓDIGO: NO-028	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SEGURIDAD FÍSICA

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD FÍSICA	
	CÓDIGO: NO-028	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD FÍSICA	
	CÓDIGO: NO-028	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Garantizar el correcto tratamiento e identificación de las áreas seguras del Ministerio de Educación, en adelante el Ministerio.

2. Definición de términos

2.1. **Área segura:** Oficina cerrada o varios despachos dentro de un perímetro de seguridad física

3. Disposiciones Generales

El Oficial de Seguridad es responsable verificar el cumplimiento de lo dispuesto en la presente norma.

4. Descripción

4.1. Todo recurso de información debe encontrarse ubicado fuera de cualquier área de acceso público.

4.2. Toda área segura no debería dar indicación de su presencia. Se deben evitar señales y cualquier medio visual, auditivo o de cualquier tipo que advierta de su presencia y contenido.

4.3. Todo medio de acceso a las zonas seguras como ventanas, puertas u otros, debe permanecer cerrado si es que no hay ninguna persona presente. Así mismo no se debería tener equipos tipo fax, fotocopiadoras, impresoras u otro dispositivo de salida cerca de un acceso abierto al público en general.

4.4. Se deben tener dispositivos de detección de movimientos en zonas aquellas donde no es permitido el acceso, así como para todos los puntos de entrada a las áreas seguras.

4.5. No se debe contar con material inflamable ni de almacenamiento de los mismos cerca de las áreas seguras.

4.6. Por ningún motivo se debe sacar equipos informáticos de las instalaciones del Ministerio sin la autorización respectiva del Jefe de Informática del Ministerio.

4.7. Cada vez que un equipo salga de las instalaciones del Ministerio, se debe registrar su fecha y hora de salida, persona que retira el equipo y destino del equipo como mínimo.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SERVICIOS EXTERNOS	
	CÓDIGO: NO-029	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SERVICIOS EXTERNOS

Ministerio de Educación	DOCUMENTO: NORMA DE SERVICIOS EXTERNOS	
	CÓDIGO: NO-029	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

0107 -2008-ED

Ministerio de Educación	**DOCUMENTO:** NORMA DE SERVICIOS EXTERNOS	
	CÓDIGO: NO-029	**EDICIÓN:** 01
		FECHA APROBACIÓN:

1. Objetivo

Reducir posibles riesgos que puedan presentar a raíz del manejo de información del Ministerio de Educación, en adelante el Ministerio, por parte de entidades externas.

2. Disposiciones Generales

El Oficial de Seguridad es responsable verificar el cumplimiento de lo dispuesto en la presente norma.

3. Descripción

3.1. Toda información que sea manejada por terceros y que sea propiedad del Ministerio debe contar con la aprobación de los propietarios de la mencionada información.

3.2. Se debe contar con controles y mecanismos que permitan continuar con las operaciones del negocio en caso de verse comprometida la confidencialidad, integridad o disponibilidad de información.

3.3. Las aplicaciones vitales y sensibles del Ministerio deben ser identificadas e inventariadas.

3.4. Se deben tener responsabilidades designadas que permitan el tratamiento de incidentes de seguridad.

3.5. Se deberán establecer cláusulas en los contratos con terceros que permitan mitigar los riesgos asociados a los servicio que brinda el tercero, definiendo los controles a implementar y las responsabilidades de las partes.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE USO DE CORREO ELECTRÓNICO	
	CÓDIGO: NO-030	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE USO DE CORREO ELECTRÓNICO

Ministerio de Educación	DOCUMENTO: NORMA DE USO DE CORREO ELECTRÓNICO	
	CÓDIGO: NO-030	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE USO DE CORREO ELECTRÓNICO	
	CÓDIGO: NO-030	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Minimizar los riesgos asociados al uso del correo electrónico del Ministerio de Educación, en adelante el Ministerio.

2. Definición de términos

2.1. **Usuario:** Persona que realiza determinada labor dentro de una Unidad Orgánica del Ministerio, y a quién se le ha asignado una identificación digital, para que pueda acceder a ciertos recursos informáticos y de telecomunicaciones disponibles en la red.

2.2. **Mesa de ayuda (Help Desk):** Servicio de ayuda y soporte en línea que brinda la Sub Gerencia de Soporte Técnico Operativo a todos los Usuarios de la Institución. Cuenta con herramientas en hardware y software que le permite resolver cualquier tipo de problema.

2.3. **Virus:** Pequeño programa escrito intencionalmente para auto instalarse en la computadora de un usuario sin el conocimiento o el permiso de éste. Normalmente se comporta como un programa parásito porque el programa infecta y ataca a los archivos del sistema y del usuario. Para propagarse se replica a si mismo ilimitadas veces, llegando a producir serios daños que pueden afectar a los sistemas y archivos en general, pudiendo estos últimos daños borrar, corromper o destruir dichos archivos.

2.4. **Correo electrónico:** Es un servicio de red para permitir a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos.

3. Disposiciones Generales

Se definen las siguientes responsabilidades:

3.1 El Oficial de Seguridad es responsable de:

- Controlar que el proceso de otorgamiento de cuentas de correo a los usuarios se realice de acuerdo a lo estipulado por el PR-04-01-01 - Procedimiento Creación y/o Modificación de Accesos y el PR-04-01-02 - Procedimiento de Eliminación de Accesos.

3.2 El Custodio de Información es responsable de:

- Velar por que las credenciales de acceso se encuentren adecuadamente configuradas en la plataforma de correo electrónico del Ministerio.

4. Descripción

4.1. La dirección de correo electrónica asignada a los empleados es propiedad del Ministerio y es suministrada únicamente con el propósito de enviar y recibir comunicación de los miembros del Ministerio, proveedores y terceros relacionados a los fines institucionales.

4.2. El correo electrónico es un medio de comunicación cuya confidencialidad está en función de una contraseña de acceso personal e intransferible. En el caso de que se envíe y/o reciba a través de

Internet documentos altamente confidenciales, éstos deberán estar protegidos con una contraseña adicional.

4.3. El Ministerio tendrá el derecho o facultad para verificar que se está dando el uso adecuado a estos medios, por lo que podrá acceder a la información contenida en los mismos para realizar investigaciones por sospecha y abuso; intentando hacerlo solamente cuando exista una razón de interés institucional que afecte las operaciones del Ministerio.

4.4. El uso de los grupos por división, categoría y todo el personal, es exclusivamente para envío de comunicaciones con fines institucionales; quedando estrictamente prohibido su uso para envío de comunicaciones personales, cadenas o mensajes que no involucren directamente a los destinatarios.

4.5. Nunca deben ser transmitidos en mensajes de correo electrónico los siguientes elementos: identificadores de entrada al sistema (Login, IDs), contraseñas, configuraciones de redes internas, direcciones y nombres de sistemas.

DEL USO DEL CORREO

4.6. El servicio de correo es provisto por el Ministerio a los usuarios con el objeto de apoyar el desarrollo de sus funciones, por lo tanto toda información transferida por este medio es de propiedad del Ministerio.

4.7. El Ministerio definirá el estándar de una plataforma de correo único, queda estrictamente prohibido la utilización de otro sistema de correo.

4.8. El uso aceptable del correo se basará fundamentalmente en la comunicación entre empleados y no empleados para fines institucionales.

4.9. Los correos electrónicos enviados desde las cuentas provistas por el Ministerio deben tener las mismas consideraciones tomadas en cuenta al enviar una carta formal con el membrete del Ministerio.

4.10. En la comunicación por correo se deberá mantener las mismas reglas de cortesía y formalidades de la información escrita, aplicando también todas las reglas semánticas y ortográficas.

4.11. Cada usuario es responsable de mantener el espacio asignado en su cuenta o limites de correo para permitir la correcta recepción de mensajes, para lo cual deberá realizar labores de mantenimiento y limpieza de su correo.

4.12. El Custodio de Información tendrá la facultad de borrar correos, condicionado a eventos de seguridad que ponga en juego la disponibilidad del servicio. Si llegase a hacer uso de esta facultad, y fuese posible, deberá respaldar estos correos.

4.13. El Ministerio no es responsable por el efecto que pueda causar un mensaje enviado por un empleado a otro empleado o a un grupo de empleados. Los mensajes enviados desde cualquier cuenta de correo son responsabilidad únicamente de la persona a la que se le confió dicha cuenta.

4.14. El Ministerio deberá agregar en el pie de cada correo enviado, una nota que indique la clasificación de esta información.

4.15. El Oficial de Seguridad deberá aprobar el uso de las cuentas genéricas de correo electrónico, éstas deberán ser asignadas a una persona, la cual será la responsable de la cuenta y aparecerá como tal.

4.16. Todas las cuentas genéricas deberán tener contraseñas robustas.

DEL USO PROHIBIDO DEL SERVICIO DE CORREO

4.17. Se prohíbe el uso del correo electrónico para fines ajenos a la institución, como por ejemplo para recibir o transmitir música, videos, humor, gráficos e imágenes inapropiadas. El contenido de los mensajes no debe ser injurioso, ofensivo o irrespetuoso, ni debe hacer referencia a temas filosóficos, políticos, religiosos, de sexo u otros que por su contenido se aparten de temas propios de la Institución.

4.18. En caso de que información particular sea canalizada a través de una persona que se ausente del Ministerio, ésta deberá delegar esta función a otra persona de la misma dependencia durante su ausencia y anunciar a sus corresponsales el cambio.

4.19. Se prohíbe difundir por correo electrónico al interior de la organización, noticias que provengan de Internet o de otros medios, o tomar información de dicha red dándola por cierta. Cualquier información debe ser aprobada por la Gerencia correspondiente y coordinada con el Oficial de Seguridad.

4.20. Cualquier documento que se adjunte a un mensaje, deberá estar libre de virus. Será responsabilidad del usuario emisor del mensaje la revisión mediante antivirus. Las áreas receptoras de mensajes infectados con virus deberán abstenerse de abrirlos y deberán informar al Custodio de Información sobre su presencia.

4.21. Se prohíbe difundir por correo electrónico, dentro o fuera del Ministerio información clasificada como confidencial. En este caso todo correo electrónico deberá tener en el campo asunto la palabra CONFIDENCIAL, y de ser posible se deberá utilizar técnicas de encriptación.

4.22. En caso se reciba un correo electrónico desde algún usuario no identificado, o con sospecha de algún tipo de ataque, se deberá informar al Oficial de Seguridad sobre dichos eventos.

4.23. Se debe restringir el acceso remoto de los usuarios a las cuentas de correo electrónico. En caso sea necesario contar con este acceso, este deberá ser autorizado por la jefatura inmediata, de acuerdo al procedimiento PR-04-01-01 Creación y modificación de accesos. Esta jefatura deberá ser conciente de los riesgos asociados a esta autorización así como responsable de las consecuencias en caso estos riesgos se materialicen.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN EQUIPOS MÓVILES	
	CÓDIGO: NO-031	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE SEGURIDAD EN EQUIPOS MÓVILES

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN EQUIPOS MÓVILES	
	CÓDIGO: NO-031	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE SEGURIDAD EN EQUIPOS MÓVILES	
	CÓDIGO: NO-031	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Garantizar que no se comprometa la información del Ministerio de Educación, en adelante el Ministerio, cuando se utilizan dispositivos informáticos móviles.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

2.1. La Oficina de Informática es responsable de:

- Otorgar los permisos de acceso a la red del Ministerio, para los equipos móviles de terceros, en caso se requiera.
- Autorizar el ingreso a las instalaciones del Ministerio de equipos móviles de terceros, ya sean proveedores, consultores, auditores externos o equipos personales de los empleados.

2.2. El Oficial de Seguridad es responsable de:

- Asegurar que el equipo móvil de terceros no representa riesgo alguno o que no pone en riesgo la integridad de los datos del Ministerio y sistemas que los soportan.

2.3. El Encargado de Soporte Técnico es responsable de:

- Configurar los equipos móviles de terceros con el fin de alinearlos a los estándares de seguridad del Ministerio y de esta forma puedan ingresar de forma segura a la red.

3. Descripción

3.1. Cuando se utilizan dispositivos informáticos móviles tales como computadoras personales, organizadores y/o teléfonos móviles, se debe tener especial cuidado en garantizar que no se comprometa la información del Ministerio. Se debe tomar en cuenta los riesgos que implica trabajar con herramientas informáticas móviles en particular en ambientes no protegidos. Dentro de estas consideraciones debe incluirse los requerimientos de protección física, controles de acceso, técnicas criptográficas, resguardos y protección contra virus. Debe incluirse además reglas y asesoramiento en materia de conexión de dispositivos móviles a redes y orientación sobre uso de estos dispositivos en lugares públicos.

3.2. Se deben tomar consideraciones al utilizar dispositivos informáticos móviles en lugares públicos, salas de reuniones y otras áreas no protegidas fuera de la sede de la organización. Se debe implementar protección para evitar el acceso no autorizado a la información almacenada y procesada por estas herramientas, o la divulgación de la misma, por ejemplo, mediante técnicas criptográficas.

3.3. Es importante que cuando dichos dispositivos sean utilizados en lugares públicos se tomen consideraciones para evitar el riesgo de que la información que aparece en pantalla, sea vista por personas no autorizadas. Se debe implementar procedimientos contra software malicioso y estos deben mantenerse actualizados. El equipamiento debe estar disponible para permitir un procedimiento de resguardo rápido y fácil de la información. Estos procedimientos deben estar adecuadamente protegidos contra situaciones como robo o pérdida de la información.

3.4. Se debe brindar protección adecuada para el uso de dispositivos móviles conectados a redes. El acceso remoto a la información del Ministerio a través de redes públicas, utilizando herramientas informáticas móviles, sólo debe tener lugar después de una identificación y autenticación exitosa y con mecanismos adecuados de control de acceso.

