

UNIVERSIDAD PEDAGOGICA NACIONAL
FRANCISCO MORAZAN

DIRECCIÓN TECNOLOGÍA DE INFORMACIÓN

DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN



MANUAL DE NORMAS, POLÍTICAS Y
PROCEDIMIENTOS DE SISTEMAS DE
INFORMACIÓN

TEGUCIGALPA, M.D.C.,

NOVIEMBRE, 2006.

14, 12, 2006

ACUERDO N° 30-CSU-2006.- EL CONSEJO SUPERIOR UNIVERSITARIO DE LA UNIVERSIDAD PEDAGOGICA NACIONAL FRANCISCO MORAZAN.

CONSIDERANDO: Que la Universidad Pedagógica Nacional Francisco Morazán debe contar con instrumentos técnicos administrativos, que le permitan agilizar y efficientar el uso y manejo de sus recursos. **CONSIDERANDO:** Que el acelerado avance en los sistemas de información obliga a diseñar mecanismos de control para el uso y manejo de las distintas herramientas informáticas. **CONSIDERANDO:** Que el Consejo Directivo aprobó en primera instancia para la Universidad Pedagógica Nacional Francisco Morazán **EL MANUAL DE NORMAS Y PROCEDIMIENTOS DE SISTEMAS DE INFORMACION** y recomendó elevarlo al este Consejo para su aprobación. **CONSIDERANDO:** Que según el artículo 9 inciso f2 del Estatuto de la Universidad Pedagógica Nacional Francisco Morazán, es atribución del Consejo Superior Universitario de la UPNFM, aprobar las disposiciones internas que regulen el funcionamiento de la misma. **POR TANTO EN USO DE LAS FACULTADES QUE LA LEY LE CONFIERE ACUERDA:** 1) Aprobar para la Universidad Pedagógica Nacional Francisco Morazán **EL MANUAL DE NORMAS Y PROCEDIMIENTOS DE SISTEMAS DE INFORMACIÓN.** 2) El presente acuerdo entrará en vigencia a partir de su aprobación por el Consejo Superior Universitario. Dado en la ciudad de Tegucigalpa, Municipio del Distrito Central, a los catorce días del mes de diciembre del año dos mil seis. **M.Sc. LEA AZUCENA CRUZ CRUZ, PRESIDENTA; M.Sc. OSCAR FRANCISCO MUNGUÍA, SECRETARIO.**



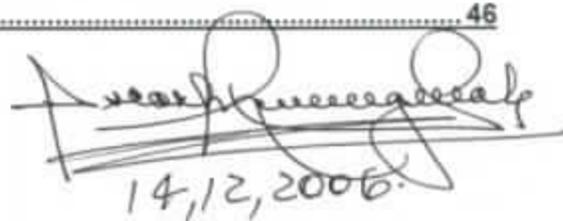
Tabla de Contenido

INTRODUCCIÓN.....	4
OBJETIVOS.....	5
PROCESO DE ATENCIÓN A USUARIOS.....	6
PROCESO DE ATENCIÓN SOBRE APLICACIONES.....	8
PASOS PARA CREACIÓN DE CUENTA DE CORREO Y/O ACCESO A INTERNET	10
PROCEDIMIENTO DE INGRESO DE EQUIPO A OFICINAS IT.....	12
PROCEDIMIENTO DE ACCESO A LOS SERVIDORES.....	13
POLÍTICAS DE RESPALDO DE INFORMACIÓN.....	16
MEDIOS DE ALMACENAMIENTO	16
LUGARES FÍSICOS DE ALMACENAJE	16
DE LA ROTACIÓN DE LOS RESPALDOS Y SU ROTULACIÓN	17
PRUEBAS A LOS RESPALDOS	18
POLÍTICAS DE SEGURIDAD INFORMÁTICA.....	21
INTRODUCCIÓN	21
SOBRE EL USO DE INTERNET Y CORREO ELECTRÓNICO	21
SOBRE EL USO DE LOS EQUIPOS	21
DE LOS ACCESOS	23
SOBRE EL SOFTWARE EN LOS EQUIPOS	24
DE LA PUBLICACIÓN WEB (WWW.UPNFM.EDU.HN)	26
DEL USO DEL EQUIPO EN LOS LABORATORIOS	26
ASPECTOS GENERALES	27
RESPONSABILIDADES INDIVIDUALES	27
SANCIONES	27
REGLAMENTO PARA LA PUBLICACIÓN EN LA PÁGINA WEB INSTITUCIONAL	30
ALCANCE Y DEFINICIONES	30
DE LA INFORMACIÓN	31
DE LAS FACILIDADES OFRECIDAS PARA LA ADMINISTRACIÓN DE SERVICIOS WEB.	34
DE LA ASIGNACIÓN DE ESPACIO	34
DE LAS OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS DE LAS PÁGINAS	35
DE LAS AMONESTACIONES Y SANCIONES	36
DE LA CREACIÓN DE UN SERVIDOR	37
DE LAS PUBLICACIONES EN SERVIDORES EXTERNOS	38
ANEXO 1. TÉRMINOS DE USO	40
ANEXO 2. SOLICITUD DE CUENTA DE ACTIVACIÓN	40



[Handwritten signature]
4, 9, 2006.

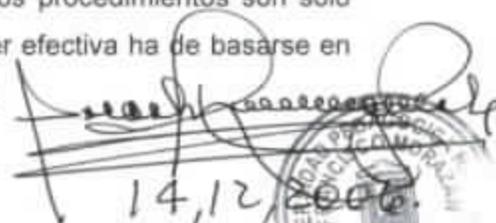
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.....	40
ANEXO 3. PROCEDIMIENTO PARA LA PUBLICACIÓN DE PÁGINAS WEB	41
Recomendaciones para elaborar el sitio web.....	41
Páginas académicas.....	41
Páginas de grupos estudiantiles.....	42
Páginas de eventos.....	42
Páginas de Unidades Académicas y Administrativas.....	42
Creación de un servidor propio.....	43
NOMENCLATURAS	44
EN DIAGRAMACIÓN	45
ANEXOS.....	46


14,12,2006.

Introducción

Dentro del marco de definición de las unidades dependientes de la Dirección de Tecnologías de Información y en el marco de la estandarización de procesos dentro del Departamento de Sistemas de Información, se presenta este documento en el cual se incorporan los lineamientos, normas y las políticas de la Dirección de Tecnología de Información, de la Universidad Pedagógica Nacional Francisco Morazán (UPNFM)

Uno de los principales objetivos de este documento es de establecer un marco de actuación concreto para que los miembros del departamento sean integrados a los procesos y las actividades del mismo, garantizando así que todos conozcan y respeten los lineamientos establecidos. No hay que olvidar que los procedimientos son solo una herramienta de trabajo útil pero no suficiente. Para ser efectiva ha de basarse en el compromiso y en la confianza de todos los involucrados.

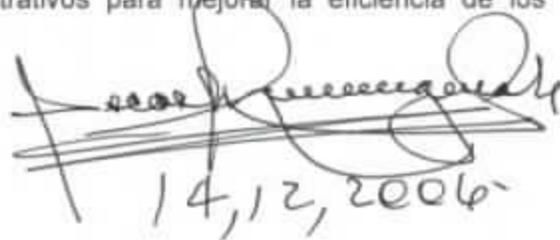

14,12,2006.



Objetivos

El presente documento, denominado Normas, Políticas y Procedimientos de Sistemas de Información, se presenta con el propósito de establecer una normativa bajo la cual tengan lugar las actividades relacionadas con el quehacer del Departamento de Sistemas de Información, para lo cual se establecen los objetivos siguientes:

- Establecer la normativa que rige los procesos de servicios a usuarios
- Definir el mecanismo y ámbito de aplicación de la normativa interna de trabajo y servicios
- Documentar los procesos administrativos para mejorar la eficiencia de los servicios



Handwritten signature and date: 14, 12, 2006

Proceso de Atención a Usuarios

Objetivo:

Mantener los equipos de escritorio, de comunicación y sistemas de información en el óptimo desempeño.

Descripción:

Este proceso indica los pasos a seguir en caso de existir alguna solicitud de apoyo por parte del departamento de Tecnología de Información.

No.	Actividad	Responsable
1.	Solicitud apoyo a la unidad de DTI	Unidad - Usuario
2.	Levantamiento de Orden de Trabajo	HelpDesk
3.	Asignación de trabajo al personal indicado (a) Técnicos (b) Desarrolladores Si es (a) seguir con ir al Paso #4 Sino ver <u>Proceso de atención sobre aplicaciones</u>	HelpDesk
4.	Visita de personal al sitio del problema Si el problema se resuelve Paso # 9 Sino Paso #5	HelpDesk
5.	Se revisa el equipo en busca de fallos de hardware y/o Software	Técnico
6.	Resguardo de la información	Técnico Usuario
7.	Verificar si el equipo se encuentra en garantía Si es así Es necesario realizar <i>dictamen técnico</i> para trámite de garantía (Depto. de Compras) Sino Se verifica si es requerida su compra, Si es así Se realiza <i>dictamen técnico</i> para trámite de compra Sino Sigue Paso #8	Técnico Admin. Redes
8.	Reparación del equipo	Técnico
9.	Entrega del equipo y registro de las actividades hechas en la orden de trabajo.	Técnico
10.	Firma de aceptación de servicio	Unidad - Usuario
11.	Archivar la orden de trabajo	HelpDesk

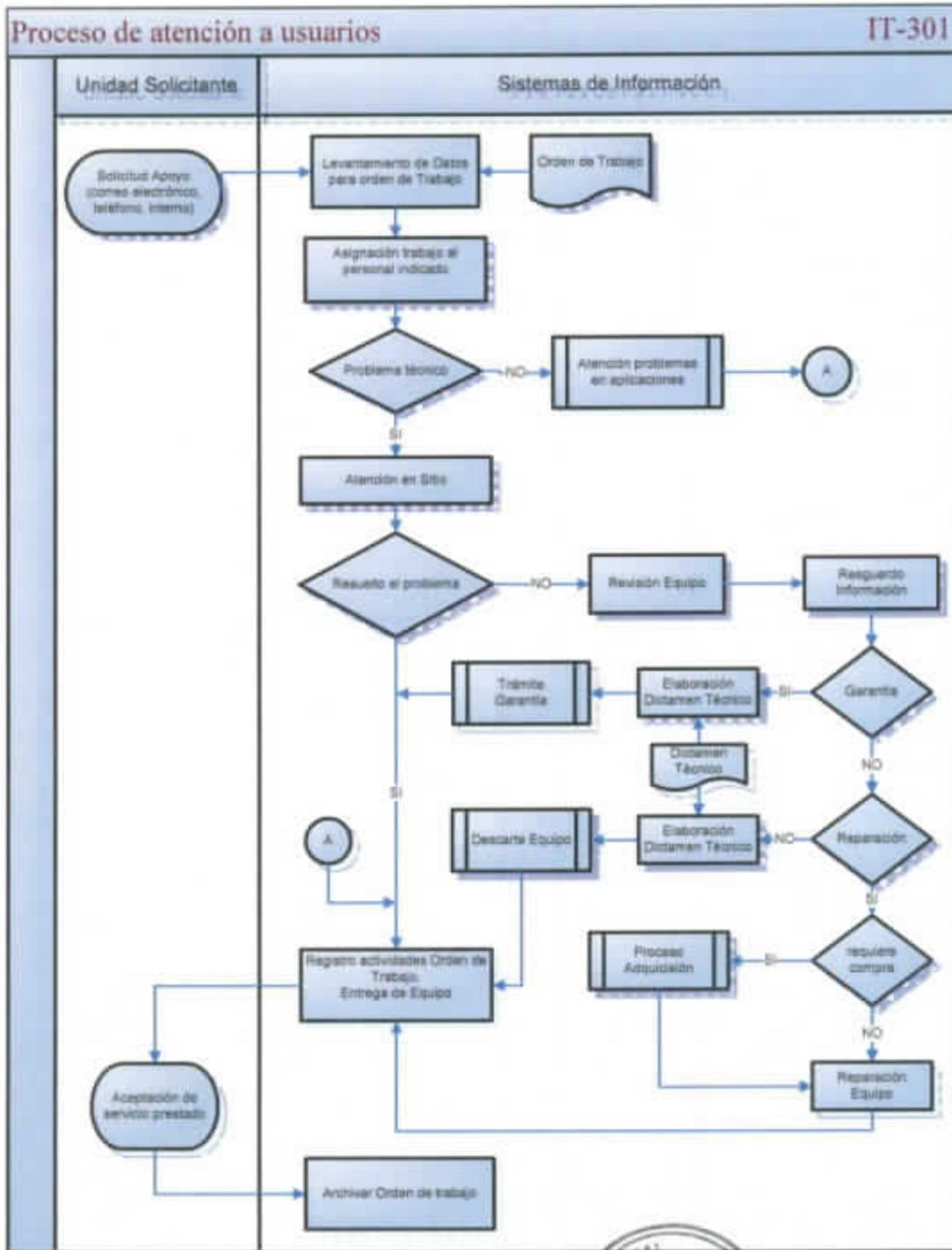
Lineamientos:

- Si se pone en riesgo la información del equipo, es **Obligación** del técnico en coordinación con el **usuario** realizar un resguardo de la información contenida en ese equipo, siempre y cuando no exista problema físico permanente sobre el disco duro. Este respaldo deberá ser quemado en CD / DVD si así lo amerita dicha información. El departamento de tecnología de información no se hace

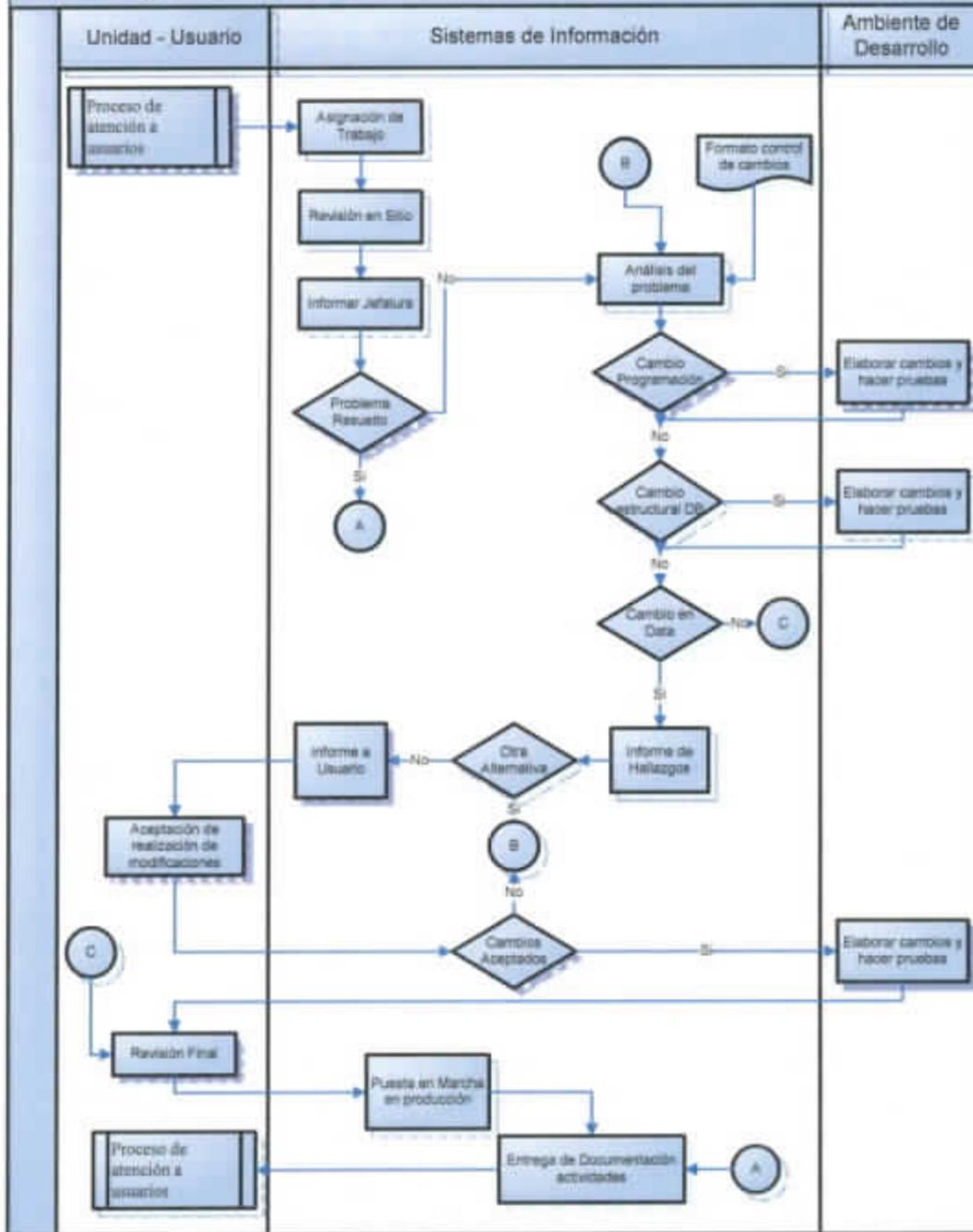


responsable por documentos y/o archivos que no sean afines al trabajo realizado (ej. Películas, videos, pornografía, música, etcétera)

- Para el equipo que se tramita en garantía se le dará 1 día hábil para la prueba, previo de finalización de la orden de trabajo.
- La persona a quien se le brindo el apoyo, es quien debe dar por recibido o aceptado el servicio prestado, en su defecto esta orden deberá ser firmada por una persona responsable a espera de la firma final de aceptación.



[Handwritten signature]
14,12,2006



Handwritten signature and date: 14/12/2006. Includes a circular stamp from the Universidad Tecnológica Nacional (UTN) with the text "UNIVERSIDAD TECNOLÓGICA NACIONAL" and "CENTRO DE INVESTIGACIONES Y DESARROLLO".

Proceso de atención sobre aplicaciones

Objetivo:

Realizar las actividades de soporte en ambiente controlado y de la forma mas transparente para el usuario final, documentando estos para futuras referencias.

Descripción:

Este procedimiento debe aplicarse cuando sea requerida alguna revisión sobre los sistemas informáticos en los que el departamento tiene responsabilidad directa de su mantenimiento.

No.	Actividad	Responsable
1.	Asignación de trabajo a un desarrollador	Jefe de Sistemas
2.	Revisión en sitio del problema	Desarrollador
3.	Informe de actividades a la Jefatura Si el problema se solucionó Paso #10 Sino Paso #4	Jefe Sistemas Inf.
4.	Investigación del causante del problema y la posible solución al mismo En caso de requerir Cambio programación: realización cambios y elaborar pruebas. Cambio en estructuras DB: realización de cambios y elaborar pruebas. Modificación de la data: si es si Paso #5, sino Paso # 9	Desarrollador
5.	Informar modificación de la data al Jefe de Sistemas, redactando un informe del porque de la misma. Si se encuentra otra posible alternativa a Paso #3 Sino Paso #6.	Desarrollador
6.	Elaborar informe de notificación (escrita), al jefe departamento que origino la solicitud de apoyo, indicando las causas y el planteamiento de realización del cambio. Aceptando este hecho.	Jefe de Sistemas Desarrollador
7.	Lectura y aprobación informe Si fue aprobado el cambio Paso #8 Sino Paso #4	Unidad - Usuario
8.	Elaboración de cambios y pruebas sobre los datos.	Desarrollador
9.	Revisión y aceptación de que todo este bien.	Desarrollador Usuario
10.	Entrega documentación proceso	Desarrollador
11.	Anexar documentación a Orden de trabajo	



4/12/2006

Pasos para creación de cuenta de correo y/o acceso a Internet

Objetivo:

Definir claramente los pasos que deben llevarse a cabo para la habilitación de cuentas de correo electrónico y el acceso a Internet.

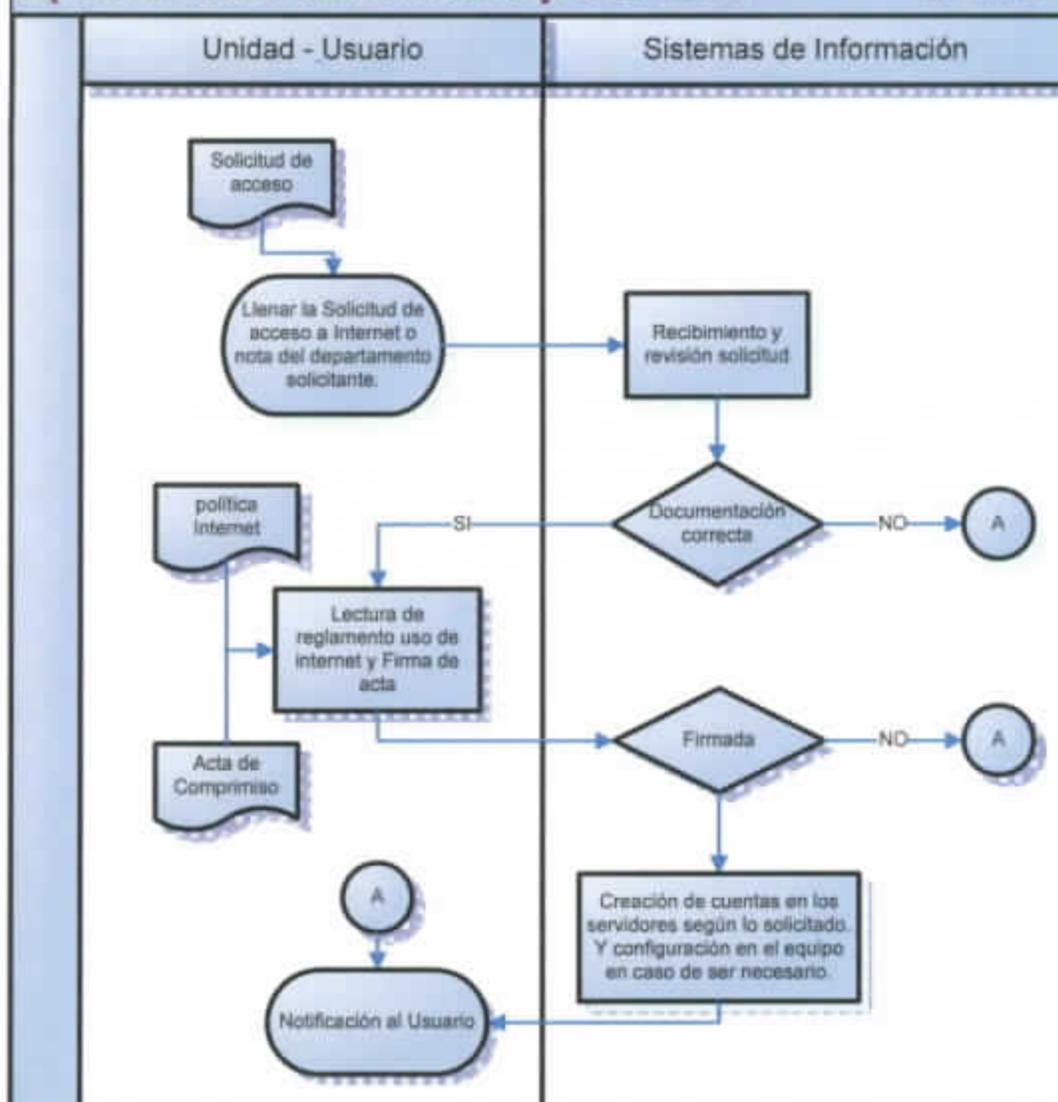
Descripción:

Este procedimiento debe aplicarse cuando sea solicitado al departamento uno de ambos accesos, documentando dicha solicitud.

No.	Actividad	Responsable
1.	Solicitud de creación de cuenta y acceso Internet	Usuario – Unidad
2.	Recibimiento de la solicitud	HelpDesk Secretaria
3.	Revisión de firmas y permisos Si se encuentra correcto Paso #4 Sino Paso #7	Administrador Red
4.	Lectura por parte del solicitante del reglamento de uso de Internet. Si acepta los lineamientos establecidos Paso#5 Sino Paso #7	Usuario
5.	Firma de Acta de Compromiso	Usuario
6.	Creación de cuenta en los servidores según lo solicitado	Administrador Red
7.	Carta de Notificación al Usuario	Administrador Red


14,12,2006





Lineamientos

- Las cuentas de correo y de acceso a Internet puede ser dadas de baja por cualquier de las siguientes razones:
 - Las estipuladas en el reglamento de Internet y de seguridad del departamento.
 - Por solicitud del jefe de departamento o unidad donde se encuentra laborando el dueño de la cuenta.
 - Por despido o renuncia y no se requiere la existencia de las mismas.
- En caso de cambios a cuentas existentes, deberá ser manejado con el mismo procedimiento de apertura.



14, 12, 2006.

Procedimiento de ingreso de equipo a oficinas IT

Al momento de ingresar equipo a las oficinas del área de Informática para efectos de mantenimiento deberá cumplirse con el siguiente procedimiento.

