# Administración de contenido web en servicios centrales

| | | |
|---|---|---|
| **Versión** | : | 1.0 |
| **Preparado por** | : | SIT – Área de Seguridad |
| **Preparado para** | : | Pontificia Universidad Católica de Chile |
| **Autor** | : | Andres Altamirano, Ivan Llanos |
| **Fecha creación** | : | 08/04/2010 |
| **Última modificación** | : | 25/05/2010 12:39 |
| **Revisado por** | : | Paulina Contreras, Iñigo Meza |
| **Nombre del Documento** | : | Administracion de Contenido Web.docx |

# HISTORIA DE REVISIONES

| *REV.* | *VER.* | *FECHA* | *AUTOR* | *OBSERVACIONES* |
|---|---|---|---|---|
| **1** | **1.0** | **08/04/2010** | **Andres Altamirano, Ivan Llanos** | **Versión Inicial** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# TABLA DE CONTENIDOS

# 1. INTRODUCCIÓN

## *1.1. Idea del documento*

El presente documento detalla la normativa y requisitos necesarios para acceder al servicio de actualización de contenido de sitios web alojados en los servicios de información centrales de la Universidad administrados por la Dirección de Informática.

## *1.2. Implementación*

El procedimiento está destinado a su implementación por parte de la comunidad universitaria en su totalidad.

## *1.3. Glosario de términos y abreviaturas*

Los acrónimos y términos técnicos utilizados en éste documento son:

| | | |
|---|---|---|
| **Secuencias** | : | Secuencias de comandos que se ejecutan en el navegador del cliente. Por ejemplo, JavaScript o VisualScript. |
| **DI** | : | Dirección de Informática |
| | | |

# 2. DEFINICIÓN DEL SERVICIO

La Dirección de Informática está encargada de la operación y administración de los servicios informáticos centrales de la Universidad. La plataforma tecnológica que permite que esa información sea publicada en los sitios Web de la Universidad es parte de estos servicios.

La Dirección de Informática provee los medios para que las unidades académicas responsables del contenido puedan modificarlo en forma autónoma, de acuerdo a sus necesidades de periodicidad particulares.

## *2.1. Descripción general del funcionamiento*

Existen dos métodos para actualizar el contenido web público. Las unidades cuentan con acceso individualizado para los encargados de esta función, quienes utilizan sus credenciales UC (usuario y clave UC) para acceder.

### *2.1.1. Administrador de Contenidos*

Existe un Administrador de Contenido UC mediante el cual provee la unidad puede modificar el contenido del sitio utilizando un editor web. Esto permite trabajar con texto y algunos códigos HTML.

### *2.1.2. Modificación directa de archivo*

Adicionalmente, se ofrece la posibilidad de modificar directamente los archivos en su estructura y código, para aquellas unidades que requieran una mayor flexibilidad que la entregada por el editor mencionado antes.

## 3. CONDICIONES

Acceder a este servicio implica las siguientes condiciones.

1. La unidad, a través de los encargados designados, es responsable del contenido publicado en el sitio.

2. La unidad es responsable del código HTML, secuencias y hojas de estilo.

3. Las estaciones de trabajo de los usuarios responsables de esta función dentro de la unidad deben satisfacer estrictamente las condiciones de seguridad que resguarden de afectar a la plataforma Web de la UC. Entre las condiciones que deben observarse están las siguientes:

    - Correcto funcionamiento del antivirus, con las actualizaciones al día.

    - Sistema operativo con las actualizaciones al día.

    - No utilizar software de descarga o intercambio de archivos como Ares, Bittorrent o similares.

    - No utilizar sitios de descarga masiva como Megaupload, Rapidshare o similares.

    - Instalar sólo software autorizado.

Como parte de las funciones que tiene la Dirección de Informática de resguardar la seguridad y operatividad de plataforma Web, podrá verificar que las estaciones de trabajo los usuarios autorizados cumplan con las condiciones descritas. Se sugiere aplicar las recomendaciones disponibles en el sitio web de la Dirección de Informática:

http://www.uc.cl/informatica/documentos/protegetucomputador.pdf

# 4. REQUISITOS

Para acceder al servicio de actualización de contenido, la unidad dependiendo del método que utilice deberá cumplir con los siguientes requisitos:

## *4.1. Requisitos comunes*

1. La unidad debe definir un responsable del proceso de actualización de contenido que tenga contrato indefinido, el cual será el interlocutor válido entre la unidad y la Dirección de Informática.

2. Quién o quiénes sean designados como administradores del contenido de cada unidad, deberán firmar la carta de conocimiento y aceptación de esta normativa (ver Anexo A: Carta de aceptación).

## *4.2. Para el Administrador de Contenidos*

1. Administrativos o académicos contratados por la Universidad

2. Haber asistido a la capacitación realizada por la DI para el uso de esta herramienta.

## *4.3. Para modificación directa de archivos*

1. Funcionarios o académicos contratados con plazo indefinido por la Universidad, que cuenten con credenciales UC y competencias adecuadas al uso de la tecnología provista por la DI para este fin.