DE LA SEGURIDAD FISICA DE LOS EQUIPOS MÓVILES

3.5. Los dispositivos informáticos móviles también deben estar físicamente protegidos contra robo. El equipamiento que transporta información importante del Ministerio, sensible y/o crítica no debe dejarse desatendido; cuando resulte posible debe estar físicamente resguardado bajo llave, o debe utilizarse cadenas de escritorio preferiblemente con llave, ya que las que utilizan clave pueden ser decodificadas.

3.6. Se debe brindar entrenamiento al personal que utiliza equipos móviles para incrementar su conocimiento de los riesgos adicionales ocasionados por esta forma de trabajo y de los controles que se deben implementar.

DE LA SEGURIDAD DE LOS EQUIPOS MÓVILES FUERA DE LAS INSTALACIONES DEL MINISTERIO

3.7. El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la organización debe ser autorizado por la Oficina de Informática. La seguridad provista debe ser equivalente a la suministrada dentro de la organización teniendo en cuenta los riesgos de trabajar fuera de la misma. El equipamiento de procesamiento de la información incluye todo tipo de computadoras personales, organizadores, teléfonos móviles, papel u otros formularios, necesarios para el trabajo en el domicilio o que es transportado fuera del lugar habitual de trabajo.

3.8. Se debe considerar los siguientes lineamientos:

- El equipamiento y dispositivos retirados del ámbito de la organización no deben permanecer desatendidos en lugares públicos. Las computadoras personales deben ser transportadas como equipaje de mano.
- Se deben respetar permanentemente las instrucciones del fabricante como la protección por exposición a campos electromagnéticos fuertes.

- Los controles de trabajo fuera de la institución deben ser determinados a partir de un análisis de riesgo y se aplicará controles adecuados según corresponda, como por ejemplo, gabinetes de archivo con cerradura, política de escritorios limpios y control de acceso a computadoras.
- Una adecuada cobertura de seguro debe estar en orden para proteger el equipamiento dentro y fuera del ámbito de la organización.

3.9. Los riesgos de seguridad tales como robo o interceptación de información pueden variar considerablemente según las ubicaciones y deben ser tenidas en cuenta al determinar los controles más apropiados.

DE LA CONEXIÓN DE EQUIPOS MÓVILES DE TERCEROS A LA RED DEL MINISTERIO

3.10. Los equipos de terceros que deban ser conectados a la red del Ministerio deberán contar con la aprobación previa del Oficial de Seguridad.

3.11. Todo equipo de terceros a ser conectado a la red del Ministerio deberá ser revisado para comprobar que cuente con un sistema antivirus actualizado. De no ser así la Oficina de Informática se encargará de notificar al tercero la necesidad de instalar el antivirus necesario.

3.12. Se deberá verificar que el sistema operativo cuente con las últimas actualizaciones publicadas por el fabricante.

3.13. Se deberá asignar un perfil para la persona que utilizará el equipo considerando las restricciones a los recursos de red.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: NORMA DE USO DE PROTECTORES DE PANTALLA Y ESCRITORIOS LIMPIOS	
	CÓDIGO: NO-032	EDICIÓN: 01
		FECHA APROBACIÓN:
RESOLUCIÓN MINISTERIAL:		

SECRETARÍA DE PLANIFICACIÓN ESTRATÉGICA

OFICINA DE INFORMÁTICA

NORMA DE USO DE PROTECTORES DE PANTALLA Y ESCRITORIOS LIMPIOS

Ministerio de Educación	DOCUMENTO: NORMA DE USO DE PROTECTORES DE PANTALLA Y ESCRITORIOS LIMPIOS	
	CÓDIGO: NO-032	EDICIÓN: 01
		FECHA APROBACIÓN:

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados

Ministerio de Educación	DOCUMENTO: NORMA DE USO DE PROTECTORES DE PANTALLA Y ESCRITORIOS LIMPIOS	
	CÓDIGO: NO-032	EDICIÓN: 01
		FECHA APROBACIÓN:

1. Objetivo

Reducir el riesgo de accesos no autorizados, pérdida y daño de la información en estaciones de trabajo desatendidas y/o escritorios de el Ministerio de Educación, en adelante el Ministerio.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

2.1. El Oficial de Seguridad es responsable de:

- Verificar el cumplimiento de las medidas de protección de información a través de revisiones periódicas.

2.2. Los Usuarios son responsables de:

- Proteger la información que se encuentre alojada ya sea en sus propias estaciones de trabajo, equipos móviles, medios magnéticos removibles o documentos impresos.

3. Descripción

3.1. La adopción de una norma de escritorios limpios para proteger documentos en papel así como dispositivos de almacenamiento removibles, y una norma de protectores de pantalla en las estaciones de trabajo, reduce el riesgo de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

3.2. La información debe ser clasificada contemplando la seguridad de la misma, según se estipula en la NO-003 - Norma de Clasificación y Manejo de la Información.

3.3. La información que se deja sobre los escritorios se encuentra expuesta a sufrir daños o destrozos en caso de producirse un desastre como incendio, inundación o explosión.

DE LA PROTECCION DE LA INFORMACIÓN

3.4. Cuando corresponda, los documentos en papel y los medios informáticos deben ser almacenados bajo llave en gabinetes y/u otro tipo de mobiliario seguro cuando no estén siendo utilizados, especialmente fuera del horario de trabajo.

3.5. La información sensible o crítica del Ministerio debe guardarse bajo llave (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.

3.6. Las estaciones de trabajo, y terminales no deben dejarse prendidas cuando están desatendidas y las mismas deben ser protegidas mediante contraseñas u otros controles cuando no están en uso.

3.7. Cada vez que un usuario abandone temporalmente su escritorio por períodos cortos, deberá dejar su computadora en condición de bloqueada, para lo cual deberá ir al menú de inicio de sesión, presionando simultáneamente las teclas "Control", "Alt" y "Supr" luego seleccionar la opción "Bloquear computador". Esta opción solo cierra el acceso al equipo y mantiene activas todas las aplicaciones que estén en uso.

3.8. Se deben proteger los puntos de recepción y envío de correo, y las máquinas de fax no atendidas.

3.9. Las fotocopiadoras deben estar bloqueadas (o protegidas de alguna manera, del uso no autorizado) fuera del horario normal de trabajo.

3.10. La información sensible o confidencial, una vez impresa, debe ser retirada de la impresora inmediatamente.

3.11. Todas las estaciones de trabajo, computadoras móviles y servidores del dominio del Ministerio deben contar con un protector de pantalla institucional, el cual se activará automáticamente luego de 5 minutos de inoperatividad y debe encontrarse protegido mediante una contraseña.

3.12. Las computadoras portátiles deberán estar protegidas con cadenas u otros dispositivos de seguridad cuando estas sean utilizadas dentro o fuera de las instalaciones y se encuentren desatendidas.

3.13. Las computadoras portátiles adicionalmente deben llevar contraseña de hardware o BIOS.

DE LA AUDITORIA Y REVISION DEL CUMPLIMIENTO DE LA PROTECCION DE LA INFORMACIÓN

3.14. El Oficial de Seguridad deberá realizar trimestralmente una revisión aleatoria a las estaciones de trabajo para verificar la correcta configuración de protectores de pantalla y que se encuentren alineados a los estándares del Ministerio. Las no conformidades de cumplimiento de esta regla deben quedar documentadas.

3.15. El Oficial de Seguridad así como el personal de vigilancia deberá realizar rondas de observación a los escritorios de los empleados para comprobar el cumplimiento de la norma.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución Ministerial.

0107 -2008-ED

Ministerio de Educación

Procedimientos de Seguridad de la Información

Versión 1
(Versión 1.0)

Enero 2008

Ministerio
de Educación

Ministerio de Educación

PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACION

ID GRUPO	GRUPO DE PROCESOS	PROCESO	ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	DETALLE DEL PROCEDIMIENTO	FLUJOGRAMA DEL PROCEDIMIENTO
PR-01	Desarrollar la estrategia y planificar la operación del Centro de Datos	Evaluar ambiente de TI del Centro de Datos	PR-01-01-01	Evaluación del ambiente de TI	PR-01-01 (Hoja)	PR-01-01-01 (Diagrama)
		Identificar soluciones de TI para el Ministerio	PR-01-02-01	Evaluación de proyectos de TI nuevos	PR-01-02 (Hoja)	PR-01-02-01 (Diagrama)
		Definir estrategia de TI	PR-01-03-01	Administrar los cambios en la estrategia de TI	PR-01-03 (Hoja)	PR-01-03-01 (Diagrama)
PR-02	Planificar e implementar la arquitectura del Centro de Datos	Elaborar y actualizar políticas, normas y estándares de TI	PR-02-01-01	Elaboración de políticas, normas y estándares	PR-02-01 (Hoja)	PR-02-01-01 (Diagrama)
		Diseñar y administrar la arquitectura de TI y los repositorios de información	PR-02-02-01	Diseñar arquitectura de TI	PR-02-02 (Hoja)	PR-02-02-01 (Diagrama)
			PR-02-02-02	Evaluar arquitectura de TI	PR-02-02 (Hoja)	PR-02-02-02 (Diagrama)
PR-03	Desplegar y mantener productos y servicios de TI	Definir la funcionalidad requerida de sistemas y de seguridad, probar y desplegar los sitemas	PR-03-01-01	Gestión del control de cambios en los sistemas de información	PR-03-01 (Hoja)	PR-03-01-01 (Diagrama)
			PR-03-01-02	Ejecución de la solución	PR-03-01 (Hoja)	PR-03-01-02 (Diagrama)
			PR-03-01-03	Validación de la solución	PR-03-01 (Hoja)	PR-03-01-03 (Diagrama)
PR-04	Administrar la seguridad y los riesgos	Administrar la seguridad de los sistemas	PR-04-01-01	Creación y/o modificación de accesos	PR-04-01 (Hoja)	PR-04-01-01 (Diagrama)
			PR-04-01-02	Eliminación de accesos	PR-04-01 (Hoja)	PR-04-01-02 (Diagrama)
			PR-04-01-03	Eliminación de información sensible	PR-04-01 (Hoja)	PR-04-01-03 (Diagrama)
		Administrar el ambiente físico del Centro de Datos	PR-04-02-01	Otorgamiento de acceso físico	PR-04-02 (Hoja)	PR-04-02-01 (Diagrama)
			PR-04-02-02	Control de acceso físico	PR-04-02 (Hoja)	PR-04-02-02 (Diagrama)
			PR-04-02-03	Autorización de un nuevo recurso de tratamiento de la información	PR-04-02 (Hoja)	PR-04-02-03 (Diagrama)
		Evaluar y administrar riesgos de TI	PR-04-03-01	Identificación de Riesgos	PR-04-03 (Hoja)	PR-04-03-01 (Diagrama)
			PR-04-03-02	Evaluación de Riesgos	PR-04-03 (Hoja)	PR-04-03-02 (Diagrama)
			PR-04-03-03	Definición de Estrategia de Mitigación de Riesgos	PR-04-03 (Hoja)	PR-04-03-03 (Diagrama)
			PR-04-03-04	Monitoreo de Estrategia de Mitigación de Riesgos	PR-04-03 (Hoja)	PR-04-03-04 (Diagrama)
			PR-04-03-05	Clasificación de activos de la información	PR-04-03 (Hoja)	PR-04-03-05 (Diagrama)
			PR-04-03-06	Marcado de la información	PR-04-03 (Hoja)	PR-04-03-06 (Diagrama)
		Administrar incidencias de seguridad	PR-04-04-01	Respuesta ante incidencias de seguridad	PR-04-04 (Hoja)	PR-04-04-01 (Diagrama)
			PR-04-04-02	Administración de incidentes de seguridad	PR-04-04 (Hoja)	PR-04-04-02 (Diagrama)
PR-05	Administrar la operación del ambiente de TI	Planificar y administrar la capacidad	PR-05-01-01	Monitoreo de la Disponibilidad	PR-05-01 (Hoja)	PR-05-01-01 (Diagrama)
			PR-05-01-02	Monitoreo de la Capacidad	PR-05-01 (Hoja)	PR-05-01-02 (Diagrama)
			PR-05-01-03	Monitoreo de Logs de incidencias	PR-05-01 (Hoja)	PR-05-01-03 (Diagrama)