Pasos para el ingreso / salida:

No.	Actividad	Responsable
1.	Verificación de espacio disponible para el alojamiento del equipo. (no mayor a 3 equipos)	Técnico de área
2.	Levantar documento de ingreso de equipo	Técnico de área
3.	Revisión del equipo, con descripción de especificaciones.	Admin. Redes
4.	Resguardo del equipo hasta que se realice su mantenimiento, este debe estar en un lugar accesible solamente por el personal a cargo de su mantenimiento o en efecto del jefe inmediato del mismo.	Técnico
5.	Una vez reparado el equipo o diagnosticado su estado, y que el equipo requiera salir del departamento, deberá ser revisado y certificada su entrega al departamento origen	Admin. Redes

En caso de anomalías en el recibo del equipo:

De existir algún tipo de duda, o de hecho demostrado, de que el equipo ha sido saqueado o sus partes no coinciden con el estatus conocido por el departamento, se deberá proceder de la siguiente forma:

No.	Actividad	Responsable
1.	Hacer una solicitud al departamento de Activos Fijos un informe sobre los datos del activo.	Admin. Redes
2.	Comparar estos datos con los encontrados.	Admin. Redes
3.	En el caso de demostrar irregularidad, se procederá a levantar un acta de estado del mismo indicando, si se tiene, al responsable y las observaciones o medidas a tomar sobre el mismo.	Admin. Redes Jefe de Unidad

En caso de anomalías en la salida del equipo:

De existir algún tipo de duda, o de hecho demostrado, que el equipo ha sido saqueado o sus partes no coinciden con el estatus con el que ingreso al departamento, se deberá proceder de la siguiente forma:

No.	Actividad	Responsable
1.	Identificar exactamente la irregularidad, el encargado del resguardo del activo y las personas con acceso al área donde se encontraba.	Admin. Redes
2.	Levantamiento de acta.	Admin. Redes Jefe de Unidad
3.	Pasar caso a las autoridades respectivas.	Jefe de Unidad



14,12,2006

Procedimiento de Acceso a los Servidores

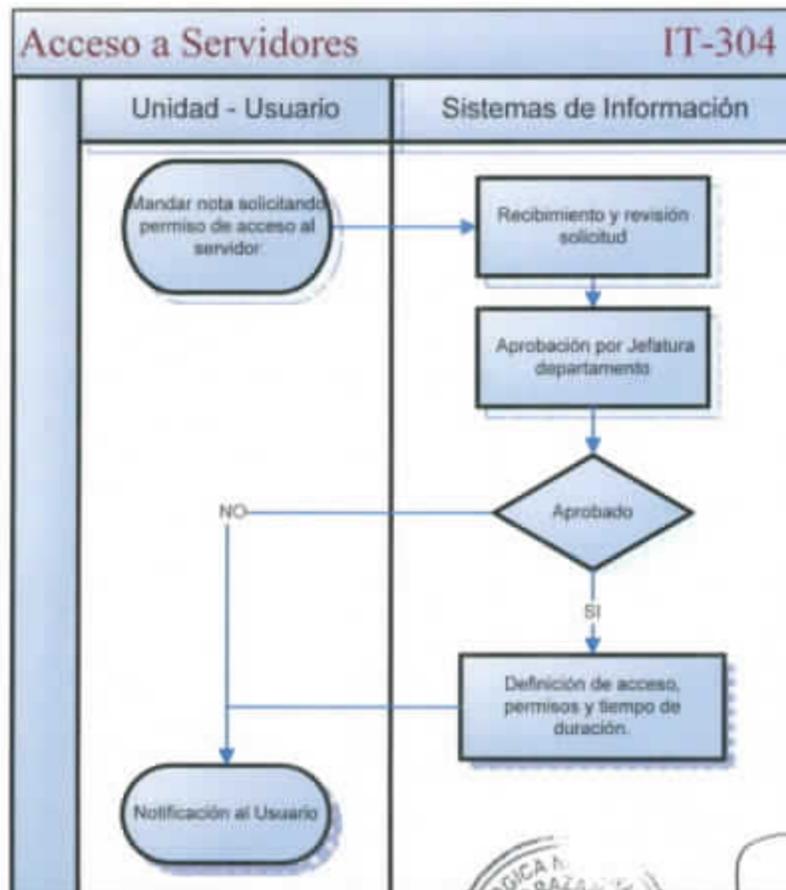
Objetivo:

Regular el acceso a los servidores que son custodiados por el departamento de sistemas de información.

Descripción:

Este procedimiento debe aplicarse cuando sea solicitado al departamento de acceso a los servidores, aunque la información contenida en ellos pertenezca a otro departamento o unidad.

No.	Actividad	Responsable
1.	Nota de solicitud de acceso al servidor	Usuario – Unidad
2.	Recibimiento de la solicitud y análisis de efectos del mismo.	Administrador Red
3.	Aprobación de acceso Si es aprobado Paso#4 Sino Paso#5	Jefe de Depto.
4.	Se concede el acceso, con supervisión de actividades	Usuario Admin. Redes
5.	Se notifica al Usuario	



Manejo de los Perfiles

Los perfiles locales y las cuentas mínimas a crear en los servidores que trabajan con Windows como OS, serán las siguientes.

Cuenta: *administrador*
Miembro de: *administradores*
Propietario: *Cuenta reservada y privada*
Característica General:

El uso de esta cuenta se encontrará restringido a todo personal, cuya contraseña estará resguardada por el Director de Tecnología de Información y será empleada solamente en los casos de emergencia y/o ausencia de la entidad administradora en ese momento.

Cuenta: *redadmin*
Miembro de: *administradores*
Propietario: *Administrador de la Red*
Característica General:

El uso de esta cuenta será exclusivamente para el administrador de red, quien tendrá todos los privilegios (sin restricciones) para el cuidado y resguardo del servidor.

Cuenta: *nusuario*
Miembro de: ---
Propietario: *Usuarios Invitados*
Característica General:

El uso de esta cuenta será administrada por el administrador de red, quien establecerá la vigencia, privilegios y horarios temporales de uso según le sea solicitado.

Otro tipo de Cuentas

- En el caso de accesos a los servidores compartidos en su administración (como por ejemplo es el caso del servidor DETED), deberán crearse cuentas que indiquen que personal del mismo tendrá el acceso y el tipo de acceso que se requiera.
- Usuarios requeridos para conexión, deberán ser definidos como usuarios normales, dando privilegios y/o permisos sobre las carpetas, archivos, sistemas que requiera su conexión.

De la duración de los accesos temporales

- Deberá definirse claramente el período de tiempo que la cuenta se encontrará activa y definirlo en el sistema operativo para que automáticamente sea bloqueada, para su posterior eliminación.



[Handwritten signature]
14, 12, 2006.

Estado Actual de uso de perfiles en los servidores

➤ Servidor de Aplicaciones

Cuenta	Perfil	Descripción
administrador	Administradores	Reservada
ropez	Administradores	Funciones administrador red
aramos	Administradores	Funciones administrador aplicaciones
conserver	Administradores	Conectividad de aplicaciones

➤ Servidor Magic

Cuenta	Perfil	Descripción
Admin. varias	Administradores Limitada	Reservada Funciones de conexión al servidor

➤ Servidor de Web

Cuenta	Perfil	Descripción
administrador	Administradores	Reservada
ropez	Administradores	Funciones administrador red
jconde	Power users	Funciones de webmaster
cagular	Backup user	Realización de respaldos

➤ Servidor TACATS

Cuenta	Perfil	Descripción
Administrador	Administradores	Reservada
ropez	Administradores	Funciones administrador red
Jconde	Power users	Funciones de admón. cuentas

➤ Servidor Backup

Cuenta	Perfil	Descripción
Administrador	Administradores	Reservada
ropez	Administradores	Funciones administrador red
Cagular	Administradores	Funciones de admón. de respaldos

➤ Servidor DNS

Cuenta	Perfil	Descripción
Admin. ropez	Administradores Power User	Reservada Funciones administrador DNS

➤ Servidor Teleduc

Cuenta	Perfil	Descripción
Root Teleduc	Administradores Limitada	Reservada Funciones de verificación servicio



POLÍTICAS DE RESPALDO DE INFORMACIÓN

Objetivo:

Lograr que la información custodiada por el departamento en su área de servidores, pueda ser recuperada - con un margen mínimo de pérdida - ante la necesidad de su recuperación por cualquier situación adversa.

Descripción:

La información es uno de los bienes más importantes con lo que contamos en nuestro medio, por lo que el resguardo de la misma (Backups) ha tomado mayor importancia. Las pérdidas de información se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, "hackers", errores humanos, incendios, inundaciones, etc. Y aunque no se pueda prevenir completamente cada una de estas pérdidas, la UPNFM sí puede prepararse para evitar las consecuencias de pérdidas graves en sus sistemas de información.

Medios de almacenamiento

Dependiendo del volumen de la información, el departamento cuenta con los siguientes medios para el almacenaje de los respaldos:

Item	Medio Almacenaje	Capacidad Almacenamiento	Fiabilidad	Velocidad de Recuperación
bk1	Disco Duro (Interno-mismo equipo)	Según Equipo	Alta	Alta
bk2	Disco Duro (Externo - otro equipo o unidad externa)	40Gb	Alta	Media
bk3	Unidad CD	700Mb	Media	Media
bk4	Unidad DVD	4.4 GB	Media	Media
bk5	Unidad de Tape DLT	40/80	Alta	Baja

Lugares físicos de almacenaje

Los respaldos que se realicen en media externa (CD, DVD., tapes, otras unidades), podrán ser almacenados en los siguientes espacios disponibles:

Item	Lugar	Custodiado por
L1	DTI - Tegucigalpa (Edif. Biblioteca nuevo)	Administrador Redes
L2	Backbone fibra - Tegucigalpa	Administrador Redes
L3	DTI - San Pedro Sula	Soporte a Redes
L4	Caja fuerte Banco	Administrador Redes

En cada lugar deberá existir un espacio físico asignado y restringido con control de llaves único, para el responsable de la custodia de los respaldos. Respondiendo siempre a un plan de contingencia institucional.



14/12/2006

De la rotación de los respaldos y su rotulación

Para la información (sitios Web, bases de datos). Estos se realizarán con los siguientes períodos:

Periodicidad	Elaborado por	Horario
Diario	Automático	Lunes a Viernes, horario no hábil (1-3 a.m.).
Semanal	Automático	Sábado 3:00 a.m. en adelante.
Quincenal	Admin. Redes o encargado en sitio	15 y 30 c/mes, en la media que se estime conveniente. Pudiendo ser en mayor instancia DVD o DLT.

Para los programas fuentes y ejecutables:

Periodicidad	Elaborado por	Horario
Semanal	Programadores	Viernes 3:00pm en adelante.
Quincenal	Programadores / Admin. Redes	15 y 30 c/mes

Lineamientos

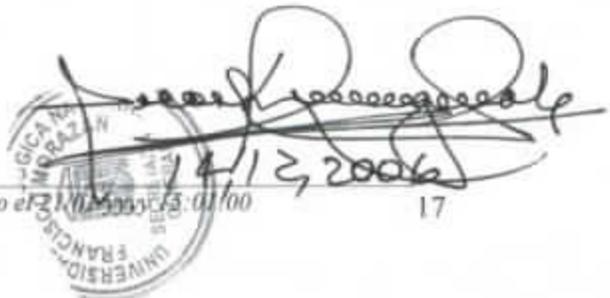
- Toda la información debe ser respaldada quincenalmente.
- Los respaldos quincenales pueden ser manejados en la misma media, siempre que se encuentre bien identificado cada elemento y que la capacidad del medio lo permita.
- Los respaldos diarios y semanales son completos y auto-reemplazables. De tal forma que solo se mantendrá el último realizado y no el histórico de los mismos.
- Se sacarán dos juegos de respaldos quincenales, el 1ro se hospedará en las mismas instalaciones (de preferencia otro edificio) y el 2do en localidad distante.
- Por sitio (fuera de DTI) se mantendrá únicamente un margen de dos meses máximo de respaldos (4 juegos), al cumplir este período deberán ser regresados a DTI al administrador de Redes para su custodia.
- Cualquier otro respaldo será considerado como extraordinario y podrá ser realizado por diversos motivos como mantenimiento a servidores, modificaciones, cambios estructurales de bases de datos u otros. Y serán custodiados en DTI por el administrador de redes.

Rotulación para respaldos Quincenales

El número del backup será creado de la siguiente manera para respaldos:

<Año>.<Mes>.<Quincena A/B> <9999><99><A>

De tal forma que si estamos en enero/2006 y es el primer respaldo quincenal que se realiza. El número será **2006.01.A**



Rotulación para respaldos Extraordinarios

El número del backup será creado de la siguiente manera para respaldos extraordinarios:

<Año>.<Mes>.<día> <9999><99><99>

De tal forma que si estamos en 11/enero/2006 e hicimos un respaldo de emergencia. El número será **2006.01.11**

La información rotulada en la media deberá contener.

- No. Backup: <número>
- Realizado en: <cede>
- Realizado por: <Nombre administrador>
- Contenido: <lista del contenido respaldado>

Y ser registrado en el documento denominado "bitácora de Backups"

Pruebas a los respaldos

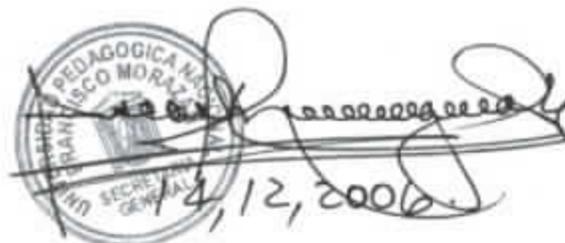
Con el propósito de asegurar que los respaldos se están realizando de forma correcta y que la información puede ser recuperada y puesta en producción en caso de ser necesario, se establecen los siguientes lineamientos.