2. Una estación de trabajo destinada a esta función.

# 5. NORMATIVA

## *5.1. Del contenido*

La unidad es responsable completamente del contenido publicado. Esto implica hacerse cargo de:

- No violar leyes de protección de propiedad intelectual.
- Cumplir con las normativas editoriales y gráficas de la Universidad disponibles en la Facultad de Comunicaciones.
- Cumplir con la normativa técnica para sitios web de la Universidad. Ver http://www.uc.cl/informatica/documentos/normativas.pdf

## *5.2. Del código HTML, secuencias y hojas de estilo*

En relación con la edición de código HTML y publicación de páginas en dicho lenguaje, secuencias de comandos (como .js, .vbs, etc.) y uso de hojas de estilo (como .css) se establecen las siguientes normativas.

### *5.2.1. Condiciones del código*

El código HTML debe cumplir la única función de estructurar el contenido dentro de la página, las hojas de estilo sólo deben ocuparse del aspecto y formatos, y las secuencias de comandos de algunos efectos y funciones básicas. **No** se permiten los siguientes códigos:

- Uso de frames e iframes en el código HTML.
- Incluir script desde servidores externos.
- La inclusión de funciones y código de secuencias se puede realizar siguiendo las siguientes reglas:
  - Todo el contenido de tipo script debe estar incluido en el ámbito HEAD del cuerpo HTML.
  - Es posible incluir código de secuencias (archivo.js), desde archivos alojados en el mismo servidor.

- No se permitirá la inclusión de archivos alojados en distintos sitios. Es decir, las inclusiones deben ser sólo con rutas de archivo relativas. La línea siguiente, por ejemplo, está permitida:
  - *<script src="/directorio/archivo.js">*

  La siguiente línea **no** está permitida:
  - *<script src="http://www.dominio.com/directorio/archivo.js">*

- No se permite la inclusión al interior de los archivos de secuencias, de archivos alojados en servidores externos al sitio.

### *5.2.2. Auditoría*

La Dirección de Informática realizará procesos de auditoría aleatorios en los archivos, para controlar que las condiciones descritas en el punto anterior se cumplan.

Esto implica, por ejemplo, que los de iframes serán eliminados si se encuentran en el código del sitio, al igual que los párrafos de código de secuencias dentro del body.

Lo anterior, sin perjuicio de que la responsabilidad de la calidad de construcción del contenido sigue siendo de la unidad, la cual debe hacer este tipo de revisiones como parte del proceso de actualización.

## *5.3. Del acceso al servicio*

El acceso a los servicios de actualización de contenidos es personal e intransferible. El usuario autorizado debe utilizar sus propias credenciales de acceso. No está permitido entregar las credenciales a terceros para que accedan al servicio.

De ser detectada esta actividad, la cuenta de acceso en cuestión será bloqueada y se informará la situación a la dirección de la unidad.

El servicio cuenta con un registro de cada actualización realizada. Esta información es utilizada para identificar al responsable de la modificación y su estación de trabajo.

## *5.4. Herramientas de apoyo*

Antes de publicar los archivos en el servidor de producción, se deberá verificar en el servidor de desarrollo que estos se encuentren libres de infecciones malware. Se deben verificar a lo menos a través de 3 herramientas en las cuales se debe colocar la ruta de los archivos o del directorio en el cual se realizó la actualización:

- http://safeweb.norton.com
- http://linkscanner.explabs.com/linkscanner/default.aspx
- http://www.google.com/safebrowsing/diagnostic?site=google.com
- http://www.avg.com.au/resources/web-page-scanner/

Adicionalmente a estas herramientas existen otras herramientas gratuitas de revisión

- http://www.malwarehelp.org/freeware-open-source-commercial-website-security-tools-services-downloads.html

Debido a que los recursos de apoyo mejoran periódicamente, se tiene la siguiente página web: http://informatica.uc.cl. En ella se encuentra una lista actualizada, que se sugiere consultar para chequear el contenido que ha sido modificado por los encargados de las páginas web.

## 6. EFECTOS DEL NO CUMPLIMIENTO DE ESTA NORMATIVA

La publicación de contenido en los sitios web de la Universidad conlleva una gran responsabilidad. La normativa presente establece las condiciones necesarias para que este proceso se lleve a cabo sin problemas para la Universidad y la sociedad en su conjunto.

El no cumplimiento de la normativa, facilitaría situaciones como:

- Utilización de medios para difamación.
- Violación de la legislación vigente.
- Violación de la propiedad intelectual.
- Publicación de software malicioso, que puede afectar la seguridad informática de los visitantes.
- Poner en riesgo la seguridad de la plataforma Web de la UC.

De haber registros o pruebas de situaciones como las descritas, se aplicará el siguiente procedimiento:

1. Bloqueo de las cuentas de correo electrónico que actualizaron por última vez el contenido causante del incidente. Este bloqueo puede durar el tiempo que tome resolver la situación.

2. Notificación a la unidad.

3. La unidad debe resolver la situación que originó el problema y modificar el contenido.

4. En el caso de incidentes de seguridad, la unidad debe hacerse cargo de la reparación de la fuente causante del problema, por ejemplo, reinstalación de las estaciones de trabajo utilizadas para actualizar el contenido.

5. La limpieza del contenido web será realizada en conjunto entre la Dirección de Informática y la unidad.

6. Las cuentas de acceso FTP permanecerán bloqueadas hasta que la situación sea resuelta.

# 7. ANEXO A: CARTA DE ACEPTACIÓN

Yo, _____(nombre),

RUT _____ - _, _____ (cargo), perteneciente a

_____(unidad académica), declaro haber leído y estar de acuerdo con la normativa presente, con el fin de acceder al servicio de Administración de Contenido.

_____

Firma del responsable