0107 -2008-ED

Ministerio de Educación

PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACION

ID GRUPO	GRUPO DE PROCESOS	PROCESO	ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	DETALLE DEL PROCEDIMIENTO	FLUJOGRAMA DEL PROCEDIMIENTO
		Desarrollar y administrar el Plan de Contingencia del Centro de Datos	PR-05-02-01	Elaboración del plan de contingencia	PR-05-02 (Hoja)	PR-05-02-01 (Diagrama)
			PR-05-02-02	Implementación del plan de contingencia	PR-05-02 (Hoja)	PR-05-02-02 (Diagrama)
			PR-05-02-03	Prueba al plan de contingencia	PR-05-02 (Hoja)	PR-05-02-03 (Diagrama)
		Desarrollar y administrar la protección de la información	PR-05-03-01	Definición de Plan de Respaldo	PR-05-03 (Hoja)	PR-05-03-01 (Diagrama)
			PR-05-03-02	Ejecución de Plan de Respaldo	PR-05-03 (Hoja)	PR-05-03-02 (Diagrama)
			PR-05-03-03	Ejecución de Plan de Restauración	PR-05-03 (Hoja)	PR-05-03-03 (Diagrama)
			PR-05-03-04	Custodia Externa de Respaldos	PR-05-03 (Hoja)	PR-05-03-04 (Diagrama)
			PR-05-03-05	Custodia Interna de Respaldos	PR-05-03 (Hoja)	PR-05-03-05 (Diagrama)
			PR-05-03-06	Prueba de respaldo de información	PR-05-03 (Hoja)	PR-05-03-06 (Diagrama)
			PR-05-03-07	Definición de Catálogo de Respaldo	PR-05-03 (Hoja)	PR-05-03-07 (Diagrama)
		Resolver problemas de los sistemas	PR-05-04-01	Administración de incidentes de operación	PR-05-04 (Hoja)	PR-05-04-01 (Diagrama)
			PR-05-04-02	Administración de incidentes de usuario	PR-05-04 (Hoja)	PR-05-04-02 (Diagrama)
		Mejorar y mantener los recursos de TI	PR-05-05-01	Control de cambios sobre recursos de TI	PR-05-05 (Hoja)	PR-05-05-01 (Diagrama)
			PR-05-05-02	Mantenimiento preventivo/correctivo	PR-05-05 (Hoja)	PR-05-05-02 (Diagrama)
			PR-05-05-03	Recolección de evidencia	PR-05-05 (Hoja)	PR-05-05-03 (Diagrama)
		Administrar los activos de TI	PR-05-06-01	Elaboración inventario de activos de TI	PR-05-06 (Hoja)	PR-05-06-01 (Diagrama)
			PR-05-06-02	Actualización inventario de activos de TI	PR-05-06 (Hoja)	PR-05-06-02 (Diagrama)
PR-06	Brindar soporte y capacitar a los usuarios	Capacitar a los usuarios finales y monitorear su progreso	PR-06-01-01	Brindar capacitación	PR-06-01 (Hoja)	PR-06-01-01 (Diagrama)
		Medir la satisfacción del usuario	PR-06-02-01	Elaboración de Encuestas Aleatorias	PR-06-02 (Hoja)	PR-06-02-01 (Diagrama)
			PR-06-02-02	Elaboración de Encuestas en Capacitaciones	PR-06-02 (Hoja)	PR-06-02-02 (Diagrama)
		Resolver problemas de usuarios de TI	PR-06-03-01	Administración de incidentes de usuario	PR-06-03 (Hoja)	PR-06-03-01 (Diagrama)
		Administrar los recursos de Help Desk	PR-06-04-01	Seguimiento de Desempeño de Help Desk	PR-06-04 (Hoja)	PR-06-04-01 (Diagrama)
PR-07	Administrar el Centro de Datos	Entrenar al personal del Centro de Datos	PR-07-01-01	Elaborar Plan de Capacitación	PR-07-01 (Hoja)	PR-07-01-01 (Diagrama)
			PR-07-01-02	Capacitar al Personal	PR-07-01 (Hoja)	PR-07-01-02 (Diagrama)

0107 -2008-ED

Min o de Educación

GLOSARIO DEL DIAGRAMA DE PROCESO

ID PROCEDIMIENTO	Código que identifica un procedimiento (un proceso puede estar compuesto por uno o varios procedimientos). Esta compuesto por el código identificador del procedimiento (Por ejemplo: PR-02-01) seguido de un numero correlativo.
TITULO DEL PROCEDIMIENTO	Nombre del procedimiento.
TAREA	Descripción de la actividad a realizar. Cada actividad se documenta como un renglón dentro de la tabla contenida en esta sección.
TIPO DE TAREA	Sección que indica información del tipo de la actividad.
	Iteración (loop)
	Actividad de procesamiento del algun tipo.
	Actividad de toma de decisión
	Actividad de análisis de entrada y/o emisión de salidas
	Actividad de documentación.
REGISTRO	Nombre del registro generado por la actividad.
SECCION DE REGISTRO	Sección del registro en el que se registra algun control definido por la actividad.
RESPONSABLE	Persona encargada de ejecutar la actividad.

0107 -2008-EE

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-01-01
PROCESO	Evaluar ambiente de TI del Centro de Datos
GRUPO DE PROCESOS	Desarrollar la estrategia y planificar la operación del Centro de Datos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Evaluar el ambiente actual de datos, plataformas y telecomunicaciones en el Centro de Datos:
- Evaluar si la información es accesible, precisa, administrada y si se han definido propietarios, describir los distintos ambientes de información soportados actualmente.
- Evaluar el número de plataformas que son soportadas actualmente. Describir el ambiente de TI existente.
- Evaluar cuán bien se emplea la comunicación electrónica. Determinar si el ambiente actual soporta la carga de tráfico

ALCANCE

Todos los activos de información incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del Procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en evaluar de manera integral del ambiente de procesamiento para identificar necesidades de mejora en las estrategias de TI y la operación del Centro de Datos.

REGISTROS

Informe de Evaluación	

INDICADORES

De metas	De desempeño
% de componentes de infraestructura que no se pueden soportar (o que no lo seran en el futuro).	# y tipo de modificaciones de emergencia a componentes de la infraestructura.

VIGENCIA

Inicio		Fin	
Revision			

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Evaluar ambiente de TI del Centro de Datos**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO ASOCIADO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-01-01-01	**Evaluación del ambiente de TI**	Revisar información relevante de evaluaciones de ambiente previas en los **Informes de Evaluación anteriores**				●				Responsable de Infraestructura
		Revisar la estrategia de TI en el **Plan Estratégico de TI** para validar los desafíos en los servicios y productos a implementar en el futuro				●				Responsable de Infraestructura
		Identificar los activos de información mas importantes para el ambiente de TI		●						
		Evaluar la capacidad actual de los activos de información mas críticos para el ambiente de TI		●				Ver procedimiento PR-02-02-02		
		Por cada activo de información identificado	●							
		Proyectar la demanda de capacidad para el siguiente periodo		●						Especialista de Infraestructura
		Documentar los resultados de la evaluación de capacidad					●	Informe de Evaluación		Especialista de Infraestructura
		Evaluar el desempeño de los servicios de HelpDesk		●				Ver Procedimiento PR-06-04-01		
		Documentar los resultados consolidados del desempeño de HelpDesk					●	Informe de Evaluación		Responsable de HelpDesk
		Analizar los costos operativos del Ambiente de TI		●						Responsable de Infraestructura
		Evaluar la arquitectura de TI de los activos de información mas críticos para el ambiente de TI		●				Ver procedimiento PR-02-02-01		
		Documentar los resultados de la evaluación de arquitectura de TI					●	Informe de Evaluación		Especialista de Infraestructura
		Documentar las necesidades de TI aplicables					●	Informe de Evaluación		Responsable de Infraestructura
		Documentar las conclusiones de la evaluación del ambiente de TI					●	Informe de Evaluación		Responsable de Infraestructura
		Revisar el informe realizado		●						Jefe de Oficina Informática
		Enviar el informe a la Alta Dirección		●						Jefe de Oficina Informática

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-01-02
PROCESO	Identificar soluciones de TI para el Ministerio
GRUPO DE PROCESOS	Desarrollar la estrategia y planificar la operación del Centro de Datos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPÓSITO

Identificar y priorizar aquellas soluciones de TI críticas para el Ministerio y que permiten y permitirán alcanzar la estrategia del mismo. El resultado de esta identificación deberá ser revisado y priorizado por un Comité de Sistemas / Comité Ejecutivo.

ALCANCE

Todos las necesidades de TI que aún no se encuentran definidas dentro de la estrategia de TI que puedan afectar de manera importante los activos de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en asegurar una adecuada evaluación de los requerimientos de TI que pueden convertirse en nuevos proyectos dentro de la estrategia de TI del Ministerio.

REGISTROS

Estudio Técnico-Financiero	

INDICADORES

De metas	De desempeño
% de inversiones en TI que generan los beneficios predefinidos	% de proyectos con beneficios definidos por adelantado

VIGENCIA

Inicio		Fin	
Revisión			

Mi[illegible] de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Identificar soluciones de TI para el Ministerio**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-01-02-01	**Evaluación de proyectos de TI nuevos**	Evaluar el ambiente de TI para identificar necesidades de implementación				●		Ver Procedimiento PR-01-01-01		Especialista de Infraestructura
		Contrastar las necesidades identificadas en el **Informe de Evaluación** del ambiente con **el Plan Estratégico Institucional,** el **Plan Estratégico Sectorial,** el **Plan Estratégico de TI** y los **Macroprocesos del Ministerio.**				●				Responsable de Infraestructura
		Por cada necesidad de TI identificada	●							
		Identificar alternativas de solución		●						Especialista de Infraestructura
		Por cada alternativa identificada	●							
		Evaluar los requerimientos de arquitectura de TI		●				Ver Procedimiento PR-02-02-01		
		Elaborar un análisis de los flujo de efectivo operativos asociado a la alternativa					●	Estudio Técnico-Financiero		Especialista de Infraestructura
		Elaborar un análisis la TIR y el VPN asociado a la implementación de la alternativa					●	Estudio Técnico-Financiero		Especialista de Infraestructura
		Elaborar un análisis costo/beneficio de la alternantiva					●	Estudio Técnico-Financiero		Especialista de Infraestructura
		Identificar la mejorar alternativa en base al análisis y documentar las conclusiones pertinentes					●	Estudio Técnico-Financiero		Responsable de Infraestructura
		Revisar el estudio realizado		●						Jefe de Oficina Informática

0107 -2008-ED

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-01-03
PROCESO	Definir estrategia de TI
GRUPO DE PROCESOS	Desarrollar la estrategia y planificar la operación del Centro de Datos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPÓSITO

Brindar soporte en el desarrollo de una visión de alto nivel de la arquitecturas de información, tecnologías y telecomunicaciones futuras del Ministerio. Brindar soporte a la visión estratégica de TI de la entidad.

ALCANCE

Todos los proyectos definidos factibles de ejecución que no se encuentran dentro de la estrategia de TI y que puedan afectar de manera importante los activos de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas para incluir los proyectos factibles de ejecución dentro de la estrategia de TI del Ministerio.

REGISTROS

Plan Estratégico de TI	
Plan de Operaciones Anual	

INDICADORES

De metas	De desempeño
% de proyectos de TI en el portafolio de proyectos de TI que pueden rastrear directamente al plan estratégico/táctico de TI.	Retraso entre las actualizaciones de planes estratégicos de TI y actualizaciones de planes tácticos de TI.

VIGENCIA

Inicio		Fin	
Revisión			

Mir[illegible]o de Educación

DIAGRAMA DE PROCEDIMIENTO
Procedo: **Definir estrategia de TI**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-01-03-01	**Administrar los cambios en la estrategia de TI**	Revisar el **Plan Estratégico de TI**				●				Responsable de Infraestructura
		Revisar el **Plan de Operaciones Anual**				●				Responsable de Infraestructura
		Evaluar los nuevos proyectos de TI identificados		●				Ver Procedimiento PR-01-02-01		
		Evaluar los proyectos de TI en ejecución		●						
		Identificar los proyectos que impactan de manera importante la estrategia de TI definida según los **Informes de Evaluación de Proyectos**				●				Responsable de Infraestructura
		Por cada proyecto identificado	●							
		Si el proyecto afecta la estrategia de TI a largo plazo			●					
		Actualizar el Plan Estratégico de TI					●	Plan Estratégico de TI		Responsable de Infraestructura
		Revisar el Plan Estratégico de TI		●						Jefe de Oficina Informática
		Caso contrario, si el proyecto afecta la estrategia de TI a corto/mediano plazo			●					
		Actualizar el Plan de Operaciones Anual					●	Plan de Operaciones Anual		Responsable de Infraestructura
		Revisar el Plan de Operaciones Anual		●						Jefe de Oficina Informática
		Comunicar las estrategias nuevas / modificadas a la Alta Dirección		●						Jefe de Oficina Informática

0107 -2008-ED

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-02-01
PROCESO	Elaborar y actualizar políticas, normas y estándares de TI
GRUPO DE PROCESOS	Planificar e implementar la arquitectura del Centro de Datos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Desarrollar políticas y normas de TI para soportar las operaciones de la unidad. Definir estándares para elementos como software, hardware y telecomunicaciones para uniformizar las operaciones de la unidad.

ALCANCE

Todos las actividades que determinan la operación de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en la elaboración de normativa que rija los princpales procesos de operación de la plataforma de tecnología del Ministerio.

REGISTROS

Política, Norma y/o Estándar	

INDICADORES

De metas	De desempeño
% de requerimientos normativos que se encuentran documentados formalmente.	Frecuencia de revisiones/actualizaciones de las políticas

VIGENCIA

Inicio		Fin	
Revisión			

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
Proceso: **Elaborar y actualizar políticas, normas y estándares de TI**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-02-01-01	**Elaboración de políticas, normas y estándares**	Identificar requerimientos de documentación según **Requerimientos de normativas**				●				Especialista de Infraestructura y
		Por cada requerimiento de documentación	●							
		Revisar mejores prácticas que apoyan al proceso y/o actividad asociada a la normativa que se desea documentar		●						Especialista de Infraestructura y
		Documentar la normativa alineándola a la plataforma de tecnología existente					●	Política, Norma y/o Estándar		Especialista de Infraestructura y
		Documentar responsabilidades en la normativa alineadas a la estructura organizacional de la Oficina Informática.					●	Política, Norma y/o Estándar		Especialista de Infraestructura y
		Revisar la normativa desarrollada		●						Especialista de Infraestructura y
		Aprobar la normativa desarrollada		●						Jefe de Oficina Informática
		Si la normativa tiene alcance fuera de la Oficina Informática			●					
		Enviar la normativa para aprobación por parte de la Secretaría Estratégica de Planificación		●						Jefe de Oficina Informática

0107 -2008-ED

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-02-02
PROCESO	Diseñar y administrar la arquitectura de TI y los repositorios de información
GRUPO DE PROCESOS	Planificar e implementar la arquitectura del Centro de Datos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Diseñar y administrar las arquitecturas de telecomunicaciones, aplicaciones, datos, plataformas de cómputo y red.
Diseñar y administrar los repositorios de información del negocio.