De la periodicidad de los Respaldos: El administrador de redes deberá verificar semanalmente que los respaldos automáticos se estén ejecutando en los horarios y períodos establecidos.

De la extracción de la media: El administrador de redes deberá probar quincenalmente que se pueda extraer de la media en la que se esta guardando los respaldos toda la información almacenada en la misma.

Pruebas de recuperación: este tipo de pruebas deben de ser emitidas de la siguiente manera:

- Los respaldos automáticos deberán verificarse inmediatamente del primer bloque obtenido
 - a. **De archivos:** deberá recuperarse en un ambiente de prueba los mismos y verificar su consistencia. *Administrador Redes.*
 - b. **De Bases de datos:** recuperación en un ambiente de pruebas en colaboración del administrador redes y el admin. de bases de datos o Analista programador responsable del aplicativo.
- Cualquier otra prueba que el Administrador de Redes determine por sospecha de posible fallas.



SECRETARÍA GENERAL DE EDUCACIÓN DEL ESTADO DE MORELOS
14, 12, 2006

Estado Actual

Los sistemas y otra información que se maneja en el departamento se resumen en la siguiente tabla:

Tegucigalpa (Actualizada el 09-01-2005)

Item	Nombre del Sistema	Servidor	En	Espac
C1	Sistema de Control Presupuestario	Registro01	Carpeta	200Mb
C2	Sistema de Control de Ingresos	Registro01	SQL Server	50Mb
C3	Sistema de Control de Activos		Dbf	
C4	Sistema de Recursos Humanos	Magic	Btrieve	200Mb
C5	Sistema de Contabilidad	Magic		
C6	Sistema de Librería			
C7	Sistema Académico	Registro01	SQL Server	600Mb
C8	Modulo de Becarios	Registro01	SQL Server	50Mb
C9	Sistema de Gestión de Biblioteca (ALTAIR)	DETED_Server	SQL Server	12Gb
C10	Sitio Web www.upnfm.edu.hn	Upnfmweb	Carpeta	
C11	Sitio Web Postgrados	Linux Server	Carpeta	
C12	Configuración equipo de comunicación y redes		Carpeta	5Mb
C13	Servidor de Archivos (NO IMPLEMENTADO)			

Servidor Magic (Novell)

- A nivel de Carpeta
 - MagicDev
 - Public

A	Diario	Bk2	L1	Lunes a Viernes a la 1:00 a.m.
B	Semanal	Bk2	L1	Sábado a la 1:00 a.m.
C	Quincenal	Bk4	L2 y L3	

A → En el servidor Backups en *d:\respaldos\magic\diario*

B → En el servidor Backups en *d:\respaldos\magic\semanal*

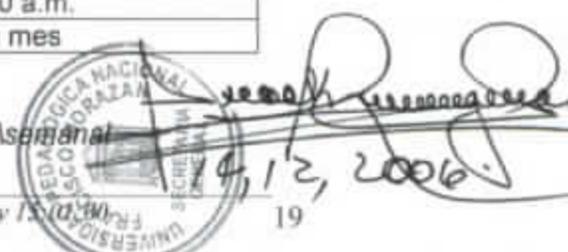
Servidor Registro01 (172.16.10.1)

- En SQL Server las siguientes bases de datos
 - Académico
 - Becarios
 - Caja
 - CIIE
 - Planilla
 - Registro
- A nivel de Carpeta
 - C:\upnfm\sig

A	Diario	Bk1	L1	Lun. a Vier. de 1:00 a 2:00 a.m.
B	Semanal	Bk2	L1	Sábado a la 1:00 a.m.
C	Quincenal	Bkp4	L2 y L3	15 y 30 de cada mes

A → En el mismo servidor en *d:\respaldos\diario*

B → En el servidor Backups en *d:\respaldos\registro\semanal*



Servidor DETED Server

- En SQL Server las siguientes bases de datos
 - Honduras
 - Dinamis

A	Diario	Bk1	L1	Lunes a Viernes de 1:00 a 2:00 a.m.
B	Semanal	Bk2	L1	Sábado a la 1:00 a.m.
C	Quincenal	Bkp4	L2 y L3	15 y 30 de cada mes

- A → En el mismo servidor en *d:\respaldos\diario*
- B → En el servidor Backups en *d:\respaldos\deted\semanal*

Servidor UPNFMWEB

- A nivel de Carpeta
 - D:\inetPub

A	Diario	Bk1	L1	Lunes a Viernes de 1:00 a 2:00 a.m.
B	Semanal	Bk2	L1	Sábado a la 1:00 a.m.
C	Quincenal	Bkp4	L2 y L3	15 y 30 de cada mes

Servidores CUED

- En SQL Server las siguientes bases de datos
 - Registro

A	Diario	Bk1	L1	Lunes a Viernes de 1:00 a 2:00 a.m.
B	Semanal	Bk1	L1	Sábado a la 1:00 a.m.
C	Quincenal	Bkp4	L1	15 y 30 de cada mes

- A → En el mismo servidor en *c:\respaldos\diario*
- B → En el servidor Backups en *d:\respaldos\cued\<sede>\semanal*

Fuentes y Ejecutables

- En SQL Server las siguientes bases de datos
 - Registro

A	Semanal	Bk2	L1	Sábado a la 1:00 a.m.
B	Quincenal	Bkp4	L1	15 y 30 de cada mes

- A → En el servidor Backups en *d:\respaldos\fuentes\<aplicativo>*

Configuración de Equipo de Comunicaciones y redes

- Configuración del los Routers, Switches y Pix

-	Mensual	Bk4		30 de cada mes
---	---------	-----	--	----------------



POLÍTICAS DE SEGURIDAD INFORMÁTICA

Introducción

El departamento de Sistemas de Información ha asumido la responsabilidad de contribuir en el desarrollo Tecnológico de la Universidad Pedagógica Francisco Morazán (UPNFM); por ello se ha dispuesto una serie de medidas, las cuales se describen en las siguientes páginas, con el objetivo de obtener los mayores beneficios de la tecnología con la que se cuenta.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concienciar a cada uno sobre la importancia y la sensibilidad de la información y de los servicios críticos que favorecen el desarrollo y un buen funcionamiento.

Las tecnologías por sí mismas son un medio, es lo que las personas hacen con ella lo que marca la diferencia.

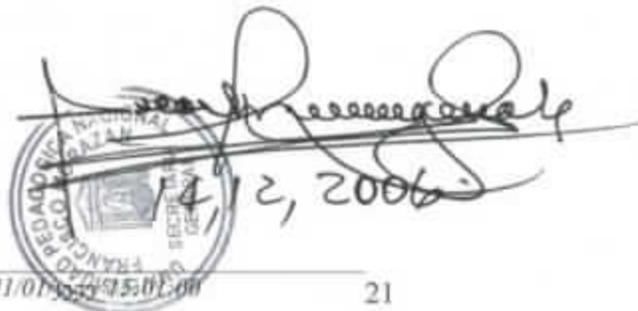
Sobre el uso de Internet y correo electrónico

La UPNFM cuenta con su reglamento sobre uso de Internet, en el cual se detallan los lineamientos a seguir tanto a nivel de navegación, correo electrónico y otros. Ver anexo.

Sobre el uso de los equipos

De la instalación de equipo de cómputo.

1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores, equipo de comunicación, y equipo accesorio), que esté o sea conectado a la Red de la universidad, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe de sujetarse a las normas y procedimientos de instalación que emite el departamento de Sistemas de Información.
2. DTI en coordinación con el departamento de Activos deberá tener un registro de todos los equipos propiedad de la UPNFM.
3. El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada como ser los gabinetes de comunicaciones, servidores locales u otros; requieren estar ubicados en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales apropiadas, alimentación eléctrica correcta y con acceso no restrictivo para personal del departamento de sistemas.
4. La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a las autoridades correspondientes (departamento de Activos, DTI y otros de competencia).



14/2/2006

Del mantenimiento de equipo de cómputo.

1. Al departamento de Sistemas de Información, corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y las recomendaciones del acondicionamiento específico que requiera el lugar.
2. El personal técnico de los departamentos y laboratorios académicos se apegarán a los requerimientos establecidos en las normas y procedimientos que el departamento de Sistemas de información emita.
3. Los responsables de las áreas de Cómputo de un departamento pueden otorgar mantenimiento preventivo y correctivo, a partir del momento en que sean autorizados por la DTI.
4. Por motivos de normatividad queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no es propiedad de la institución, de lo contrario DTI no se hace responsable por daños que puedan ocurrir de estas revisiones.

De la actualización del equipo

1. Todo el equipo de cómputo: computadoras personales, estaciones de trabajo, servidores, equipo de telecomunicaciones y demás relacionados; que sean propiedad de la universidad, requieren del diagnóstico del personal de DTI para mejorar o cambiarlo completamente o en sus partes.
2. Se prohíben la manipulación interna de los equipos al personal que no sea autorizado por DTI.
3. Las actualizaciones a nivel de software realizada por los técnicos de los diversos departamentos académicos deberán ser informados y autorizados por DTI para fines de control de licenciamiento.

De la reubicación del equipo de cómputo.

1. La reubicación del equipo de cómputo en lo referente a computadoras de escritorio, podrá realizarse por el departamento que lo requiriera siempre que sea comunicado DTI y éste determine que no presenta ningún riesgo su traslado. De lo contrario se dispondrá al personal de DTI para la supervisión del mismo.
2. En caso de existir personal técnico de apoyo de los departamentos académicos, éste notificará de los cambios tanto físicos como de software de red que realice, y en caso de cambio de responsable del equipo, se hará al departamento de Activos. Notificando también los cambios de equipo inventariado (cambio de monitores, de impresoras etc.).
3. El equipo de cómputo a reubicar se hará únicamente bajo la autorización del responsable, contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.



10/12/2006

De los accesos

Del acceso al site.

1. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta DTI.
2. DTI asignará los permisos y el nivel de acceso requerida con base en los requerimientos.
3. Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso al site estará sujeto a lo que especifiquen las autoridades superiores de la institución.

Del control de acceso al equipo de cómputo.

1. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
2. Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que DTI emita.
3. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la DTI tiene la facultad de acceder a cualquier equipo de cómputo que no esté bajo su supervisión, y que por falla en la configuración éste pueda afectar el buen funcionamiento de los servicios que presta el departamento como ser la red interna.

De control de acceso remoto.

1. DTI es responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles, como ser horarios de conexión, permisos y registro de actividades a realizar.
2. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la DTI.

De acceso a los sistemas administrativos y académicos.

1. Tendrá acceso a los sistemas administrativos y académicos solo el personal del cual haya realizado el proceso de solicitud de forma correcta y que haya sido aprobada según las normas establecidas por DTI.
2. Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos, ya sea de forma física o remota, no autorizados.
3. El tipo de usuario, el nivel de acceso a la información (modificación, eliminación, consulta, etcétera) dependerán del nivel de seguridad que permita el aplicativo, y la determinación de los mismos será una tarea en conjunta del personal de DTI con el encargado directo de la Administración de dicha información de las diversas áreas: caja, registro, contabilidad, presupuesto, etcétera.
4. El tiempo de vigencia de los accesos estará determinada por lo que estipule el administrador de la información, por inactividad o por terminación de sus funciones.
5. El obtener acceso a recursos no disponibles al público o el ingresar de manera no autorizada o ilegal a los sistemas computacionales o redes constituye una violación a esta política.
6. El uso o aceptación de información obtenida por medios ilegales constituye una violación a los derechos de los otros y esta sujeta a acción disciplinaria.



Sobre el software en los equipos

De la adquisición de software.

1. DTI y el Comité de Informática son los organismos oficiales para establecer los mecanismos de adquisición de sistemas informáticos.
2. Las adquisiciones de programas deberá ser con licencia de uso a favor de la UPNFM.
3. DTI propiciará la adquisición de licencias en cantidad, para obtener mejores ofertas económicas y de acorde a las necesidades de la universidad.
4. Corresponderá a DTI emitir los indicadores para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.
5. En cuanto a la paquetería sin costo deberá respetarse la propiedad intelectual intrínseca del autor.
6. DTI verificará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.
7. DTI deberá promover el uso de sistemas programáticos que redunden en la independencia de la institución con los proveedores.

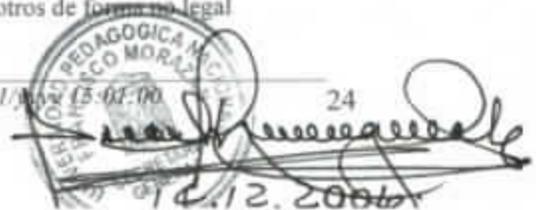
De la instalación de software.

1. Corresponde al Departamento de Sistemas de Información emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.
2. En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.
3. DTI es el responsable de brindar asesoría y supervisión para la instalación de software informático, así mismo para el software de telecomunicaciones.
4. La instalación de software que desde el punto de vista de DTI pudiera poner en riesgo los recursos de la institución, no está permitida.
5. Con el propósito de proteger la integridad de los sistemas informáticos, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, accesos, privilegios de uso en los equipos y otros que se apliquen). Los cuales no pueden ser desinstalados o cambiados por otro personal que no pertenezca a DTI.
6. No se permite la instalación de programas P2P¹ o similares que puedan poner en riesgo el rendimiento de la red en cuanto a saturación de enlaces o posibles ataques informáticos.
7. Las consecuencias que por instalaciones de Software - No aprobados por DTI - incurran en deterioro, fallas o cualquier otro causante de mal funcionamiento del equipo será responsabilidad directa de la persona a quien se le tiene asignado el equipo.

De la actualización del software.

1. La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo a la calendarización que sea propuesta por la DTI.
2. Corresponde a DTI autorizar cualquier adquisición y actualización del software.
3. Las actualizaciones del software de uso común para equipos de escritorio, como

¹ Programas para descarga de aplicaciones, música, videos, juegos u otros de forma no legal



las de herramienta ofimáticas, podrán ser realizadas por personal técnico de apoyo en los laboratorios o por el personal de DTI.

De la auditoria de software instalado.

1. DTI tiene la facultad de realizar revisiones periódicas para asegurar que sólo aplicaciones con licencia estén instaladas en las computadoras de la institución, pudiendo realizar limpieza (desinstalación) de aquellos programas que no se encuentren autorizados para su uso.
2. DTI propiciará la conformación de un grupo para la realización de las auditorias de sistemas de cómputo y sistemas de información.

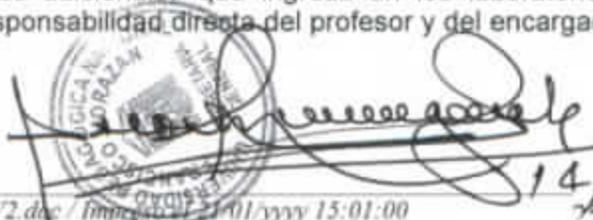
Del software propiedad de la institución.

1. Toda la programática adquirida por la institución sea por compra, donación o cesión es propiedad de la institución. Ella mantendrá los derechos que la ley de propiedad intelectual le confiera.
2. DTI en coordinación con el departamento de Activos deberá tener un registro de todos los paquetes de programación propiedad de la UPNFM.
3. Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfases) desarrollados con o a través de los recursos de la UPNFM se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.
4. Es obligación de todos los usuarios que manejen información institucional, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.
5. Las bases de datos de los sistemas de información de la institución deben estar resguardados por DTI.
6. Corresponderá a DTI promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos.
7. DTI en conjunto con el Comité de informática propiciará la gestión de patentes y derechos de creación de software propiedad de la institución.
8. La UPNFM se reserva el derecho a rehusarse a defender a cualquier empleado administrativo, personal docente o estudiante ante cualquier asunto legal relacionado a infracciones de las leyes de copyright o piratería de software.
9. DTI administrará los diferentes tipos de licencias de software y vigilará su vigencia.
10. No se prestará el software original a los usuarios directamente, sino a través de copias debidamente autorizadas o instalaciones directas por el personal de DTI.
11. Todo software o manual original deberá remitirse a DTI para su adecuada administración.
12. No se instalará ningún software excepto el permitido por la licencia correspondiente

Sobre el uso de software académico.

1. Cualquier software que requiera ser instalado para trabajar sobre la red de la universidad deberá ser evaluado por el personal del DTI.
2. Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la universidad.
3. El equipo o programas didácticos adicionales que ingrese en los laboratorios, como apoyo a una clase, será responsabilidad directa del profesor y del encargado del laboratorio.

De la propiedad intelectual.



14, 12, 2006.
25

1. Corresponde a DTI procurar que todo el software instalado en los equipos de la universidad estén de acuerdo a la ley de propiedad intelectual a que dé lugar.

De la Publicación Web (www.upnfm.edu.hn)

Se establece una reglamentación especial denominado "Reglamento de Publicación en la Pagina Web Institucional", del cual se desprenden estas disposiciones generales:

1. DTI a través del departamento de sistemas de Información es el responsable de instalar y administrar el o los servidor(es) Web. Es decir, sólo se permiten servidores de páginas autorizados por DTI y el consejo de Informática.
2. A los administradores de los diversos sitios que se hospedan bajo el dominio de la universidad, corresponde realizar los cambios para luego ser publicados por el webmaster de DTI.
3. Toda la programación involucrada en el desarrollo Web deberá estar de acuerdo con la tecnología con la que cuenta DTI.
4. El material que aparezca en el sitio de Internet deberá respetar los lineamientos del "Reglamento para la Publicación en la Página Web Institucional", la cual se encuentra en este documento.
5. En concordancia con la libertad de investigación, se acepta que en el sitio Web pueda ponerse información individual (siempre y cuando no contravenga las disposiciones de la institución), pero deberá llevar el enunciado siguiente: "Las expresiones, opiniones o comentarios que aquí aparecen pertenecen al autor individual y no necesariamente a la UPNFM"; no debe llevar el logotipo oficial de la institución y deberá siempre responder a un comportamiento profesional y ético.

Del uso del equipo en los laboratorios

Los siguientes lineamientos serán tomados como base para establecer el uso de los computadores personales de los diversos Laboratorios de Cómputo que la universidad posee.

El siguiente comportamiento está prohibido:

1. Permanecer como espectadores en el laboratorio y/o estar más de una persona por máquina, salvo que el profesor de la asignatura así lo autorice.
2. Consumir alimentos, bebidas o fumar dentro del laboratorio.
3. Utilizar servicio de voz, sonido o imagen no autorizados.
4. Usar lenguaje soez dentro del laboratorio y/o en la comunicación de Internet.
5. Demorar la entrega de máquina cuando sea solicitado por el profesor o supervisor del laboratorio.
6. Conectar periféricos o instalar software al equipo sin previa autorización del encargado del laboratorio.
7. Hablar en voz alta o ninguna otra actividad que perturbe el ambiente de estudio y trabajo.
8. Sentarse en las mesas, el piso y otros lugares no apropiados.
9. Instalar juegos y jugar en las computadoras.
10. Consultar y/o desplegar cualquier tipo de erotismo o de pornografía.
11. Mover máquinas, equipos, cables u otros elementos propios del laboratorio, sin supervisión y autorización del encargado del laboratorio.
12. Utilizar el equipo de para piratería o acceso no autorizado (hacking) a servidores propios o ajenos.
13. Borrar Software instalado de la Universidad.
14. Irrespetar de palabra o acción a los supervisores o encargados del Laboratorio.
15. Sustraer equipos del laboratorio.



16. Realizar acción voluntaria que cause daño a los equipos del laboratorio.
17. Causar daños o perjuicios a terceras personas
18. Otras, que afecten en forma grave el funcionamiento del laboratorio.

Aspectos Generales

1. El principio básico de seguridad en la red de la UPNFM será: *"Lo que no se permite expresamente, esta prohibido"*
2. El personal de DTI y cualquier otra persona con acceso a la información de los sistemas de la UPNFM, deberá de conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.
3. La UPNFM no es responsable de los contenidos que los usuarios posean en los directorios particulares en la red o en sus equipos (discos duros).
4. La confidencialidad y privacidad serán respetados por el personal de DTI hasta el mayor punto posible. Los equipos, el correo electrónico y los archivos electrónicos solo podrán ser accedidos por el personal autorizado por motivos pertinentes a la operación del sistema y por razones de seguridad.
5. Se prohíbe la utilización de las tecnologías de información de la UPNFM para el acceso no autorizado, destrucción, alteración, desmantelamiento, desfiguración, o deshabilitación de cualquier recurso institucional de información, propagación de virus, ataques o acoso a otros usuarios electrónicamente, el cometimiento de un crimen o actividad ilegal.

Responsabilidades Individuales

1. Los usuarios que utilicen algún servicio informático de la universidad, acuerdan que al usar estas facilidades aceptan cumplir con los lineamientos establecidos en este manual y otorgan a la institución el derecho de implementar estas políticas y condiciones de uso.
2. Se debe ser conciente de las necesidades de los demás y por tanto usar de manera razonable los recursos asignados respetando la intimidad y los derechos personales de los otros.
3. Los usuarios se comprometen a proteger sus recursos: Guardar el secreto de sus *cuentas y contraseñas*, no prestar su clave bajo ninguna circunstancia.

Sanciones

1. Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por DTI.
2. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.
3. Corresponderá al consejo de Informática hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la institución.
4. Todas las acciones en las que se comprometa la seguridad de la Red y que no estén previstas en esta política, deberán ser revisadas por DTI y el consejo de Informática para dictar una resolución sujetándose al estado de derecho.



[Handwritten signature]
14,12,2006.

AI PERSONAL ADMINISTRATIVO Y DOCENTE

1. Faltas Leves

- 1.1. Daños al equipo sin mal-intencionalidad evidente, que no son producidos por el uso normal del mismo, como ser: descuido, ignorancia de uso u otros.
- 1.2. Dar mantenimiento a equipo ajeno al de la Universidad, empleando los instrumentos, tiempo y/o accesorios pertenecientes a la institución.
- 1.3. El obtener acceso a la red de forma no autorizada.
- 1.4. El prestar o hacer uso de contraseñas que en principio han sido asignadas otro usuario para el acceso a Internet o a algún sistema de información.
- 1.5. Realizar pagos por concepto compra o actualizaciones de licencias de Software sin las autorizaciones de las autoridades correspondientes.
- 1.6. La desinstalación de software necesario para los equipos como ser los antivirus o el de los aplicativos que son empleados en la institución.
- 1.7. La instalación de Software no licenciado y no autorizado por las autoridades de la universidad (ViceRectoría Administrativa, DTI).
- 1.8. La instalación de software que degenere el rendimiento de los equipos o de la red, como ser programas para descarga (video, música, software), P2P, juegos, barras para Internet, otros.
- 1.9. El emplear video y voz por medio de nuestro enlace de comunicación de forma no autorizada.
- 1.10. Fallas producida por consecuencia de instalaciones de Software - No aprobados por DTI -, fallas o cualquier otro causante de mal funcionamiento del equipo.

2. Faltas Graves

- 2.1. Conexión de equipos ajenos a la Universidad y que por su naturaleza o condición, generen problemas de comunicación dentro de la red UPNFM o infección masiva de virus en los equipos.
- 2.2. Por daño en equipos que fueron manipulados por personal ajeno a DTI o que actuó sin la autorización correspondiente.
- 2.3. Comprar equipo sin el dictamen que emite DTI.
- 2.4. La reinstalación del Sistema Operativo con propósito de liberar las restricciones que DTI ha emitido como estrategia de aseguramiento y control de aplicaciones.
- 2.5. Mandar a reparación de forma directa a un proveedor o taller de reparación, un equipo sin previa revisión del departamento técnico de la universidad.

3. Faltas Muy Graves

- 3.1. Daño a equipo y/o información, con intencionalidad demostrada.
- 3.2. Avería, desconfiguración o cualquier otro daño en los equipos que se encuentran en los gabinetes de las diversas unidades y que son necesarios para la comunicación de la red.
- 3.3. Que sea demostrado que un equipo ha sido ultrajado intencionalmente en sus partes, y no se encuentren registros de dicha acción.

14, 12, 2006.

- 3.4. Acceso a un equipo de terceros sin autorización del responsable directo del equipo por medio de mecanismos de acceso remoto o cualquier otro a fin de tomar el control, alterar o distorsionar la labor de la persona afectada.
- 3.5. El uso o aceptación de información obtenida por medios ilegales constituye una violación a los derechos de los otros y esta sujeta a acción disciplinaria.
- 3.6. El obtener acceso a recursos o el ingresar de manera no autorizada a los servidores y sistemas computacionales.

Cualquier otro que no se encuentre considerado en éste, será evaluado por DTI y el Consejo de Informática.

AI ALUMNADO

1. Faltas Leves

- 1.1. Permanecer como espectadores en el laboratorio y/o estar más de una persona por máquina, salvo que el profesor de la asignatura así lo autorice.
- 1.2. Demorar la entrega de máquina cuando sea solicitado por el profesor o supervisor del laboratorio.
- 1.3. Conectar periféricos o instalar software al equipo sin previa autorización del encargado del laboratorio.
- 1.4. Hablar en voz alta o ninguna otra actividad que perturbe el ambiente de estudio y trabajo.
- 1.5. Sentarse en las mesas, el piso y otros lugares no apropiados.
- 1.6. Instalar juegos y jugar en las computadoras.
- 1.7. Consultar y/o desplegar cualquier tipo de erotismo o de pornografía.
- 1.8. Borrar Software instalado de la Universidad.
- 1.9. Escuchar música, ver video o cualquier otra acción de distracción que no corresponde al contenido de la clase.