ALCANCE

Todos los activos de información incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en el diseño y evaluación de la arquitectura de TI que soporta los principales activos de información de la plataforma de tecnología del Ministerio.

REGISTROS

Acta de Reunión	
Informe de Evaluación	

INDICADORES

De metas	De desempeño
% de componentes de infraestructura que no se pueden soportar (o que no lo seran en el futuro).	# y tipo de modificaciones de emergencia a componentes de la infraestructura.

VIGENCIA

Inicio		Fin	
Revision			

0107 -2008-ED

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO **Diseñar y administrar la arquitectura de TI y los repositorios de información**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA							REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-02-02-01	**Diseñar arquitectura de TI**	Identificar el activo de información sobre el cuál se desea validar la arquitectura que lo soportará según los **requisitos de evaluación de arquitectura**				●					Especialista de Infraestructura
		Si es un activo administrado por el área de Sistemas de Información			●						
		Coordinar reunión con personal de Sistemas de Información					●		Correo		Especialista de Infraestructura
		Verificar los **requisitos de arquitectura** a nivel de sistema operativo				●					Especialista de Infraestructura
		Verificar los **requisitos de arquitectura** a nivel de comunicaciones				●					Especialista de Infraestructura
		Verificar los **requisitos de arquitectura** a nivel de base de datos				●					Especialista de Infraestructura
		Verificar los **requisitos de arquitectura** a nivel de acceso a servicios existentes				●					Especialista de Infraestructura
		Comparar los requisitos contra la arquitectura actual		●							Especialista de Infraestructura
		Concluir sobre si la arquitectura actual soportará el activo de información a implementar					●		Acta de Reunión		Especialista de Infraestructura
PR-02-02-02	**Evaluar arquitectura de TI**	Identificar los activos de información mas críticos para el ambiente de TI según el **Informe de Evaluación de Ambiente**				●					Especialista de Infraestructura
		Evaluar la capacidad actual de los activos de información mas críticos para al ambiente de TI		●					Ver Procedimiento PR-05-01-02		
		Analizar las fortalezas y debilidades de los productos y servicios implementados					●		Informe de Evaluación		Especialista de Infraestructura
		Analizar tecnologías y prácticas alternativas a las actualmente implementadas					●		Informe de Evaluación		Especialista de Infraestructura
		Identificar las necesidades aplicables al ambiente de TI					●		Informe de Evaluación		Especialista de Infraestructura
		Documentar las conclusiones de la evaluación de la arquitectura					●		Informe de Evaluación		Responsable de Infraestructura
		Revisar el informe realizado		●							Jefe de Oficina Informática

0107 -2008-ED

Ministerio de Educación

FICHA DE PROCEDIMIENTO

IDENTIFICADOR	PR-03-01
PROCESO	Definir la funcionalidad requerida de sistemas y de seguridad, probar y desplegar los sitemas
GRUPO DE PROCESOS	Desplegar y mantener productos y servicios de TI
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Implementar los requerimientos de cambios a los sistemas de información. Esto incluye la definición del requerimientos, análisis del impacto del cambio, ejecución de pruebas y puesta en producción.

ALCANCE

Todos las actividades que rijan la operación adecuada del desarrollo de sistemas de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del prodedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCION

El procedimiento refiere a actividades realizadas por el área de Sistemas de Información, las cuáles se realizan fuera del ámbito del Centro de Datos

REGISTROS

Resgistro de control de requerimientos	

INDICADORES

De metas	De desempeño

VIGENCIA

Inicio		Fin	
Revisión			

0107 -2008-ED

Mi[illegible]o de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Definir la funcionalidad requerida de sistemas y de seguridad, probar y desplegar los sitemas**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-03-01-01	**Gestión para el cambio en las operaciones**	Enviar requerimiento al área de Sistemas de Información				●				Área Usuaria
		Registrar el requerimiento				●		Registro de control de requerimientos		Analísita de Sistemas de Información
		Evaluar el requerimiento considerando aspectos de seguridad, disponibilidad, confidencialidad, integridad e impacto.				●				Analísita de Sistemas de Información
		Determinar si el requerimiento es un proyecto, mejora, corrección o soporte. De ser necesario consultar al responsable de Sistemas de Información la decisión a tomar				●				Analísita de Sistemas de Información
		Si el requerimiento corresponde a un proyecto			●					
		Registrar el proyecto considerando los factores de: • Impacto; considerando los beneficios y consecuencias que produciría el cambio • Costos; considerando los costos de infraestructura, desarrollo, modificación de aplicación, cambio en el modelo de negocio o adquisición de software o hardware. • Viabilidad; considerando un plan alternativo de reversión en caso de					●	Ver Procedimiento PR-01-02-01		Analísita de Sistemas de Información
		Revisar la evaluación del proyecto				●				Responsable de Sistemas de Información
		Solicitar aprobación del requerimiento	●							Responsable de Sistemas de Información
		Caso contrario, Si el requerimiento corresponde a un soporte			●					
		Brindar solución por email, teléfono o personalmente				●				Analísita de Sistemas de Información
		Validar la solución con pruebas realizadas al momento con el usuario				●				Analísita de Sistemas de Información / Usuario
		Determinar la necesidad de capacitar al usuario				●		Ver Procedimiento PR-06-01-01		Analísita de Sistemas de Información
		Si el requerimiento corresponde a una mejora			●					
		Generar la propuesta de solución al requerimiento siempre que se trate de una nueva funcionalidad o facilidad que permita mejorar el desarrollo de las actividades		●						Analísita de Sistemas de Información
		Caso contrario, si el requerimiento corresponde a una corrección				●				
		Gestionar la solución propuesta del error que ha sido reportado				●				Analísita de Sistemas de Información
		Si la propuesa está conforme			●					
		Autorizar la solución al requerimiento				●				Responsable de Sistemas de Información
		Caso contrario, informar al usuario la decisión tomada				●				Analísita de Sistemas de Información
PR-03-01-02	**Ejecución de la solución**	Si se determina la necesidad de contratar a un proveedor de servicios			●					
		Cordinar con el proveedor la realización del mismo considerando siempre los aspectos de seguridad, disponibilidad, confidencialidad e integridad.				●		Ver Norma de inclusión de requisitos de seguridad en contratos con terceros		Responsable de Sistemas de Información
PR-03-01-03	**Validación de la solución**	Realizar las pruebas a la solución desarrollada para verificar que cumple con los requerimientos establecidos inicialmente		●						Analísita de Sistemas de Información
		Si existe conformidad con la solución			●					
		Informar al usuario que realice las pruebas de certificación necesarias				●				Analísita de Sistemas de Información
		Caso contrario, solicitar la solución de las observaciones identificadas		●						Analísita de Sistemas de Información

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-04-01
PROCESO	Administrar la seguridad de los sistemas
GRUPO DE PROCESOS	Administrar la seguridad y los riesgos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Procedimiento de gestión de la seguridad para mantener la integridad de la información y proteger los activos de TI. Esto incluye la definición y mantenimiento de privilegios de acceso, roles, perfiles y grupos. Tambien incluye la definición de responsabilidades de seguridad, políticas, normas y estándares, el monitoreo de la seguridad y la prueba periódica e implementación de acciones correctivas para vulnerabilidades o incidentes de seguridad.

ALCANCE

Todos los activos de información de la plataforma de tecnología de información del Centro de Datos.

CONTROL	
Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en la adecuada administración de la seguridad lógica de los recursos de hardware, software base y comunicaciones de la plataforma de tecnología del Centro de Datos.

REGISTROS

Formato de Registro y Actualización de Datos de Usuarios	
Listado de usuarios inactivos	
Bitácora de accesos de usuario	
Listado de Usuarios Inactivos	

INDICADORES

De metas	De desempeño
Cantidad de acceso no autorizado identificados por inadecuada eliminación de información.	# de derechos de acceso autorizados, revocados, restaurados o cambiados

VIGENCIA

Inicio		Fin	
Revisión			

Mi[illegible] de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Administrar la seguridad de los sistemas**

Ir al Índice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-04-01-01	**Creación y/o modificación de accesos**	Recibir un **Requerimiento de acceso** a la plataforma de TI				●		Formato de Registro y Actualización de Datos de Usuarios		Especialista de Infraestructura
		Si es un requerimiento de acceso para software base			●					
		Verificar la existencia de una autorización de dicha solicitud por parte del Jefe de Área Solicitante en el **Requerimiento de acceso** (Validar con la Matriz de dueños de la información)		●						Especialista de Infraestructura
		Si el requerimiento de accesos se encuentra debidamente autorizado			●					
		Otorgar los accesos solicitados		●				Bitácora de accesos de usuario		Especialista de Infraestructura
		Si se requiere algun tipo de configuración en la estación del usuario solicitante			●					
		Realizar una solicitud de configuración de la estación del usuario via Help Desk		●				Ver procedimiento: IT-07-04-01		
		Caso contrario, Si es un requerimiento de accesos a Sistemas de Información			●					
		Escalar la solicitud al área de Sistemas de Información		●						Especialista de Infraestructura
		Validar la autorización del acceso del usuario con la matriz de dueños de la información				●		Matriz de dueños de la información		
		Si el acceso se encuentra debidamente autorizado			●					
		Ejecutar accesos solicitados		●						
		Registrar la generación de accesos					●	Bitácora de accesos de usuario		
		Caso contrario, informar la denegación de acceso		●						
PR-04-01-02	**Eliminación de accesos**	Identificar los usuarios que se han mantenido inactivos por un periodo de tiempo regular					●	Listado de Usuarios Inactivos		Especialista de Infraestructura
		Revisar el listado de los usuarios inactivos identificados		●						Responsable de Infraestructura
		Enviar el listado de usuarios a las diferentes áreas solicitando acciones a tomar		●						Jefe de la Oficina Informática
		Recibir las **Respuestas de las áreas correspondientes sobre acciones a tomar**				●				Jefe de la Oficina Informática
		Por cada usuario identificado en la respuesta	●							
		Si se solicita eliminar el usuario y/o algún acceso otorgado			●					
		Eliminar el usuario y/o acceso		●				Bitácora de accesos de usuario		Especialista de Infraestructura
		Caso contrario			●					
		Mantener los accesos otorgados		●				Bitácora de accesos de usuario		Especialista de Infraestructura
PR-04-01-03	**Eliminacion de información sensible**	Recibir un requerimiento para eliminación de información sensible.				●				HelpDesk
		Verificar la clasificación de la información según la norma de clasificación y manejo de la información.		●						Responsable de Infraestructura
		Realizar la destrucción de la información de acuerdo a la clasificación del activo y a los establecido en la Norma de seguridad y re-uso o eliminación de equipos y medios informáticos.		●				Ver Norma de seguridad y re-uso o eliminación de equipos y medios informáticos		Responsable de Infraestructura

0107-2008-ED

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-04-02
PROCESO	Administrar el ambiente físico del Centro de Datos
GRUPO DE PROCESOS	Administrar la seguridad y los riesgos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPÓSITO

Diseño y administración de instalaciones físicas para la protección de los recursos de TI (equipos y personal). Incluye la definición de requerimientos de sitios físicos, la seleccción de instalaciones apropiadas, el monitoreo de condiciones ambientales y la administración del acceso físico.

ALCANCE

Todos los activos de información físicos de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCION

Procedimiento encargado de todas las actividades involucradas en la adecuada administración de la seguridad física de los recursos de hardware y comunicaciones de la plataforma de tecnología del Centro de Datos.

REGISTROS

Bitácora de acceso físico al Centro de Datos	
Bitácora de resultados de pruebas	

INDICADORES

De metas	De desempeño
# de incidentes causados por fallas o violaciones a la seguridad física	Frecuencia de las revisiones y evaluaciones de riesgo físico

VIGENCIA

Inicio		Fin	
Revisión			

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Administrar el ambiente físico del Centro de Datos**

Ir al Índice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-04-02-01	**Otorgamiento de acceso físico**	Recibir un **Requerimiento de acceso físico** al Centro de Datos				●				Jefe de la Oficina Informática
		Autorizar el acceso físico indicando la fecha de inicio y la vigencia		●						Jefe de la Oficina Informática
		Si el acceso físico es para personal interno de la oficina informática			●					
		Configurar las condiciones de acceso en el sistema de control de acceso físico		●						Especialista de Infraestructura
		Entregar tarjeta de proximidad configurada al usuario		●						Especialista de Infraestructura
PR-04-02-02	**Control de acceso físico**	Identificar al personal que quiere acceder al ambiente del Centro de Datos		●						
		Si es personal interno de la oficina informática			●					
		Verificar el uso adecuado de la tarjeta de proximidad para acceder al ambiente		●						Especialista de Infraestructura
		Caso contrario			●					
		Registrar al visitante en el registro de visitas antes del ingreso al ambiente		●				Bitácora de acceso físico al Centro de Datos		Especialista de Infraestructura
PR-04-02-03	**Autorización de un nuevo recurso de tratamiento de la información**	Recibir un **Requerimiento de acceso de un nuevo recurso de tratamiento de información** al Centro de Datos				●				Especialista de Infraestructura
		Autorizar el acceso asegurando que se cumplan con las políticas y requisitos de seguridad correspondientes		●						Jefe de la Oficina Informática, Oficial de seguridad
		Si el acceso es debidamente autorizado			●					
		Comprobar que el hardware y el software son compatibles con los demás dispositivos del sistema en producción		●						Especialista de Infraestructura
		Registrar el ingreso del nuevo recurso de tratamiento de información					●	Control de activos de tratamiento de información		
		Caso contrario			●					
		Comunicar la cancelación de la atención		●						Especialista de Infraestructura

0107 -2008-ED

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-04-03
PROCESO	Evaluar y administrar riesgos de TI
GRUPO DE PROCESOS	Administrar la seguridad y los riesgos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPÓSITO

Crear y mantener un marco de administración del riesgo, documentando los niveles acordados de riesgos de TI y las estrategias de mitigación. Cualquier impacto potencial en las metas causada por un evento no planificado debe ser identificado, analizado y evaluado. Los resultados deben ser expresados en términos financieros entendibles para informar a la dirección.

ALCANCE

Todos los riesgos que puedan afectar los activos de información más importantes incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL	
Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

#	Descripción	Tipo	Fecha
1	Documentación inicial del procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Índice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en asegurar una adecuada identificación de riesgos, así como la definición de planes de acción apropiados que permitan mitigarlos.

REGISTROS

Marco de evaluación de riesgos	Documento de clasificación de activos
Análisis de Riesgo	
Plan de Remediación de Riesgos	

INDICADORES

De metas	De desempeño
% de riesgos críticos identificados con un plan de acción elaborado	% de planes de acción de administración de riesgos aprobados para su implantación

VIGENCIA

Inicio		Fin	
Revisión			

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Evaluar y administrar riesgos de TI**

Ir al Indice
Ir a la Ficha del proceso

NÚMERO DE PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-04-03-01	**Identificación de Riesgos**	Revisar la clasificación para los riesgos en el **Marco de Evaluación de Riesgos**				●				Responsable de Infraestructura
		Identificar los riesgos que pueden afectar a la confidencialidad, integridad y/o disponibilidad de la información.					●	Análisis de Riesgo		
		Por cada riesgo identificado	●							
		Clasificar el riesgo según la clasifición definida					●	Análisis de Riesgo		Responsable de Infraestructura
PR-04-03-02	**Evaluación de Riesgos**	Revisar los riesgos identificados en el documento de **Análisis de Riesgo**				●				
		Por cada riesgo identificado	●							
		Identificar las ubicaciones de TI que pueden verse afectadas					●	Análisis de Riesgo		Responsable de Infraestructura
		Asignar un valor de probabilidad de ocurrencia					●	Análisis de Riesgo		Responsable de Infraestructura
		Asignar un valor de impacto y estado de atención					●	Análisis de Riesgo		Responsable de Infraestructura
		Detallar los servicios y/o sistemas de aplicación afectados					●	Análisis de Riesgo		Responsable de Infraestructura
		Describir las consecuencias asignadas a cada riesgo					●	Análisis de Riesgo		Responsable de Infraestructura
		Revisar la evaluación de riesgos asignada		●						Jefe de la Oficina Informática
PR-04-03-03	**Definición de Estrategia de Mitigación de Riesgos**	Revisar los riesgos identificados, las probabilidades y los impactos asignados en el documento de **Análisis de Riesgo**				●				Responsable de Infraestructura
		Por cada riesgo identificado	●							
		Detallar controles mitigantes disponibles					●	Análisis de Riesgo		Responsable de Infraestructura
		Detallar controles mitigantes propuestos					●	Análisis de Riesgo		Responsable de Infraestructura
		Incluir los controles mitigantes propuestos en un plan de mitigación					●	Plan de Reducción de Riesgos		Responsable de Infraestructura
		Revisar la estrategia de mitigación de riesgos existente		●						Jefe de la Oficina Informática
		Revisar la estrategia de mitigación de riesgos propuesta		●						Jefe de la Oficina Informática
PR-04-03-04	**Monitoreo de Estrategia de Mitigación de Riesgos**	Revisar los riesgos que poseen una estrategia de mitigación propuesta en el **Plan de Reducción de Riesgos**				●				Responsable de Infraestructura
		Por cada riesgo identificado	●							
		Identificar los controles mitigrantes propuestos					●	Plan de Reducción de Riesgos		Responsable de Infraestructura
		Por cada control mitigante propuesto	●							
		Si el control mitigante planea implementarse en el periodo			●					
		Verificar el estado de implementación		●						Responsable de Infraestructura
		Registrar el estado de implementación					●	Plan de Reducción de Riesgos		Responsable de Infraestructura
		Caso Contrario			●					
		Registrar el periodo previsto para la implementación					●	Plan de Reducción de Riesgos		Responsable de Infraestructura
		Revisar el estado de la estrategia de mitigación de riesgos propuesta		●						Jefe de la Oficina Informática
PR-04-03-05	**Clasificación de activos de la información**	Identificar los recursos de TI que constituyen los activos de información según el inventario de activos de información levantado				●				Especialista de Infraestructura
		Por cada activo de información identificado	●							
		Verificar el nivel de riesgo tecnológico asociado por aplicación (Ver informe de Riesgo Tecnológico)				●				Especialista de Infraestructura
		Clasificar los activos de información según el nivel de riesgo asociado en base a la evaluación de la confidencialidad, integridad y disponibilidad.				●				Responsable de Infraestructura
		Registrar la clasificación del riesgo del activo de información					●	Documento de clasificación de activos de la información		Especialista de Infraestructura
PR-04-03-06	**Marcado de la información**	Recibir un requerimiento para Marcado de Información		●						Especialista de Infraestructura
		Si el activo es digital			●					
		Clasificar al activo de información como crítica, sensible o pública en el inventario de activos de información				●		Inventario de activos de información		Especialista de Infraestructura, Oficial de Seguridad
		Por cada activo de información registrar la función (Copia, almacenamiento, destrucción)	●							Especialista de Infraestructura
		Caso contrario si el activo es físico (Cintas, discos, CDs, Casetes)			●					
		Registrar por medio de etiquetas físicas la clasificación de la información (Crítica, sensible) y la función del misma (Copia, almacenamiento, destrucción)				●				Especialista de Infraestructura, Oficial de Seguridad

0107 -2008-ED

Secretaría de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-04-04
PROCESO	Administrar incidencias de seguridad
GRUPO DE PROCESOS	Administrar la seguridad y los riesgos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Crear y mantener un marco de administración de incidencias de seguridad, documentando la ocurrencia de TI y las estrategias de mitigación ante cualquier vulnerabilidad detectada. Cualquierincidencia causada por un evento debe ser identificado, analizado y evaluado. Los resultados deben ser expresados en términos financieros entendibles para

ALCANCE

Todas las incidencias que puedan afectar los activos de información más importantes incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL	
Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del prodedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en asegurar una adecuada identificación de las incidencias de seguridad así como registro de acción apropiados que permitan mitigarlos.

REGISTROS

Bitácora de incidencias de seguridad	
Registro en Sistema de HelpDesk	

INDICADORES

De metas	De desempeño
% de incidentes identificados a tiempo de acuerdo a los niveles de servicio vs total de incidentes idntificados.	% de incidentes resueltos vs incidentes no resueltos en el tiempo especificado en los acuerdos de niveles de servicio vs total de incidentes identificados

VIGENCIA

Inicio		Fin	
Revisión			

0107 -2008-ED

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Administrar incidencias de seguridad**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-04-04-01	**Respuesta ante incidencias de seguridad**	Comunicar las incidencias de seguridad a HelpDesk				●				Áreas usuarias
		Identificar el incidente				●				HelpDesk
		Registrar las incidencia de seguridad					●	Bitácora de incidencia de seguridad		Especialista de Infraestructura
		Identificar alternativa de solución al incidente				●				Especialista de Infraestructura
		Implementar la mejor alternativa de solución identificada				●				Especialista de Infraestructura
		Si la alternativa de solución involucra labores de mantenimiento			●					
		Coordinar la ejecución de labores de mantenimiento		●				Ver Procedimiento PR-05-05-02		
		Si el incidente afectó de manera importante la plataforma de TI			●					
		Documentar un informe del incidente, incluyendo la causa y la solución implementada					●	Bitácora de incidencias de seguridad		Especialista de Infraestructura
		Validar el informe realizado		●						Responsable de Infraestructura
		Revisar el informe realizado		●						Jefe de la Oficina Informática
PR-04-04-02	**Administración de incidentes de seguridad**	Recibir / Detectar un incidencia de seguridad				●		Monitoreo de Log, registros de auditoria		Especialista de Infraestructura
		Identificar alternativas de solución al incidente		●						Especialista de Infraestructura
		Si el problema esta asociado a temas de software base			●					
		Asignar un técnico de HelpDesk para la atención					●	Registro en Sistema de HelpDesk		Especialista de Infraestructura
		Implementar la mejor alternativa de solución identificada		●						Especialista de Infraestructura
		Registrar la causa y la solución identificada para el problema					●	Bitácora de incidencias de seguridad		Especialista de Infraestructura
		Actualizar el estado de la incidencia					●	Bitácora de incidencias de seguridad		Especialista de Infraestructura
		Revisar el adecuada cierre de la incidencia		●						Especialista de Infraestructura
		Caso Contrario si esta asociado a temas de hardware			●					
		Escalar solución al área de Recupero de Hardware		●						Especialista de Infraestructura
		Caso Contrario si esta asociado a temas de sistemas			●					
		Escalar solución al área de Sistemas de Información		●						Especialista de Infraestructura

Secretaría de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-05-01
PROCESO	Planificar y administrar la capacidad
GRUPO DE PROCESOS	Administrar la operación del ambiente de TI
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPÓSITO

Evaluar los requerimientos de capacidad del ambiente de TI a corto y largo plazo, tales como almacenamiento, ancho de banda, memoria y desempeño del CPU.

ALCANCE

Todos los activos de información de hardware, software base y/o comunicaciones incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por:	
Aprobado por:	

HISTORIAL

No.	Descripción	Tipo	Fecha
1	Documentación inicial del	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en asegurar la disponibilidad y adecuada capacidad sobre los recursos de TI (hardware, software base y comunicaciones).

REGISTROS

Bitácora de incidencias de seguridad	

INDICADORES

De metas	De desempeño
Tasa de falla de transacciones	Frecuencia de los pronósticos de desempeño y capacidad

VIGENCIA

Inicio		Fin	
Revisión			

Mi[illegible]o de Educación

DIAGRAMA DE PROCEDIMIENTO
Proceso: **Administrar la operación del ambiente de TI**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-05-01-01	**Monitoreo de la Disponibilidad**	Identificar los activos de información mas críticos en base a la experiencia e impacto en la disponibilidad de servicios según el **Análisis de Riesgos**				●				Especialista de Infraestructura
		Por cada activo de información identificado	●							
		Verificar que el activo de información se encuentre brindando servicio		●						Especialista de Infraestructura
		Si el activo no encuentra brindando servicio			●					
		Reportar un incidente por la indisponibilidad del servicio		●						Especialista de Infraestructura
PR-05-01-02	**Monitoreo de la Capacidad**	Identificar los activos de información mas críticos en base a la experiencia e impacto en la capacidad según el **Análisis de Riesgos**				●				Especialista de Infraestructura
		Por cada activo de información identificado	●							
		Definir los niveles de capacidad óptimos para desempeño del activo		●						Responsable de Infraestructura
		Medir la demanda actual del activo		●						Especialista de Infraestructura
		Comparar la capacidad óptima contra la demanda actual		●						Especialista de Infraestructura
		Si la demanda actual es mayor a la capacidad óptima			●					
		Identificar alternativa de solución		●						Especialista de Infraestructura
		Implementar la mejor alternativa identificada según **requerimientos de capacidad/disponibilidad**				●				Especialista de Infraestructura
		Si la ampliación de capacidad implica un cambio en la plataforma de TI			●					
		Implementar el cambio en la plataforma de TI		●				Ver Procedimiento PR-05-05-01		
PR-05-01-03	**Monitoreo de Logs de incidencias**	Revisar los registros de monitoreo				●				Especialista de Infraestructura
		Por cada registro de error identificado	●							
		Evaluar el impacto en la confidencilidad, integridad y disponibilidad que representa				●				Especialista de Infraestructura
		Registrar la incidencia de seguridad detectada					●	Bitácora de incidencias de seguridad		Especialista de Infraestructura

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-05-02
PROCESO	Desarrollar y administrar el Plan de Contingencia del Centro de Datos
GRUPO DE PROCESOS	Administrar la operación del ambiente de TI
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPÓSITO

Desarrollar y probar un Plan de Contingencias para el Centro de Datos. Asegurar pérdidas mínimas de productividad debido a caídas de los sistemas. Adoptar un enfoque sistemático en caso se produzcan fallas con el fin de asegurar que los servicios de producción de TI requeridos son recuperados rápidamente.

ALCANCE

Todos los activos de información incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en asegurar la disponibilidad de información, ante eventos externos que puedan afectar el Centro de Datos.