2. Faltas Graves

- 2.1. Consumir alimentos, bebidas o fumar dentro del laboratorio.
- 2.2. Utilizar servicio de voz, sonido o imagen no autorizados.
- 2.3. Usar lenguaje soez dentro del laboratorio y/o en la comunicación de Internet.
- 2.4. Mover máquinas, equipos, cables u otros elementos propios del laboratorio, sin supervisión y autorización del encargado del laboratorio.
- 2.5. Utilizar el equipo para piratería o acceso no autorizado (hacking) a servidores propios o ajenos

3. Faltas Muy Graves

- 3.1. Irrespetar de palabra o acción a los supervisores o encargados del laboratorio.
- 3.2. Sustraer equipos del laboratorio sin autorización o sin control establecido en el departamento.
- 3.3. Realizar acción voluntaria que cause daño a los equipos del laboratorio.
- 3.4. Causar daños o perjuicios a terceras personas.

Cualquier otro que no se encuentre considerado en éste, será evaluado por DTI y la DISE.



REGLAMENTO PARA LA PUBLICACIÓN EN LA PÁGINA WEB INSTITUCIONAL

Alcance y Definiciones

Artículo 1.- Este Reglamento tiene como objetivo dictar las políticas que se deberán seguir al crear, publicar y mantener una sección en cualquier servidor de World Wide Web (Web) de la Universidad Pedagógica Nacional Francisco Morazán (UPNFM), que sea administrado por la Dirección de Tecnologías de Información.

Artículo 2.- Al utilizar el servicio de publicación electrónica ofrecido por la UPNFM, los usuarios aceptan las políticas, normas y estándares que aquí se establecen. De igual forma, pueden existir reglamentos que añadan más políticas para situaciones específicas de este servicio, pero que no contradigan las aquí descritas.

Artículo 3.- Definiciones

Conjunto de Información (En adelante "Información")

Es el grupo de archivos en formato impreso o digital de los cuales se compone una publicación.

Directorio de publicación (En adelante "Sección")

Se entiende por sección, a la *información* colocada en cualquier servidor Web de la UPNFM, y que se ubique dentro de un directorio con un nombre específico y adecuado al contenido de la misma. La finalidad de esta información es nutrir a las personas que visiten las Páginas Web de la UPNFM, con datos útiles sobre la Universidad; el Campus, sus actividades,

Cuenta de Publicación

Se entiende por Cuenta de Publicación, un espacio para la *sección* que ha sido habilitada para ser accesible desde un servidor web.

Artículo 4.- Este Reglamento se basa en las políticas establecidas por la Dirección de Tecnologías de Información sobre Normas, Políticas y Procedimientos de Sistemas de Información y se complementa con el Reglamento Institucional sobre el Uso de Internet aprobado por el Consejo Superior Universitario.

Artículo 5.- Se entiende por Administrador de Servicios Web (Webmaster), a la persona designada por la Dirección de Tecnologías de Información, para mantener y vigilar el buen funcionamiento de los servidores web, tanto en equipo como en programas.

Artículo 6.- Se entiende por Responsable de la Recopilación de la Información para la publicación en la Web (Encargado de Información), a la persona designada por el Departamento de Protocolo y Ceremonias, para obtener, ordenar, documentar, digitalizar la información generada en la institución en temas relacionados con eventos, grupos estudiantiles y noticias, con el propósito de auxiliar y coordinar con el Webmaster los esfuerzos para publicar información en las secciones del servidor y observar el cumplimiento de las normas contenidas en este reglamento



4/12/2006

De la Información

Artículo 7.- La publicación de información en los servidores de la UPNFM considera tres aspectos fundamentales:

Imagen institucional

Proporcionada y regulada por el Departamento de Protocolo y Ceremonial.

Funcionalidad y estética

Proporcionada y regulada por el Administrador de la Tecnología Web.

Contenido

Proporcionado por el responsable o el encargado de la sección de acuerdo al Artículo 9 y cumpliendo con lo establecido en el presente reglamento.

El contenido de la información que se desee publicar debe provenir de alguna de las siguientes fuentes:

1. *Rectoría:* Cualquier unidad académica, administrativa, técnica que dependa de la Rectoría.
2. *Vicerrectoría Académica:* Los departamentos académicos adscritos a alguna de las facultades. Los programas y proyectos académicos.
3. *Vicerrectoría del CUED:* las administraciones de sede y las unidades académicas y administrativas adscritas.
4. *Vicerrectoría de Investigación y Postgrado:* Unidades académicas y administrativas dependientes de esta Vicerrectoría.
5. *Dirección del Centro Regional de San Pedro Sula:* Unidades académicas y administrativas dependientes de esta Dirección.
6. *Grupos Estudiantiles:* Asociaciones regionales, sociedades de alumnos o grupos diversos reconocidos por la UPNFM.
7. *Páginas académicas* de personal docente y administrativo.
8. *Páginas académicas* de alumnos solicitadas por personal docente de la UPNFM.

Artículo 8.- Se prohíbe la publicación de todo lo estipulado por las leyes internacionales, estatales e institucionales vigentes, así como la publicación de información privada o secreta, calumnias, injurias o difamaciones contra cualquier persona física o moral. Además de cualquier información de carácter comercial o que persiga fines de lucro. La UPNFM no se responsabiliza por éstas cuestiones, por lo que se prohíbe la colocación de información de este tipo que pueda dañar la imagen individual o de la institución misma.

El uso de los servicios web queda prohibido para realizar cualquiera de las siguientes actividades:

1. Colocar material que sea ofensivo para la comunidad, esto incluye frases groseras, subversivas, racistas o similares.
2. Promover y/o proveer información acerca de actividades ilegales.
3. Desplegar material que muestre o promueva el abuso en cualquier forma.
4. Promover el daño físico, emocional o psicológico de un grupo o un individuo.
5. Utilizar las páginas con propósitos comerciales, incluyendo pero no limitándose a las siguientes:
 - Ofrecer para su venta cualquier producto o servicio;

- o Solicitar patrocinadores o publicistas que originen o no un ingreso económico, promoviendo actividades personales o que no tengan fines académicos.
 - o Desplegar imágenes, "banners" o logotipos comerciales de cualquier clase con o sin enlaces.
 - o Enlazar imágenes de intercambio de sitios comerciales (link exchange).
 - o Promocionar o solicitar participación en ventas, rifas y/o actividades similares.
 - o Promocionar servicios o actividades que impliquen algún ingreso económico.
6. Desplegar o enlazar material que contenga desnudos, o cualquier tipo de pornografía.
 7. Desarrollar material restringido por accesos con password.
(Excepto con autorización del Consejo de Tecnologías de Información).
 8. Desarrollar páginas o imágenes ocultas o aquellas que no puedan ser accesibles desde un lugar visible.
 9. Colocar páginas incompletas (en construcción) que generen errores o confusión.
 10. Utilizar el espacio asignado como unidad de almacenamiento o para subir o bajar archivos de otros servidores, con o sin fines de lucro.
 11. Usar las páginas para infringir los derechos de autor, incluyendo piratería o enlaces a lugares que lo contengan o lo promuevan, así como archivos en formato MP3 o similares, información o publicación de números de serie o de registro de programas, o cualquier tipo de actividad o utilidad para romper las protecciones.
 12. Violar los estándares de Internet con el propósito de promover las páginas y/o desarrollar páginas que consistan en ligas "hiperlinks", a lugares no permitidos por este reglamento.
 13. Publicar información no relevante para los fines académicos de la institución, incluyendo páginas personales, aficiones, gustos o preferencias particulares, así como fotos de eventos sociales, viajes, mascotas, etc.

Artículo 9.- Por cada unidad y/o cuenta de publicación, deberá existir un responsable de la información, y uno o más encargados de mantener la misma actualizada. Para lo cual deberá coordinar esfuerzos con el Webmaster y el responsable nombrado por el Departamento de Protocolo y Ceremonial.

Artículo 10.- El responsable de la información de la sección, es la persona que avala y se responsabiliza del contenido, debiendo ser éste el director, coordinador, jefe o responsable de la unidad. El personal docente y los alumnos, son responsables de sus cuentas.

Artículo 11.- El (los) encargado(s) de la unidad, es (son) la(s) persona(s) que se encargará(n) de recolectar y actualizar la información en dicha unidad, debiendo cubrir los estándares dictados por el Departamento Protocolo y Ceremonial y por la Dirección de Tecnologías de Información.

Artículo 12.- Cada sección deberá contener una portada o página principal (Índice), la cual será ubicada con el URL (dirección web) que determine el Webmaster.

Artículo 13.- En cuanto al contenido de información de la sección. La página principal deberá contener los siguientes elementos como mínimo:

1. Una composición, de preferencia gráfica, aunque no excesivamente cargada (es decir, que no tenga un tamaño excesivo en 256 KB, para hacer la página accesible vía módem), que identifique la fuente originaria de la información.
2. Enlaces a los siguientes URLs (direcciones web) , según a donde corresponda la sección:
 - o Al servidor upnfm.edu.hn, eventualmente, a los servidores web upnfm.edu.hn, cursps.upnfm.edu.hn, y postgrado.upnfm.edu.hn.



- Nombre y cuenta de correo de la persona responsable de la información de la unidad.
- Nombre(s) y cuenta(s) de correo del (los) encargado(s) de la unidad, en caso de ser diferente(s) al responsable de la información.
- Fecha de la última modificación realizada a la sección, no importa si se desea a la vista u oculta dentro del código HTML como un comentario.

Artículo 14.- Toda información que se encuentre en las diferentes secciones, debe ser revisada por el responsable de la información, ya que con esta persona se aclarará cualquier aspecto referente al contenido de ésta. Estas aclaraciones provendrán directamente de la Rectoría, de la Dirección de Tecnologías de Información, del Departamento Protocolo y Ceremonial y/o de los Administradores de Tecnología Web.

Artículo 15.- En cuanto al diseño de las páginas, cada entidad tendrá que ajustarse al diseño propuesto por la Dirección de Tecnologías de Información, tomando en cuenta las siguientes observaciones:

- Se debe tener un enlace para regresar a la página principal en todos los documentos, así como las estipuladas en el [Artículo 13](#).
- Utilizar un estilo determinado para crear consistencia visual en todos los documentos relacionados.
- Utilizar pequeños gráficos que identifiquen a todos los documentos de la sección.
- Que las páginas sean pequeñas y sencillas.
- No utilizar gráficos excesivamente grandes o muchos gráficos pequeños.
- Utilizar botones o imágenes que señalen ligas de interés.
- Utilizar el mínimo de texto en listas o menús.
- Utilizar la leyenda de derechos de autor (D.R., Copyright) cuando sea apropiado y/o necesario.
- Indicar el grado de avance del documento (por ejemplo: Página en construcción, Prototipo, etc.), esto no significa que la página pueda estar incompleta o con errores.
- Tener una Sección de Novedades dentro de la página principal sólo en el caso de ser necesaria.
- Indicar con una advertencia si algún enlace va a llevar a un documento o imagen grande, y señalar el tamaño en KB.
- No utilizar terminología/etiquetas HTML/PHP específicas para cierto Browser en particular.
- Utilizar como guía de estilo general para las páginas de 1er y 2do nivel, las plantillas que se proporcionan dentro de las páginas Web de la UPNFM. A partir del 3er nivel, las restricciones de uso de la Imagen Institucional no serán tan rígidas, sólo se pide mantener una buena estética, consistencia y no abusar del tamaño en KB.
- Pensar siempre en los usuarios - hacer una prueba preliminar con un grupo de usuarios para observar la facilidad de navegación, lógica de uso y tiempos de acceso.
- En las páginas del Sitio colocar en todas las páginas el siguiente pie de página:

© D.R. Universidad Pedagógica Nacional Francisco Morazán
<http://www.upnfm.edu.hn>

Servicios Web
webmaster@upnfm.edu.hn



Artículo 16.- En el caso de páginas académicas (personal administrativo, profesores y alumnos), que por su naturaleza pudieran contener alguna información privada o personal, deberán incluir en su página principal una leyenda que aclare que la información contenida en sus páginas, tanto texto como enlaces, son responsabilidad de la persona y no expresan el punto de vista de la UPNFM, ni de la DTI o alguna de sus divisiones, o hacer una liga a la página de Términos de uso (*disclaimer*) que se encuentra en el anexo 1 del presente reglamento. Lo anterior no es de ninguna manera un permiso para poder publicar aquello que se estipula en el Artículo 8.

De las Facilidades Ofrecidas para la Administración de Servicios Web.

Artículo 17.- Las facilidades ofrecidas por la Dirección de Tecnologías de Información a través de la Administración de Servicios Web, para las personas o entidades que deseen publicar información en los servidores de la UPNFMWeb, son las siguientes:

1. Servicios de WWW para la UPNFM y páginas académicas.
2. Cuentas de publicación para la creación de secciones, las que se harán una vez cada seis meses de forma rutinaria y por demanda cuando se requiera.
3. Asignación y activación de direcciones URL.
4. Un directorio con documentos de apoyo.
5. Grupos de discusión news:news.upnfm.edu.hn.
6. Aplicaciones para el funcionamiento de las secciones.
7. Diseño de páginas en función de la versión activa.