REGISTROS

Plan de Acción por Sistema	
Procedimiento de Instalación	
Plan de Contingencia	

INDICADORES

De metas	De desempeño
Frecuencia en la interrupción de servicios de sistemas críticos	Frecuencia de la revisión del plan de continuidad de TI

VIGENCIA

Inicio		Fin	
Revisión			

0107 -2008-ED

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Desarrollar y administrar el Plan de Contingencia del Centro de Datos**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-05-02-01	**Elaboración del plan de contingencia**	Identificar y evaluar los riesgos de tecnología de información que afecten al Centro de Datos				●		Ver Procedimiento PR-04-03-01		
		Revisar la evaluación de riesgos de realizada en el **Análisis de Riesgos**				●				Responsable de Infraestructura
		Revisar los controles mitigantes existentes documentados en el **Plan de Reducción de Riesgos**				●				Responsable de Infraestructura
		Identificar los servicios y/o sistemas de aplicación afectados según el **Análisis de Riesgos**				●				Responsable de Infraestructura
		Por cada servicio o sistema de información identificado	●							
		Registrar el nombre, el administrador del mismo, el dueño y las áreas que lo utilizan					●	Plan de Acción por Sistema		Responsable de Infraestructura
		Registrar el tipo de base de datos, el volúmen actual, la tasa de crecimiento y el volumen requerido para efectos de recuperación					●	Plan de Acción por Sistema		Responsable de Infraestructura
		Registrar el tiempo máximo de recuperación y su nivel de importancia					●	Plan de Acción por Sistema		Responsable de Infraestructura
		Definir el equipo necesario y las responsables de la recuperación					●	Plan de Acción por Sistema		Responsable de Infraestructura
		Documentar un procedimiento de instalación para efectos de recuperación					●	Procedimiento de Instalación de Servicio		Responsable de Infraestructura
		Revisar los planes de acción definidos		●						Jefe de Oficina Informática
		Documentar el Plan de Contingencia					●	Plan de Contingencia		Responsable de Infraestructura
		Revisar el Plan de Contingencia		●						Jefe de Oficina Informática
		Aprobar el Plan de Contingencia		●						Secretario de Planificación y Estrategia
PR-05-02-02	**Implementación del plan de contingencia**	Revisar los **Plan de Acción** definidos para los servicios y/o sistemas de aplicación según				●				Responsable de Infraestructura
		Implementar estrategias de recuperación y custodia para los servicios y/o sistemas de aplicación acorde al plan		●				Ver Procedimiento PR-05-03-01		
PR-05-02-03	**Prueba al plan de contingencia**	Definir el propósito de la prueba.				●				Comité de Pruebas / Comité de Mantenimiento
		Definir la prueba.				●				Comité de Pruebas
		Designar el equipo de prueba.				●				Comité de Pruebas
		Estructurar los aspectos a probar.				●				Comité de Pruebas
		Ejecutar las pruebas.		●						Comité de Recuperación
		Analizar los resultados y modificar el Plan de Recuperación de Desastres TI, si fuese necesario				●				Comité de Pruebas / Comité de Mantenimiento
		Supervisar y dar apoyo durante la ejecución de las pruebas y garantizar la ejecución de las mismas en los tiempos planeados.				●				Comité de Pruebas
		Apoyar al personal de las líneas de negocio involucradas en la ejecución de las pruebas.				●				
		Registrar los resultados de las pruebas y participar activamente en las pruebas a los sistemas de aplicación críticos.					●			

0107 "2008-ED

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-05-03
PROCESO	Desarrollar y administrar la protección de la información
GRUPO DE PROCESOS	Administrar la operación del ambiente de TI
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Diseñar, implementar y probar el respaldo y/o la restauración de la información. Definir claramente una metodología para procedimientos oportunos de respaldo y restauración, y almacenamiento de medios fuera de sitio.

ALCANCE

Todos los activos de información incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del proceso	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en asegurar la disponibilidad de información, mediante adecuados procedimientos de respaldo, restauración y custodia.

REGISTROS

Requerimiento de respaldo	Pruebas de Restore
Plan de Respaldo	Comprobante de Servicio
Catálogo de Respaldo	
Registro Diario de Cintas	

INDICADORES

De metas	De desempeño
# de incidentes de falta de servicio o de integridad de información causados por falta de capacidad de almacenamiento	Frecuencia de las pruebas de los medios de respaldo

VIGENCIA

Inicio		Fin	
Revisión			

Ministerio de Ed

DIAGRAMA DE PROCEDIMIENTO
PROCESO: Desarrollar y administrar la protección de la información

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-05-03-01	**Definición de Plan de Respaldo**	Identificar los activos de información a respaldar apoyándose en el **Informe de Evaluación del Ambiente**				●				Especialista de Infraestructura
		Por cada activo de información a respaldar	●							
		Especificar ubicación, frecuencia de respaldo/restauración, tiempos de retención/disponibilidad y tasa de crecimiento.					●	Requerimiento de Respaldo		Administrador de Sistemas de Información
		Incluir información del activo en el Plan de Respaldo					●	Plan de Respaldo		Especialista de Infraestructura
		Especificar tiempo y medio de retención					●	Plan de Respaldo		Especialista de Infraestructura
		Validar Plan de Respaldo con los Administradores de Sistemas de Información y Oficial de Seguridad (Registros de auditoria)		●						Especialista de Infraestructura
		Aprobar Plan de Respaldo		●						Responsable de Infraestructura
PR-05-03-02	**Ejecución de Plan de Respaldo**	Revisar **Catálogo de Respaldo**				●				Especialista de Infraestructura
		Por cada activo de información a respaldar	●							
		Si el respaldo es automatizado			●					
		Verificar el resultado del respaldo en el log de resultados		●						Especialista de Infraestructura
		Caso Contrario			●					
		Realizar el respaldo manualmente		●						Especialista de Infraestructura
		Registrar el resultado del respaldo					●	Registro Diario de Cintas		Especialista de Infraestructura
PR-05-03-03	**Ejecución de Plan de Restauración**	Identificar **Requerimiento de restauración**				●				Especialista de Infraestructura
		Si es una restauración programada			●					Especialista de Infraestructura
		Revisar el **Plan de Respaldo**				●				Especialista de Infraestructura
		Por cada activo de información a restaurar	●							
		Realizar actividades de restauración		●						Especialista de Infraestructura
		Caso Contrario			●					
		Revisar adecuada autorización en el **Requerimiento de restauración**				●				Especialista de Infraestructura
		Realizar actividades de restauración		●						Especialista de Infraestructura
		Registrar el resultado de la restauración					●	Pruebas de Restore		Especialista de Infraestructura
PR-05-03-04	**Custodia Externa de Respaldos**	Preparar cintas a remitir a custodia al proveedor externo				●				Especialista de Infraestructura
		Recibir cintas devueltas por el proveedor externo y Comprobante de Servicio - Division de Documentos				●				
		Registrar las cintas entregadas en custodia al proveedor externo					●	Comprobante de Servicio - Division de Documentos		Especialista de Infraestructura
		Requerir VoBo de Agente de Custodia					●	Comprobante de Servicio - Division de Documentos	Agente Autorizado Hermes	Especialista de Infraestructura
		Registrar VoBo de la entrega de cintas					●	Comprobante de Servicio - Division de Documentos	Firma del Remitente o Consignador	Especialista de Infraestructura
PR-05-03-05	**Custodia Interna de Respaldos**	Preparar cintas a entregar a custodia interna		●						Especialista de Infraestructura
		Guardar las cintas en el lugar de seguridad para respaldos de información		●						
		Registrar la cinta almacenada internamente					●	Bitácora		
				●						Especialista de Infraestructura
PR-05-03-06	**Prueba de respaldo de información.**	Seleccionar con una frecuencia mensual una cinta de Backup por cada sistema de información				●				Especialista de Infraestructura
		Realizar la restauración de las cintas		●						Especialista de Infraestructura
		Verificar la efectiva restauración de la infomración				●				Especialista de Infraestructura
		Documentar los resiutados de la pruebas de la restauración					●	Informe de pruebas de restauración de la		Especialista de Infraestructura
PR-05-03-07	**Definición de Catálogo de Respaldo**	Contrastar el **Plan de Respaldo** con los recursos disponibles de la plataforma de TI				●				Especialista de Infraestructura
		Agrupar tareas de respaldo en Grupo de Respaldo		●						Especialista de Infraestructura
		Asignar Grupos de Respaldo a Catálogo de Respaldo					●	Catalogo de Respaldo		Especialista de Infraestructura
		Verificar alineación de los **Catálogos de Respaldo** y el **Plan de Respaldo**		●						Especialista de Infraestructura
		Aprobar Catálogo de Respaldo		●						Especialista de Infraestructura
		Configurar respaldos en la herramienta automatizada de respaldo		●						Especialista de Infraestructura

0107 -2008-ED

Secretaría de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-05-04
PROCESO	Resolver problemas de los sistemas
GRUPO DE PROCESOS	Administrar la operación del ambiente de TI
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Proveer soporte adecuado y suficiente a sistemas para asegurar un tiempo mínimo entre la identificación y la resolución de problemas.

ALCANCE

Todos los activos de información incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en la adecuada identificación, seguimiento y resolución de los incidentes de operación de la plataforma de TI.

REGISTROS

Informe de Incidente	
Registro en bitácora de Incidenicias	

INDICADORES

De metas	De desempeño
% de problemas identificados y rastreados a tiempo de acuerdo a los niveles de servicios acordados vs total de problemas identificados.	% de problemas resueltos a tiempo de acuerdo a los niveles de servicios acordados vs total de problemas identificados.

VIGENCIA

Inicio		Fin	
Revisión			

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Resolver problemas de los sistemas**

Ir al Indice
Ir a la Ficha del proceso

NO. PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-05-04-01	**Administración de incidentes de operación**	Identificar el incidente		●						Especialista de Infraestructura
		Identificar alternativa de solución al incidente		●						Especialista de Infraestructura
		Implementar la mejor alternativa de solución identificada		●						Especialista de Infraestructura
		Si la alternativa de solución involucra labores de mantenimiento			●					
		Coordinar la ejecución de labores de mantenimiento		●				Ver Procedimiento PR-05-05-02		
		Si el incidente afectó de manera importante la plataforma de TI			●					
		Documentar un informe del incidente, incluyendo la causa y la solución implementada					●	Informe de Incidente / Registro en bitácora de		Especialista de Infraestructura
		Validar el informe realizado		●						Responsable de Infraestructura
		Revisar el informe realizado		●						Jefe de la Oficina Informática
PR-05-04-02	**Administración de incidentes de usuario**	Atender el incidente a través de la mesa de ayuda		●				Ver Procedimiento PR-06-03-01		

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-05-05
PROCESO	Mejorar y mantener los recursos de TI
GRUPO DE PROCESOS	Administrar la operación del ambiente de TI
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPÓSITO

Implementar mejoras y cambios de versiones oportunos para el hardware y software. Asegurar que el desempeño de los sistemas no es degradado significativamente como resultado de estas mejoras.

ALCANCE

Todos los activos de información de hardware, software base y/o comunicaciones incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en asegurar un adecuado control de cambios sobre los recursos de TI (hardware, software base y comunicaciones), así como un adecuado mantenimiento de dichos recursos.

REGISTROS

Protocolo de Revisión	
Informe Técnico	
Informe de Mantenimiento	
Correo	

INDICADORES

De metas	De desempeño
# de cambios que no se rastrean formalmente o no se reportan o no se autorizan	% de cambios que siguen procesos de control de cambio formales

VIGENCIA

Inicio		Fin	
Revisión			

0107 -2008-ED

Ministerio de Edu

DIAGRAMA DE PROCESO

PROCESO **Mejorar y mantener los recursos de TI**

Ir al Indice
Ir a la Ficha del proceso

No. PROCEDIMIENTO	NOMBRE DEL PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-05-05-01	**Control de cambios sobre recursos de TI**	Identificar el activo de información sobre el cúal se realizará el cambio en los **Requerimientos de cambio**				●				Especialista de Infraestructura
		Asignar un responsable por la administración del cambio		●						Responsable de Infraestructura
		Evaluar el impacto del cambio en la plataforma de TI		●						Especialista de Infraestructura
		Registrar el requerimiento de cambio					●	Registro de control de Requerimientos		
		Si el cambio puede afectar la disponibilidad de un servicio o sistema de aplicación			◆					
		Identificar a los usuarios afectados por el cambio		●						Especialista de Infraestructura
		Comunicar de la indisponibilidad a los usuarios					●	Correo		Especialista de Infraestructura
		Si no hay impedimento por parte de los usuarios del activo de información			◆					
		Ejecutar el cambio en ambiente de prueba		●						Especialista de Infraestructura
		Si es un proveedor externo el que ejecuta el cambio			◆					Especialista de Infraestructura
		Documentar las pruebas realizadas					●	Protocolo de Revisión		Especialista de Infraestructura
		Revisar los resultados de las pruebas realizadas por el proveedor		●						Responsable de Infraestructura
		Si los resultados se consideran satisfactorios			◆					
		Elaborar un informe técnico por la conformidad del cambio					●	Informe Técnico		Especialista de Infraestructura
		Revisar el informe técnico		●						Responsable de Infraestructura
		Ejecutar el cambio en ambiente de producción		●						Especialista de Infraestructura
		Caso contrario			◆					
		Elevar un informe con los requerimientos de mejora a corregir		●						Responsable de Infraestructura
		Elevar un informe con los requerimientos de mejora al proveedor		●						Jefe de Oficina Informática
		Caso contrario			◆					
		Documentar las pruebas realizadas					●	Registro de control de Requerimientos		
		Probar el adecuado funcionamiento del activo despues del cambio		●						
		Si las pruebas fueron satisfactorias			◆					
		Ejecutar el cambio en producción		●						
		Registrar el resultado del cambio a producción					●	Registro de control de Requerimientos		
		Caso contrario			◆					
		Registrar el requerimiento de cambio como inadecuado					●	Registro de control de Requerimientos		
PR-05-05-02	**Mantenimiento preventivo/correctivo**	Identificar el activo de información afecto a mantenimiento según los **Requerimientos de mantenimiento**				●				Especialista de Infraestructura
		Si es un mantenimiento preventivo programado			◆					
		Validar que la fecha esta alineada con el **Plan de Mantenimiento**				●				Especialista de Infraestructura
		Caso Contrario			◆					
		Revisar adecuada autorización del **requerimiento de mantenimiento**				●				Especialista de Infraestructura
		Si el activo de información aún se encuentra en periodo de garantía			◆					
		Coordinar servicios de mantenimiento con el proveedor de compra					●	Correo		Especialista de Infraestructura
		Caso Contrario, Si se cuenta con contrato de servicios de mantenimiento para el activo de información			◆					
		Coordinar servicios de mantenimiento con el proveedor de mantenimiento					●	Correo		Especialista de Infraestructura
		Definir una fecha para la ejecución del mantenimiento					●	Correo		Especialista de Infraestructura
		Si el mantenimiento puede afectar la disponibilidad de un servicio o sistema de aplicación			◆					
		Identificar a los usuarios afectados por el cambio		●						Especialista de Infraestructura
		Comunicar de la indisponibilidad a los usuarios					●	Correo		Especialista de Infraestructura
		Si no hay impedimento por parte de los usuarios del activo de información			◆					
		Ejecutar el mantenimiento		●						Proveedor
		Documentar actividades y pruebas realizadas					●	Informe de Mantenimiento		Proveedor
		Revisar informe de mantenimiento		●						Especialista de Infraestructura
PR-05-05-03	**Recolección de evidencia**	Activar los registro de auditoría de los principales sistemas y subsistemas		●						Especialista de Infraestructura
		Revisar el adecuado registro de fuentes (pistas de auditoría, Logs de aplicaciones, etc)				●				Especialista de Infraestructura
		Validar el adecuado respaldo de los registros de auditoría				●		Ver Procedimiento PR-05-03-01		Oficial de seguridad

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-05-06
PROCESO	Administrar los activos de TI
GRUPO DE PROCESOS	Administrar la operación del ambiente de TI
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Mantener un inventario de los activos de TI. Asignar códigos de idenitificación únicos a los activos. Manejar/seguir los reemplazos de hardware, software, bases de datos, entre otros.