La Administración de Servicios Web no provee los siguientes servicios:

1. Generación de contenidos para publicación de páginas ajenas a la Dirección de Tecnologías de Información y el Departamento de Sistemas de Información.
2. Mantenimiento y/o actualización del contenido de las secciones.
3. Promoción de páginas o eventos por ningún medio.
4. Soporte a páginas colocadas en servidores ajenos al UPNFMWeb.
5. Soporte a servidores particulares dentro o fuera del campus.

Artículo 18.- El Webmaster hará respaldos mensuales de toda la información contenida en el servidor, conservando únicamente la última versión, por lo que, en caso de que el usuario borre o pierda su información, los Administradores no serán responsables de recuperarla. Se le recomienda a cada unidad usuaria del servicio que tenga respaldos propios de toda la información publicada en sus páginas.

De la Asignación de Espacio

Artículo 19.- Para tener un espacio en el servidor WWW de la UPNFM se deberá:

1. Leer y entender el presente reglamento.



14,12,2006

2. Consultar y seguir el procedimiento para solicitud de espacio descrito en la Solicitud de activación de cuenta de publicación (ver anexo 3).
3. Seguir cuidadosamente las recomendaciones del Artículo 15 (para páginas del campus elaborarlas de acuerdo a las plantillas proporcionadas por la Dirección de Tecnologías de Información)
4. Contactar al Webmaster, donde se le indicará la cuenta de publicación, en la cual podrán colocar su información, así como el URL en el cual se podrá acceder dicha información. Se otorgará un plazo máximo de un (1) mes a partir del aviso de la creación del directorio, para colocar la información en la cuenta solicitada.

Artículo 20.- Es obligación del responsable de cada sección, optimizar el espacio que tiene asignado en la cuenta de publicación, se sugiere no subir información irrelevante o redundante sobre cierto tema, así como que cada cierto tiempo haga una limpieza de sus archivos, retirando aquellos que ya no le sean de utilidad. No se permite a nadie por ningún motivo, tener información personal en las secciones ya que no son destinadas para tal efecto. De igual forma, es obligación de los profesores dar las indicaciones necesarias, para que los alumnos puedan elaborar y colocar sus documentos, la Administración de Servicios Web no dará asesoría individual a cada alumno.

Artículo 21.- La asignación de cuotas de espacio se hará de la siguiente manera:

- A las Vicerrectoría, direcciones, centros, facultades, departamentos y unidades académicas y administrativas se les asignará una cuota de 2Mb (o lo que estipule la Administración de Redes al momento de la asignación).
- A las sociedades de alumnos, asociaciones, alumnos, personal del campus, grupos diversos y materias de cualquier carrera se les asignará una cuota de 1Mb (o lo que estipule la Administración de Redes al momento de la asignación).

En caso de que se requiera tener más espacio del asignado, se deberá solicitar siguiendo el procedimiento descrito por la Administración de Redes para el aumento de cuota.

De las Obligaciones de los Responsables y Encargados de las Páginas

Artículo 22.- Por ningún motivo se podrá cambiar el nombre del directorio o carpeta dado por el Webmaster, solamente podrán cambiar los nombres de los directorios creados por los encargados dentro de la sección asignada. En caso de que se requiera cambiar la dirección URL asignada, se enviará una solicitud por correo electrónico al Webmaster explicando el motivo por el cual se requiere el cambio, y éste hará las modificaciones necesarias en caso de considerarse pertinente.

Artículo 23.- El responsable de la información del Departamento de Protocolo y Ceremonial, deberá revisar toda información antes de que ésta sea publicada, ya que a él se dirigirá el Webmaster en caso de que haya cualquier aclaración con respecto al contenido de la sección.



Artículo 24.- El responsable de la información de cada sección deberá asegurarse de que obtener el visto bueno del Departamento de Protocolo y Ceremonial, siendo el responsable de que se publique y mantenga actualizada la información de cada sección asignada. La publicación y actualización de contenidos en las páginas no depende del Webmaster.

Artículo 25.- El responsable de la información deberá confirmar al final de cada semestre o a más tardar durante la semana siguiente a inscripciones del semestre siguiente, si desea seguir conservando su sección en el Web y/o si desea hacer cambios. Está confirmación deberá hacerse vía e-mail al Webmaster.

De las Amonestaciones y Sanciones

Artículo 26.- Se define como amonestación a toda llamada de atención realizada a cualquier persona involucrada en la sección cuando hayan incurrido en violaciones a este reglamento.

Artículo 27.- Se define como sanción a toda acción correctiva realizada por el Webmaster derivada de la violación de este reglamento por parte de cualquiera de las personas involucradas en la sección. Las sanciones pueden resultar en la suspensión temporal de la Sección, la cancelación definitiva de su cuenta, o las medidas que dicte la Dirección de Tecnologías de Información o El Consejo de Tecnologías de Información.

Artículo 28.- Es motivo de sanción realizar cualquiera de las siguientes actividades:

- Infringir lo dispuesto en los artículos 8, 11, 12, 13, 15, 20, 22, 23, 24, 32 y 33.
- La violación directa o indirecta de cualquier artículo del presente reglamento.

Si alguno de los encargados de la sección cambia el nombre al directorio dado por la Administración de Servicios Web, se sancionará al responsable de la sección y se devolverá a los volúmenes su nombre original. En caso de que se vuelva a incurrir en la misma violación, se sancionará con la cancelación de su cuenta de publicación, y éste no podrá volver a ser solicitado hasta el siguiente período académico en un lapso no menor a seis meses.

Artículo 29.- Si en un período de un (1) mes a partir del aviso de la creación del directorio solicitado no se ha publicado ninguna información, se cancelará su espacio y éste no podrá volver a ser otorgado hasta el siguiente período académico.

Artículo 30.- Los directorios o carpetas que no sean actualizados, con o sin aviso previo de la Administración de Servicios Web, serán dados de baja y no se conservará respaldo de la información ahí contenida.

Artículo 31.- El Consejo de Tecnologías de Información, a partir de dictamen del Webmaster, se reserva el derecho de suspender o cancelar las secciones, direcciones, cuentas o servidores que a su juicio contravengan el presente reglamento, aún cuando la falta cause controversia y aún no exista un dictamen por parte del Comité de Tecnologías de Información u otro órgano competente que se defina para realizar la aplicación del presente reglamento.

De la Creación de un Servidor

Artículo 32.- El establecimiento de un servidor propio por parte de cualquiera de las fuentes de información citadas en el Artículo 7, requiere ser registrado y autorizado por la Vicerrectoría Administrativa, previo dictamen de la Dirección de Tecnologías de Información; además queda entendido que toda información que sea necesaria para la Universidad deberá ser colocada dentro de las páginas oficiales www.upnfm.edu.hn, cued.upnfm.edu.hn, cursps.upnfm.edu.hn, postgrado.upnfm.edu.hn o cualquier otro servidor administrado por el Webmaster. Información que no se considere relevante, puede ser colocada en otro servidor, siempre y cuando no contradiga el Artículo 8 del presente reglamento y cuente con el registro y autorización correspondientes.

Artículo 33.- El responsable del servidor propio, permitirá el acceso irrestricto a la totalidad de secciones, al Webmaster, quién tendrá facultad de supervisar el contenido del servidor.

Artículo 34.- El Webmaster no se hará responsable del mantenimiento de servidores ajenos ni prestará servicio o asesorías, ya que está a cargo exclusivamente de servidores bajo la responsabilidad de la Dirección de Tecnologías de Información.

De las Publicaciones en Servidores Externos

Artículo 35.- La publicación de información en servidores externos UPNFMWeb, no requiere la autorización pero si requiere ser registrado con el Webmaster, de acuerdo a lo estipulado en los artículos 17, 32 y 34.

Artículo 36.- Las publicaciones en servidores externos están reguladas por el presente reglamento, siempre que en cualquier parte de su contenido esté expresado directa o indirectamente la UPNFM, cualquiera de sus unidades académicas o administrativas, eventos o actividades.

Artículo 37.- Si existe una publicación en un servidor externo, el Webmaster cancelará cualquier cuenta de publicación en los servidores de la Institución, que contengan la misma información; con el objeto de evitar confusión e inconsistencia en el contenido y su actualización.

Artículo 38.- Queda estrictamente prohibido, que una página dentro de los servidores de la Institución o que una página en un servidor externo (que haga referencia a la UPNFM), tenga un enlace a otra página que infrinja lo estipulado en el Artículo 8.

Las páginas de la UPNFM, no serán enlazadas a servidores externos que no tengan relación alguna con actividades académicas. Incluyendo, pero no limitándose, a servidores de servicios gratuitos que contengan o no publicidad comercial.

Artículo 39. De llegarse a presentar cualquier caso no considerado en estas políticas, éste se someterá a la decisión definitiva de un comité integrado por el Comité de Tecnologías de Información.



Anexo 1. Términos de Uso

Términos y Condiciones

El acceso a y/o uso del Sitio Web de la UPNFM (el "Sitio Web") requiere que todos los visitantes al mismo se adhieran a los Términos y Condiciones, aceptándolos, desde ese momento, plenamente y sin reserva alguna, así como en su caso, las Condiciones Particulares que en el futuro puedan complementarias, sustituir las o modificarlas en algún sentido en relación con los servicios y contenidos del Sitio Web. Por el solo hecho de ingresar y hacer uso de este Sitio Web, usted (el "Usuario") se adhiere en forma inmediata a todos y cada uno de los siguientes Términos y Condiciones. En consecuencia, el Usuario deberá leer detenidamente los Términos y Condiciones así como las Condiciones Particulares, que pudieran dictarse, antes de acceder y/o utilizar cualquier servicio del Sitio Web bajo su entera responsabilidad.

Modificación unilateral del Sitio Web

La UPNFM se reserva el derecho de, en cualquier momento y sin necesidad de previo aviso, modificar o eliminar el contenido, estructura, diseño, servicios y condiciones de acceso y/o uso de este Sitio Web.

Legislación

El ingreso y utilización de este Sitio Web se encuentra sujeto a las disposiciones aplicables de la legislación interna de la UPNFM, a las leyes vigentes en Honduras.

Uso del Sitio Web. Exclusión de Garantías

El Usuario se compromete a utilizar el Sitio Web y sus servicios y contenidos sin contravenir la legislación aplicable, la buena fe y el orden público. En consecuencia, queda prohibido todo uso con fines ilícitos o que perjudiquen o impidan, puedan dañar y/o sobrecargar, de cualquier forma, la utilización y normal funcionamiento del Sitio Web que directa o indirectamente atenten contra el mismo o contra cualquier derecho de un tercero.

Debido a que alguna de la información proporcionada en el Sitio Web es provista para el Usuario "en la forma que se encuentra", la UPNFM no garantiza la exactitud o conveniencia para fines especiales, no haciéndose responsable por la veracidad, precisión o exactitud de toda aquella información suministrada en el Sitio Web. En virtud de lo expuesto, la UPNFM no asume responsabilidad alguna por cualquier perjuicio, costo, daño o pérdida de ninguna naturaleza originado como consecuencia de la falta de utilidad, adecuación y/o validez del contenido del Sitio Web para satisfacer necesidades, actividades y/o resultados concretos y/o expectativas de los Usuarios. Recomendamos al Usuario verificar con adecuado asesoramiento profesional la exactitud de cualquier información suministrada en el presente Sitio Web.

Responsabilidades

La UPNFM no asume ningún tipo de responsabilidad que se derive de cualquier daño y/o perjuicio de cualquier naturaleza que se pudieran originar al Usuario como consecuencia o de cualquier forma relacionada con:

- El acceso o utilización de este Sitio Web, incluyendo la responsabilidad relacionada con daños ocasionados por virus, programas maliciosos o lesivos en los contenidos y/o cualquier otro agente que pueda llegar a infectar o afectar de cualquier modo el o los sistemas de computación utilizado por el Usuario.
- El incumplimiento por parte de terceros de sus obligaciones o compromisos en relación con los servicios prestados a los usuarios a través del Sitio Web.
- La falta de legalidad, calidad, veracidad, utilidad y disponibilidad de los servicios prestados por terceros y puestos a disposición de los usuarios del Sitio Web.
- La falta de disponibilidad, continuidad, acceso, mantenimiento y efectivo funcionamiento del Sitio Web y/o de sus servicios y/o actualización, exactitud, exhaustividad, pertinencia, actualidad y fiabilidad de sus contenidos, cualquiera sea la causa, y las dificultades o problemas técnicos o de otra naturaleza en los que tengan su origen dichos hechos.
- La recepción, obtención, almacenamiento, difusión y/o transmisión, por parte de los Usuarios, de los contenidos del Sitio Web.

El Sitio Web incluye dentro de sus contenidos enlaces con sitios pertenecientes y/o gestionados por terceros con el objeto de facilitar el acceso a información disponible a través de Internet. La UPNFM no asume ninguna responsabilidad derivada de la existencia de enlaces entre los contenidos de este sitio y contenidos situados fuera del mismo o de cualquier otra mención de contenidos externos a este sitio.



Tales enlaces o menciones tienen una finalidad exclusivamente informativa y, en ningún caso, implican el apoyo, aprobación, comercialización o relación alguna entre la UPNFM y las personas o entidades autoras y/o gestoras de tales contenidos o titulares de los sitios donde se encuentren. En este sentido el Usuario se obliga a poner la máxima diligencia y prudencia en el caso de acceder o usar contenidos o servicios de los sitios a los que acceda en virtud de los mencionados enlaces.

La enumeración anterior tiene mero carácter enunciativo y, en ningún caso, exclusivo ni excluyente en ninguno de sus puntos. En todos los supuestos, la UPNFM excluye cualquier responsabilidad por los daños y perjuicios de cualquier naturaleza derivados directa o indirectamente de los mismos y de cualquier otro caso no especificado de análogos características.

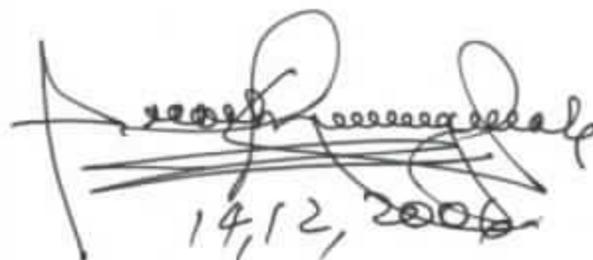
Hipervínculos

Condiciones que deben cumplir los usuarios que quieren establecer un hipervínculo entre su página web y el Sitio UPNFMWeb

- No se podrán reproducir las páginas del Sitio UPNFMWeb mediante el hipervínculo que, únicamente, permitirá el acceso a las páginas web del Sitio Web.
- Los hipervínculos sólo podrán establecerse con la home-page del Sitio Web y/o con las home-page correspondientes a las secciones primarias, y no con páginas distintas a las primeras páginas de los mismos, salvo previa y expresa autorización.
- En ningún caso se podrá dar a entender que este Sitio Web autoriza el hipervínculo o que ha supervisado o asumido de cualquier forma los servicios o contenidos ofrecidos por la página web desde la que se produce el hipervínculo.
- Se prohíbe explícitamente la creación de cualquier tipo de browser o border environment sobre las páginas del Sitio Web.
- No se podrán incluir contenidos contrarios a los derechos de terceros, ni contrarios al orden público ni a la moral y buenas costumbres, ni contenidos o informaciones ilícitas, en la página web desde la que se establece el hipervínculo.
- La existencia de un hipervínculo entre una página web y el Sitio Web no implica la existencia de relaciones entre la UPNFM y el propietario de esa página ni la aceptación y aprobación de sus servicios y contenidos.
- La UPNFM se reserva el derecho de inhabilitar hipervínculos o estructuras no autorizados.

General

Los presentes Términos y Condiciones constituyen el entero acuerdo entre las partes y derogan cualquier acuerdo anterior entre las partes en esta materia. La declaración de que alguna de las disposiciones de estos Términos y Condiciones fuese inválida o no ejecutable, no tendrá efecto alguno respecto de las demás provisiones de estos Términos y Condiciones, las cuales permanecerán con total efecto y vigencia.



Handwritten signature and date: 14/12/2008

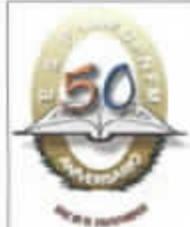


Anexo 2. Solicitud de cuenta de activación



UNIVERSIDAD PEDAGÓGICA NACIONAL FRANCISCO MORAZÁN
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

SOLICITUD DE ACTIVACIÓN DE CUENTA PARA PUBLICACIÓN



Datos Generales	
Nombre de la unidad solicitante	
Nombre del responsable	
Nombre, firma y sello de Jefe Inmediato o persona que Autorizada	
Cargo de quien autoriza	
Aspectos técnicos	
Objetivos de la solicitud	<ul style="list-style-type: none"> • . • . • .
Tipo de información que se va a publicar (Favor indicar el tipo de formato y tamaño)	
Responsable de la publicación	
Visto Bueno del Departamento de Protocolo y Ceremonial (Firma y sello)	
Visto Bueno de un representante del departamento de Letras y Lenguas (Firma y sello)	
Para uso dentro de la Dirección de Tecnologías de Información	
Fecha de la solicitud	
Nombre de quien recibe	
Fecha de publicación	
Numero de orden de trabajo	
Tiempo que estará activa la publicación	

14, 02, 2006

 14, 12, 2006

Anexo 3. Procedimiento para la Publicación de páginas Web

Antes de publicar debe leer las recomendaciones para elaborar un sitio web.

Para publicar una página en los servidores web de la UPNFM, debe seguir las indicaciones de acuerdo al tipo de página que desea colocar:

- Páginas académicas
- Páginas de grupos estudiantiles
- Páginas de eventos
- Páginas de unidades académicas y administrativas
- Creación de un Servidor propio

NOTA: En ningún caso se colocará un enlace desde la página principal, solo podrá colocarse un banner en la parte inferior que rotará alternándose con otros banners de tamaño igual a superior a 256k.

Recomendaciones para elaborar el sitio web

1. Lea detenidamente el Reglamento de Publicación.
2. Lea detenidamente el Procedimiento de Publicación correspondiente. (Unidades académicas y administrativas, Eventos, Académicas, y de Grupos Estudiantiles)
3. Determine el público a quien va dirigido (Profesores, Alumnos, Personal Administrativo, etc)
4. Determine lo que el público espera obtener de las páginas de su sitio web.
5. Determine los servicios que va a ofrecer en las páginas de web.
6. Defina los elementos más importantes.
7. Clasifique el contenido de acuerdo a los elementos más importantes.
8. Los sitios a elaborarse deberán ser implantados en plataforma de software libre con aplicaciones de código abierto, garantizando que el uso del mismo no implique pago de licencias u otros cargos por derechos de uso.
9. Estructure el sitio web.
10. Elabore la página principal.
11. Elabore la plantilla
12. Elabore el resto de las páginas.
13. Transfiera el sitio al servidor web correspondiente, vía FTP o según corresponda
14. Asigne derechos de lectura al público en general.

Páginas académicas

1. El profesor dará las indicaciones necesarias a sus alumnos para que ellos puedan elaborar sus tareas y colocar las páginas en el servidor. El área de servicios web **no** dará asesoría individual a cada alumno.
2. El profesor debe elaborar un archivo de texto con la lista de las matrículas (una por cada renglón) de los alumnos que publicarán páginas.
3. El profesor solicitará por correo electrónico a webmaster@upnfm.edu.hn la activación de las cuentas proporcionando la siguiente información: justificación del

uso, descripción del contenido y cuenta de correo electrónico en el campus, así como el archivo de texto con la lista de alumnos matriculados, durante el primer mes del semestre en que sean requeridas.

4. Los alumnos elaborarán las páginas ajustándose al Reglamento de Publicación.

Páginas de grupos estudiantiles

1. Obtener autorización escrita del director, coordinador o responsable del departamento de Desarrollo Estudiantil y del Departamento de Protocolo y Ceremonial.
2. Elaborar las páginas ajustándose al Reglamento de Publicación, siguiendo las recomendaciones del Departamento Protocolo y Ceremonial.
3. Solicitar personalmente la cuenta de correo electrónico del grupo estudiantil, al área de Soporte Técnico en Informática. (upnfm@upnfm.edu.hn)
4. Solicitar personalmente la activación de la cuenta para publicar en WEB al área de Servicios WEB en Informática, por lo menos 15 días antes de ser requerida
5. Obtener la aprobación escrita del Departamento de Protocolo y Ceremonial, de que la página esta aprobada para su publicación.

Páginas de eventos

Nota: Si el evento es organizado por un grupo estudiantil o por un departamento, vea el procedimiento de Páginas de grupos estudiantiles o el de Páginas de unidades académicas y administrativas.

1. Obtener autorización escrita del director, coordinador o responsable de la Unidad Correspondiente o de la Dirección de Servicios Estudiantiles.
2. Elaborar las páginas ajustándose al Reglamento de Publicación o solicitar el diseño al Departamento de Protocolo y Ceremonial.
3. Solicitar personalmente la activación de la cuenta para publicar en WEB al Departamento de Protocolo y Ceremonial.
4. Obtener la aprobación del Departamento de Protocolo y Ceremonial, de que la página esta aprobada para su publicación.

Páginas de Unidades Académicas y Administrativas

1. Obtener autorización escrita del director, coordinador o responsable de la unidad que desea publicar.
2. Elaborar las páginas ajustándose al Reglamento de Publicación o solicitar el diseño al Departamento de Protocolo y Ceremonial.
3. Solicitar personalmente la cuenta de correo electrónico de la unidad, al área de Soporte Técnico en Informática. (upnfm@upnfm.edu.hn)



4. Solicitar personalmente la activación de la cuenta para publicar en WEB al Departamento de Protocolo y Ceremonial.
5. Obtener la aprobación del Departamento Protocolo y Ceremonial, de que la página esta aprobada para su publicación.

Creación de un servidor propio

Para establecer un servidor propio se deberá cumplir con la totalidad de los siguientes puntos:

Cumplir Reglamentos	Cumplir con los reglamentos previstos para los servicios que se desean colocar, incluyendo pero no limitándose a: Telnet, FTP, Email, News, Chat, Web, Streaming, uso de Internet, uso de equipos, etc...
Aprobación de Imagen	Autorización de la Vicerrectoría Administrativa y el Consejo de Tecnologías de Información.*
Aprobación de Contenido	Autorización del responsable de la unidad correspondiente.*
Aprobación de Funcionalidad	Autorización de la Dirección de Tecnologías de Información

El servidor deberá ofrecer un servicio de valor agregado que no pueda ser ofrecido por ningún otro servidor ya existente.

El servicio deberá ser estrictamente para fines académicos.

El servicio no generará tráfico excesivo en la red.

El servidor permitirá el acceso irrestricto a la totalidad de los servicios, al Webmaster, quien tiene la facultad de supervisar el contenido y uso del servidor.

Firma de Carta de Responsabilidad por parte de quién estará a cargo del servidor.

Nota: La asignación de nombres en el servidor de resolución de nombres de dominio (DNS), estará sujeta a la disponibilidad de direcciones IP asignadas a la Universidad.

Nota: El cumplimiento de los puntos anteriores solo permite la creación de servidores "visibles" exclusivamente dentro del campus. Si el servidor requiere acceso del/al exterior, éste deberá ser ubicado en las instalaciones del cuarto de maquinas del departamento de Sistemas de Información las cuales han sido acondicionadas para tal efecto, quedando bajo el control del personal de dicho departamento.

Nota: Las limitaciones de los servidores existentes no son garantía de autorización de la creación de servidores propios, ya que los recursos y servicios deben ser de beneficio a la generalidad dentro de la Institución y no para beneficio de un pequeño grupo o individuo.

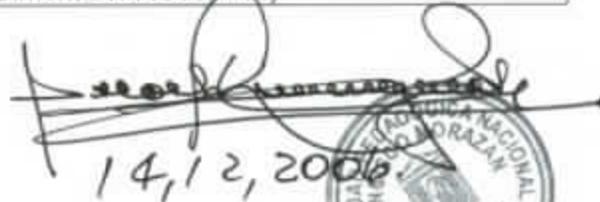
* Sujeta a las normas que estas entidades han establecido para este efecto.

UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA
SAN FRANCISCO DE QUITO
FACULTAD DE CIENCIAS ADMINISTRATIVAS
CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN
11/12/2008

Estándares manejados para este documento

Nomenclaturas

Término	Descripción / Explicación
UPNFM	Universidad Pedagógica Nacional Francisco Morazán
DTI	Dirección de Tecnología de Información
Freeware	Software Libre (con acceso ser descargado via Internet)
SW	Software
HW	Hardware
HelpDesk	Asistencia a usuarios (normalmente vía telefónica)

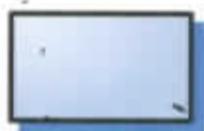

14, 12, 2006



En Diagramación



Decisión



Actividad / Proceso



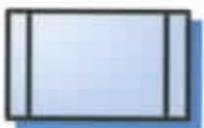
Flujo Proceso / Actividad



Conector Lógico



Documento Impreso



Llamada a procedimiento pre-establecido



[Handwritten signature]
14,12,2006.

Anexos

- [Orden de trabajo](#)
- [Control de Cambios en aplicaciones](#)
- [Formato de entrada y salida equipo al departamento.](#)
- [Bitácora de Respaldos](#)
- [Internet – Solicitud de Acceso](#)
- [Internet – Acta de Compromiso](#)
- [Asignación de equipo y herramientas – Uso interno.](#)

Handwritten signature and date: 14, 12, 2006. A circular official stamp is partially visible on the right side of the signature.