ALCANCE

Todos los activos de información incluidos dentro de la plataforma de tecnología de información del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTOS

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCION

Procedimento encargado de todas las actividades involucradas en la adecuada identificación de los activos de información de TI que se encuentren en el Centro de Datos.

REGISTROS

Inventario de Activos de TI	

INDICADORES

De metas	De desempeño
	% de activos que se encuentran en el inventario vs cantidad de activos totales.

VIGENCIA

Inicio		Fin	
Revisión			

0107 -2008-ED

Mi[illegible]o
de[illegible]ción

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Administrar los activos de TI**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-05-06-01	**Elaboración Inventario de activos de TI**	Identificar los recursos de TI que constituyen activos de información según **información levantada**				●				Especialista de Infraestructura
		Por cada activo de información identificado	●							
		Identificar el tipo de activo de información según **información levantada**				●				Especialista de Infraestructura
		Ingresar la información del activo de información en el inventario corresponspondiente al tipo de activo					●	Inventario de Activos de TI		Especialista de Infraestructura
		Revisar el inventario de Activos		●						Responsable de Infraestructura
PR-05-06-02	**Actualización inventario de activos de TI**	Identificar los activos de información que han sufrido cambios (alta, modificación y/o baja) según **información levantada**				●				Especialista de Infraestructura
		Por cada activo de información identificado	●							
		Identificar el tipo de activo de información según **información levantada**				●				Especialista de Infraestructura
		Actualizar la información del activo de información en el inventario corresponspondiente al tipo de activo					●	Inventario de Activos de TI		Especialista de Infraestructura
		Revisar el inventario de activos		●						Responsable de Infraestructura

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-06-01
PROCESO	Capacitar a los usuarios finales y monitorear su progreso
GRUPO DE PROCESOS	Brindar soporte y capacitar a los usuarios
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Determinar la infraestructura y los recursos requeridos para soportar distintos tipos de programas de capacitación. Proveer entrenamiento e información a los usuarios. Capturar los resultados y mantener un seguimiento del entrenamiento ofrecido.

ALCANCE

Todos los requerimientos de capacitación alcanzados por todas las áreas de negovio del Ministerio.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTOS

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en la capacitación a los usuarios sobre el uso de los principales activos de información.

REGISTROS

Programación de curso	
Hoja de Asistencia	
Hoja de Evaluaciones	
Constancia de capacitación	

INDICADORES

De metas	De desempeño
% de satisfacción de los interesados a quienes se les brindó capacitación	Lapso de tiempo entre la identificación de la necesidad de capacitación y la impartición de la misma

VIGENCIA

Inicio		Fin	
Revisión			

0107 -2008-ED

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Capacitar a los usuarios finales y monitorear su progreso**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-06-01-01	**Brindar capacitación**	Si la capacitación proviene de un requerimiento de capacitación			●					
		Verificar la adecuada autorización del **Requerimiento de capacitación**				●				Responsable de Capacitación
		Caso Contrario			●					
		Identificar requerimientos de capacitación en base a **información histórica de Help Desk**				●				Responsable de Capacitación
		Elaborar programación de la capacitación al personal involucrado					●	Programación de curso		Jefe de Oficina Informática
		Recibir confirmaciones de los usuarios a capacitar		●						Responsable de Capacitación
		Preparar el material de capacitación		●						Responsable de Capacitación
		Brindar capacitación a los usuarios					●	Hoja de Asistencia		Responsable de Capacitación
		Evaluar el cumplimiento de los objetivos de la capacitación		●						Responsable de Capacitación
		Registrar los resultados de la evaluaciones					●	Hoja de Evaluaciones		Responsable de Capacitación
		Emitir constancias de capacitación					●	Constancia de Capacitación		Responsable de Capacitación
		Enviar las constancias de capacitación al personal involucrado		●						Jefe de Oficina Informática

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-06-02
PROCESO	Medir la satisfacción del usuario
GRUPO DE PROCESOS	Brindar soporte y capacitar a los usuarios
PROPIETARIO	Responsable de Infraestructura Tecnológica

DIAGNOSTICO

Medir la satisfacción de los usuarios sobre:
- el servicio de Help Desk.
- los servicios de capacitación.
- las actividades de restauración y de manejo de contingencias.

ALCANCE

Todos las atenciones realizadas por los servicios de Help Desk de la Oficina de Informática.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en la obtención de una medición de la satisfacción de usuario sobre el servicio brindado por Help Desk.

REGISTROS

Encuesta de Satisfacción	

INDICADORES

De metas	De desempeño
% usuarios encuestados vs usuarios objetivos.	Cantidad o dudas de consultas sin resolver % de incidentes abiertos vs el total de incidentes

VIGENCIA

Inicio		Fin	
Revisión			

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Medir la satisfacción del usuario**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-06-02-01	**Elaboración de Encuestas Aleatorias**	Revisar la **información histórica** de requerimientos de usuario en el Sistema de HelpDesk				●				Responsable de HelpDesk
		Elegir una muestra de requerimientos de usuario atendidos					●	Encuesta de Satisfacción	Planificación	Responsable de HelpDesk
		Por cada requerimiento elegido	●							Técnico de HelpDesk
		Realizar una encuesta telefónica para obtener la opinión del usuario solicitante sobre el servicio brindado		●						Técnico de HelpDesk
		Consignar la opinión del usuario					●	Encuesta de Satisfacción		Técnico de HelpDesk
		Ponderar los resultados de todos los requerimientos					●	Encuesta de Satisfacción		Técnico de HelpDesk
		Revisar la encuesta realizada		●						Responsable de HelpDesk
PR-06-02-02	**Elaboración de Encuestas en Capacitaciones**	Revisar la información de los asistentes y el tipo de capacitación en la **Programación de Curso de Capacitación**				●				Responsable de Capacitación
		Por cada asistente a la capacitación	●							
		Realizar una encuesta escrita para obtener la opinión sobre el servicio brindado de capacitación		●						Responsable de Capacitación
		Consignar la opinión del usuario					●	Encuesta de Satisfacción		Responsable de Capacitación
		Ponderar los resultados de todos los requerimientos					●	Encuesta de Satisfacción		Responsable de Capacitación
		Revisar la encuesta realizada		●						Responsable de HelpDesk

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-06-03
PROCESO	Resolver problemas de usuarios de TI
GRUPO DE PROCESOS	Brindar soporte y capacitar a los usuarios
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Resolver todos los problemas de los usuarios o redireccionar los problemas a la persona adecuada para su resolución. Definir los mecanismos de escalamiento y comunicación adecuados para la resolución de problemas.

ALCANCE

Todos las solicitudes de usuario cursadas a la Oficina de Informática por los usuarios de los activos de información del Centro de Datos.

CONTROL	
Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCION

Procedimiento encargado de todas las actividades involucradas en la adecuada identificación, seguimiento y resolución de los incidentes de usuario informados al área de HelpDesk.

REGISTROS

Registro en Sistema de HelpDesk	

INDICADORES

De metas	De desempeño
Velocidad promedio para responder a peticiones via teléfono y via web o e-mail.	# de llamadas atendidas por el personal de mesa de servicios por hora

VIGENCIA

Inicio		Fin	
Revisión			

0107 -2008-ED

Mi[illegible]o
de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Resolver problemas de usuarios de TI**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-06-03-01	**Administración de incidentes de usuario**	Recibir un **Requerimiento de atención de usuario**				●				Responsable de HelpDesk
		Identificar alternativas de solución al incidente		●						Responsable de HelpDesk
		Si el problema esta asociado a temas de software base			●					
		Asignar un técnico de HelpDesk para la atención					●	Registro en Sistema de HelpDesk		Responsable de HelpDesk
		Implementar la mejor alternativa de solución identificada		●						Técnico de HelpDesk
		Registrar la causa y la solución identificada para el problema					●	Registro en Sistema de HelpDesk y/o Registro en Bitácora de Incidencias		Técnico de HelpDesk
		Actualizar el estado del requerimiento					●	Registro en Sistema de HelpDesk		Técnico de HelpDesk
		Revisar el adecuada cierre del requerimiento		●						Responsable de HelpDesk
		Caso Contrario si esta asociado a temas de hardware			●					
		Escalar solución al área de Recupero de Hardware		●						Técnico de HelpDesk
		Caso Contrario si esta asociado a temas de sistemas			●					
		Escalar solución al área de Sistemas de Información		●						Técnico de HelpDesk

Ministerio de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO **Administrar los recursos de Help Desk**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TÍTULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-06-04-01	**Seguimiento de Desempeño de Help Desk**	Revisar la **Información histórica** de requerimientos de usuario en Sistema de HelpDesk				●		Sistema de HelpDesk		Responsable de HelpDesk
		Agrupar la información por tipo de incidencia y por área					●	Informe de Desempeño de HelpDesk		Responsable de HelpDesk
		Incluir información de satisfacción de clientes		●				Ver Procedimiento PR-06-02-01		
		Identificar tendencias y plantear observaciones					●	Informe de Desempeño de HelpDesk		Responsable de HelpDesk
		Revisar el informe de desempeño		●						Responsable de Infraestructura

0107 -2008-ED

Ministerio de Educación

FICHA DE PROCEDIMIENTOS

IDENTIFICADOR	PR-07-01
PROCESO	Entrenar al personal del Centro de Datos
GRUPO DE PROCESOS	Administrar el Centro de Datos
PROPIETARIO	Responsable de Infraestructura Tecnológica

PROPOSITO

Entrenar al personal del Centro de Datos a través de cursos externos, seminarios y conferencias pertinentes. La unidad debe entrenar a su personal en tecnologías que se planean implementar para brindar soporte a sus planes de desarrollo.

ALCANCE

Todo el personal que realice labores relevantes para la operación del Centro de Datos.

CONTROL

Versión	1.0.0
Revisado por	
Aprobado por	

HISTORIAL

	Descripción	Tipo	Fecha
1	Documentación inicial del procedimiento	Creación	

DESCRIPCIÓN Y ELEMENTOS DEL PROCEDIMIENTO

Ir al Diagrama del Procedimiento
Ir al Indice

DESCRIPCIÓN

Procedimiento encargado de todas las actividades involucradas en asegurar una adecuada capacitación del personal; alineada a las habilidades requeridas para el cumplimiento de la estrategia de TI definida.

REGISTROS

Plan de Capacitación	
Requerimientos de capacitación	

INDICADORES

De metas	De desempeño
% de personal de TI que terminó de entrenamiento anual de TI	# promedio de dias de entrenamiento y desarrollo (incluyendo adiestramiento) por persona por año

VIGENCIA

Inicio		Fin	
Revisión			

Mi[illegible]
de Educación

DIAGRAMA DE PROCEDIMIENTO
PROCESO: **Entrenar al personal del Centro de Datos**

Ir al Indice
Ir a la Ficha del proceso

ID PROCEDIMIENTO	TITULO DE PROCEDIMIENTO	TAREA						REGISTRO	SECCIÓN DEL REGISTRO	RESPONSABLE TAREA
PR-07-01-01	**Elaborar Plan de Capacitación**	Identificar requerimientos de capacitación alineados a la estrategia de TI en el **Plan Estratégico de TI**				●				Responsable de Infraestructura
		Identificar los cursos tentativos a tomar		●						Responsable de Infraestructura
		Identificar el personal tentativo para tomar los cursos		●						Responsable de Infraestructura
		Definir un plan de capacitación de acuerdo al presupuesto disponible					●	Plan de Capacitación		Responsable de Infraestructura
		Aprobar el Plan de Capacitación		●						Jefe de la Oficina Informática
PR-07-01-02	**Capacitar al Personal**	Si el curso no esta dentro del Plan de Capacitación								
		Elaborar un Requerimiento de Capacitación			●					
		Aprobar Requerimiento de Capacitación				●		Requerimiento de capacitación		Responsable de Infraestructura
		Caso Contrario		●						Jefe de Oficina Informática
		Revisar el Plan para determinar el curso			●					
		Verificar la disponibilidad del personal que asistirá al curso				●		Plan de Capacitación		Responsable de Infraestructura
		Coordinar con el proveedor una fecha tentativa para el inicio del curso		●						Responsable de Infraestructura
		Coordinar la asistencia del personal al curso		●						Responsable de Infraestructura

0107 -2008-ED

Ministerio de Educación

Estándares de Seguridad de la Información

Versión 1
(Versión 1.0)

Enero 2008

Ministerio
de Educación

0107 -2008-ED

Ministerio de Educación	**DOCUMENTO:** ACTA DE REUNIÓN DEL COMITÉ EJECUTIVO DE SEGURIDAD DE INFORMACIÓN	
	CÓDIGO: DOC-001	**FECHA:**

1. Descripción General

Motivo:	
Lugar:	
Fecha / Hora:	DD/MM/AAAA HH:MM a.m.
Requerido por:	

2. Participantes de la reunión

Participantes:	**Hora Llegada**	**Asistió**	**Firma**
Participante 1	HH:MM a.m.	☐	
Participante 2	HH:MM a.m.	☐	
Participante 3	HH:MM a.m.	☐	

3. Agenda

Tema:	**Descripción:**	**Responsable:**
Tema 1	Tema 1	Participante 1
Tema 2	Tema 2	Participante 2
Tema 3	Tema 3	Participante 3

4. Acuerdos

Acuerdo:	**Descripción:**

5. Problemas y/o Riesgos Identificados

Descripción:	**Acción a tomar:**	**Responsable:**	**Fecha:**	**Estado:**
1.				

0107 -2008-ED

Ministerio de Educación	**DOCUMENTO:** ACTA DE REUNIÓN DEL COMITÉ OPERATIVO DE SEGURIDAD DE INFORMACIÓN	
	CÓDIGO: DOC-002	**FECHA:**

1. Descripción General

Motivo:	
Lugar:	
Fecha / Hora:	DD/MM/AAAA HH:MM a.m.
Requerido por:	

2. Participantes de la reunión

Participantes:	**Hora Llegada**	**Asistió**	**Firma**
Participante 1	HH:MM a.m.	☐	
Participante 2	HH:MM a.m.	☐	
Participante 3	HH:MM a.m.	☐	

3. Agenda

Tema:	**Descripción:**	**Responsable:**
Tema 1	Tema 1	Participante 1
Tema 2	Tema 2	Participante 2
Tema 3	Tema 3	Participante 3

4. Acuerdos

Acuerdo:	**Descripción:**

5. Problemas y/o Riesgos Identificados

Descripción:	**Acción a tomar:**	**Responsable:**	**Fecha:**	**Estado:**
1.				

Ministerio de Educación	**DOCUMENTO:** MATRIZ DE DUEÑOS DE LA INFORMACIÓN			
	CÓDIGO: DOC-003	**VERISÓN:** 1.0	**APROBADO POR:**	**FECHA APROBACIÓN:**

Activo de Información	Sub-Módulo	Descripción detallada	Dueño de la Información	Custodio de la Información

0107 -2008-ED

Ministerio de Educación	**DOCUMENTO:** BITÁCORA DE ACCESO FÍSICO AL CENTRO DE DATOS		
	CÓDIGO: DOC-004	**FECHA:**	**REVISADO POR:**

Fecha de Ingreso	Hora de Ingreso	Nombre del Visitante	Área o Empresa	Autorizador	Motivo de Ingreso	Fecha de Salida	Hora de Salida	Firma del visitante

0107 -2008-ED

Ministerio de Educación	DOCUMENTO: INVENTARIO DE ACTIVOS DE INFORMACIÓN		
	CÓDIGO: DOC-005	FECHA: DD/MM/AAAA	APROBADO:

Inventario de Activos de Información

Sistemas de aplicación

Activo intangible

Unidad Organizacional	Macroproceso	Proceso	Código de Activo	Activo de Información	Descripción	Dueño del Activo	Responsable de TI	Activos relacionados	Características técnicas	Fecha de registro

0107 "2008-ED

Ministerio de Educación	DOCUMENTO: INVENTARIO DE ACTIVOS DE INFORMACIÓN		
	CÓDIGO: DOC-005	FECHA: DD/MM/AAAA	APROBADO:

Inventario de Activos de Información

Bases de datos

Activo intangible

Unidad Organizacional	Macroproceso	Proceso	Código de Activo	Activo de Información	Descripción	Dueño del Activo	Responsable de TI	Activos relacionados	Características técnicas	Fecha de registro

Ministerio de Educación	DOCUMENTO: INVENTARIO DE ACTIVOS DE INFORMACIÓN		
	CÓDIGO: DOC-005	FECHA: DD/MM/AAAA	APROBADO:

Inventario de Activos de Información

Software de sistemas

Activo intangible

Unidad Organizacional	Macroproceso	Proceso	Código de Activo	Activo de Información	Descripción	Dueño del Activo	Responsable de TI	Activos relacionados	Características técnicas	Fecha de registro

Ministerio de Educación	DOCUMENTO: INVENTARIO DE ACTIVOS DE INFORMACIÓN		
	CÓDIGO: DOC-005	FECHA: DD/MM/AAAA	APROBADO:

Inventario de Activos de Información

Servidores

Activo tangible

Unidad Organizacional	Macroproceso	Proceso	Código de Activo	Activo de Información	Descripción	Dueño del Activo	Responsable de TI	Activos relacionados	Características técnicas	Fecha de registro

Ministerio de Educación	DOCUMENTO: INVENTARIO DE ACTIVOS DE INFORMACIÓN		
	CÓDIGO: DOC-005	FECHA: DD/MM/AAAA	APROBADO:

Inventario de Activos de Información

Almacenamiento de datos

Activo tangible

Unidad Organizacional	Macroproceso	Proceso	Código de Activo	Activo de Información	Descripción	Dueño del Activo	Responsable de TI	Activos relacionados	Características técnicas	Fecha de registro

Ministerio de Educación	DOCUMENTO: INVENTARIO DE ACTIVOS DE INFORMACIÓN		
	CÓDIGO: DOC-005	FECHA: DD/MM/AAAA	APROBADO:

Inventario de Activos de Información

Equipos de red

Activo tangible

Unidad Organizacional	Macroproceso	Proceso	Código de Activo	Activo de Información	Descripción	Dueño del Activo	Responsable de TI	Activos relacionados	Características técnicas	Fecha de registro

0107 -2008-ED

Descriptivo de las columnas del inventario

Unidad Organizacional	Esta columna indica el área organizacional al cual esta asociado el activo de información identificado. Dicha unidad organizacional debe ser una gerencia o subgerencia de acuerdo a lo indicado en el organigrama general de la institución.
Macroproceso	Agrupación de procesos de negocio orientados hacia el cumplimiento de un mismo objetivo institucional, al cual esta asociado el activo de información identificado.
Proceso	Proceso de negocio, el cual forma parte del macroproceso identificado en la columna C y al cual esta asociado el activo de información identificado.
Código de Activo	Correlativo utilizado para referenciar al Activo de Información
Activo de Información	Nombre del Activo de Información. Se define como activo todo aquello que presente valor para la organización.
Descripción	Descripción detallada de las principales características y/o funcionalidades del activo de información identificado.
Dueño del Activo	Usuario responsable de asegurar el uso adecuado del activo de información.
Responsable de TI	Custodio o responsable de los activos de información relacionados al área de Tecnología de Información (En caso corresponda).
Activos relacionados	Lista de códigos de activos de información que soportan el procesamiento del activo identificado
Características técnicas	Principales características técnicas del activo de información (modelo, versión, sistema operativo, parches, entre otras), en caso corresponda.
Fecha de registro	Fecha en la que se registró la información del activo en el Inventario.

Ministerio de Educación	**DOCUMENTO:** BITÁCORA DE INCIDENCIAS DE SEGURIDAD		
	CÓDIGO: DOC-006	**FECHA:**	**REVISADO POR:**

Código de Incidente	Fecha del Incidente	Descripción Incidente	Reportado por	Tipo de Incidente	Acciones realizadas para solución	Operador responsable solución	Fecha solución
				Incidente de Usuario / Incidente de Operación / Incidente de Sistema / Otros			

Ministerio de Educación	**DOCUMENTO:** BITÁCORA DE OPERACIONES		
	CÓDIGO: DOC-007	**FECHA:**	**REVISADO POR:**

Tarea programada	Descripción de la tarea	Operador responsable	Fecha de Ejecución	Hora de Ejecución	Resultado de Ejecución	Excepciones de procesamiento	Soluciones a las excepciones

0107-2008-ED

Ministerio de Educación	**DOCUMENTO:** BITÁCORA DE ACCESO USUARIOS		
	CÓDIGO: DOC-008	**FECHA:**	**REVISADO POR:**

Código Requerimiento	Fecha requerimiento	Solicitado por	Persona al cual se solicita el acceso	Área al cual pertenece la persona	Aprobado por dueño de la información	Identificador de Usuario	Activo de información relacionado	Privilegios requeridos

Ministerio de Educación	**DOCUMENTO:** BITÁCORA DE CUENTAS GENÉRICAS		
	CÓDIGO: DOC-009	**FECHA:**	**REVISADO POR:**

Código Requerimiento	Fecha requerimiento	Solicitado por	Motivo de creación de una cuenta genérica	Área en la cual se requiere	Aprobado por dueño de la información	Identificador de cuenta genérica	Activo de información relacionado	Privilegios requeridos

Ministerio de Educación	DOCUMENTO: CONTROL DE ACTIVOS DE TRATAMIENTO DE INFORMACIÓN		
	CÓDIGO: DOC-010	DOCUMENTO:	APROBADO POR:

1. Descripción General

Tipo de Activo	Sistema de Aplicación / Bases de Datos / Software de Sistemas / Servidores / Almacenamiento de datos / Equipos de red
Código de Activo	
Activo de Información:	
Descripción:	
Dueño del activo:	

2. Registro

Fecha de registro	
Registrado por	
Descripción del análisis de Riesgos	
Aprobado por	
Observaciones	

3. Relación con el Negocio

Unidad Organizacional	
Proceso	
Subproceso	

4. Características Técnicas

Características Técnicas	
Activos Relacionados	

Ministerio de Educación	DOCUMENTO: REGISTRO DE CONTROL DE REQUERIMIENTOS		
	CÓDIGO: DOC-011	DOCUMENTO:	APROBADO POR:

1. Descripción General

Código de Requerimiento	XXX
Tipo de Requerimiento	Cambio al sistema de información / Cambio al software base / Cambios a los dispositivos de comunicación / Cambios al Hardware
Descripción del Requerimiento	
Requerido por	
Fecha de Requerimiento:	

2. Clasificación

Complejidad	Alta / Media / Baja
Prioridad	Alta / Media / Baja
Tiempo Estimado	
Recursos Estimados	

3. Relación con el Negocio

Áreas Relacionadas	
Análisis de Impacto del cambio	

4. Análisis y diseño de la solución

Activo de Información relacionado	
Descripción del análisis y diseño de la solución	
Descripción de los cambios a efectuar	
Responsable del análisis y diseño de la solución	

Ministerio de Educación	DOCUMENTO: REGISTRO DE CONTROL DE REQUERIMIENTOS		
	CÓDIGO: DOC-011	DOCUMENTO:	APROBADO POR:

5. Implementación de la solución

Responsable Implementación	
Fecha de la Implementación de la solución	
Aprobado por	

Objeto (Actualizaciones / Ejecutables / Fuentes / Estructura de datos) relacionado al cambio	Versión del Objeto	Responsable Implementación	Fecha de Entrega	Fecha de Devolución

6. Pruebas de control de calidad

Fecha de aprobación	
Aprobado por responsable de Control de Calidad	
Aprobado por usuario que solicitó el cambio	

Descripción de la prueba	Responsable de la prueba	Fecha de ejecución de la prueba	Resultado de la prueba Fecha de Devolución

7. Pase a producción

Código de pase a producción	XXX
Aprobado por responsable de operaciones	
Fecha del pase a	

Ministerio de Educación	DOCUMENTO: REGISTRO DE CONTROL DE REQUERIMIENTOS		
	CÓDIGO: DOC-011	DOCUMENTO:	APROBADO POR:

producción	

Objeto (Actualizaciones / Ejecutables / Fuentes / Estructura de datos) relacionado al cambio	Versión del Objeto	Operador responsable

Ministerio de Educación	DOCUMENTO: REQUERIMIENTO DE ACCESO DE USUARIO		
	CÓDIGO: DOC-012	DOCUMENTO:	APROBADO POR:

1. Descripción General

Código de Requerimiento	XXX
Tipo de Acceso	Creación de cuenta / Eliminación de cuenta / Modificación de privilegios
Requerido por	
Persona al cual se le solicita acceso	
Área al cual pertenece la persona	

2. Privilegios requeridos

Aprobado por dueño de la información	

Código de Usuario el cual se solicita el acceso	Activo de información al cual se pide acceso	Privilegios requeridos

3. Pase a producción

Código de pase a producción	
Aprobado por responsable de operaciones	
Fecha del pase a producción	

Activo de información al cual se pide acceso	Privilegios requeridos	Fecha ejecución del acceso	Ejecutado por

Ministerio de Educación	**DOCUMENTO:** BITÁCORA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN		
	CÓDIGO: DOC-013	**FECHA:**	**REVISADO POR:**

Código cinta de respaldo	Ubicación de la cinta	Activo de Información	Operación	Motivo de ejecución	Fecha de Ejecución	Operador responsable	Aprobado por	Resultado operación
			Respaldo / Restauración	Programado / a Demanda / Prueba				

Activo de Información	Requerimiento de control	Tipo de Control	Descripción técnico del control	Control implementado	Responsable del control
		Cifrado / Control de Acceso a recursos / Control de Integridad de mensajes			

Ministerio de Educación	**DOCUMENTO:** BITÁCORA DE INCIDENCIAS DE OPERACIONES		
	CÓDIGO: DOC-015	**FECHA:**	**REVISADO POR:**

Código de Incidente	Fecha del Incidente	Descripción Incidente	Reportado por	Tipo de Incidente	Acciones realizadas para solución	Operador responsable solución	Fecha solución
				Incidente de Usuario / Incidente de Operación / Incidente de Sistema / Otros			

0107 -2008-ED