



**RESUELVE**

**ARTICULO 1.** Expídase Manual de Seguridad y Políticas Informáticas de la Universidad del Atlántico, el cual hace parte integral del presente Acto Administrativo.

**ARTÍCULO 2.** Inclúyase dentro de la documentación del Sistema Integrado de Gestión de Calidad, el Manual de Seguridad y Políticas Informáticas de la Universidad del Atlántico.

**ARTICULO 3. –ALCANCE.** El Manual de Seguridad y Políticas Informáticas de la Universidad del Atlántico se aplicará a todos y cada uno de los estamentos universitarios tanto administrativos como académicos que utilicen las tecnologías que brinde la Universidad para el ejercicio de sus funciones.

**ARTICULO 4.–RESPONSABLE.** El Jefe (a) de la Oficina de Informática o quien haga sus veces será el responsable de velar por la aplicación del Manual de Seguridad y Políticas Informáticas de la Universidad del Atlántico.

**ARTICULO 5. –DIVULGACION.** El Manual de Seguridad y Políticas Informáticas de la Universidad del Atlántico se divulgará a toda la Comunidad Universitaria a través de medios masivos de comunicación.

**ARTICULO 6. –VIGENCIA.** La presente resolución rige a partir de la fecha de su expedición y deroga aquellas que le sean contrarias.

**COMUNIQUESE Y CUMPLASE.**

Dado en Barranquilla, a los

27 JUL 2011

**ANA SOFÍA MESA DE CUERVO**

Rectora

V.B.  
Proyectó: JDeSantis/MVengoechea

**MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA  
DE LA UNIVERSIDAD DEL ATLANTICO**

**MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA**

**OFICINA DE INFORMATICA**

**UNIVERSIDAD DEL ATLANTICO**

**2011**

## TABLA DE CONTENIDO

### Contenido

INTRODUCCION.....	3
1. OBJETIVOS .....	4
2. ALCANCE .....	5
3. DOCUMENTOS DE REFERENCIA.....	5
4. GLOSARIO.....	5
5. POLITICAS Y CONDICIONES DE OPERACIÓN.....	9
5.1 Control de acceso a la información y los sistemas.....	9
5.2 Uso del correo Institucional .....	10
5.3 Uso de las redes e internet.....	12
5.4 Infraestructura de la red .....	13
5.5 Uso de los equipos de cómputo y el procesamiento de la Información .....	14
5.6 Administración de servidores .....	15
<b>6. POLITICA Y REGLAMENTO PARA LA OPERACIÓN DEL SITIO WEB DE LA UNIVERSIDAD DEL ATLANTICO .....</b>	<b>16</b>
<b>7. POLITICA Y REGLAMENTO PARA LA ADMINISTRACIÓN Y OPERACIÓN DE LAS SALAS DE CÓMPUTO .....</b>	<b>19</b>
7.1 Usuarios .....	19
7.2 Servicios.....	19
7.3 Horarios .....	19
7.4 Suspensión del servicio.....	20
7.5 Reserva de las salas .....	20
7.6 Deberes de los usuarios.....	20
7.7 Prohibiciones.....	21
7.8 Sanciones.....	21

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 3 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

## INTRODUCCION

Los requerimientos de seguridad que involucran las tecnologías de la Información, en pocos años han cobrado un gran auge, y más aún con las de carácter globalizador como lo son la de Internet y en particular la relacionada con la Web, llevando a que muchas desarrollen políticas que norman el uso adecuado de estas destrezas tecnológicas y recomendaciones para aprovechar estas ventajas, y evitar su uso indebido, ocasionando problemas en los bienes y servicios de las entidades.

La Oficina de Informática de la Universidad del Atlántico realiza el manual de seguridad y políticas de informática para que sean el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la entidad cumplir con su misión.

De esta manera la seguridad informática en la Universidad del Atlántico pretende cumplir con los estándares de seguridad de los sistemas de información, garantizando la confidencialidad de datos (información y de hardware) en los servicios ofrecidos como en los servicios internos a la comunidad universitaria, de acuerdo a lo estipulado en la norma ISO 27001.

El manual de seguridad y políticas de informática de la Universidad del Atlántico, se encuentra disponible para toda la comunidad universitaria.

 <b>Universidad del Atlántico</b>	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 4 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

## 1. OBJETIVOS

### Objetivo General

Propender que los servicios tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso para asegurar su correcta funcionalidad y brindando un nivel de seguridad óptimo.

### Objetivos Específicos

- a) Controlar el ancho de banda los canales de comunicación y la disponibilidad de espacio en disco en el servidor de archivos.
- b) Disminuir las amenazas a la seguridad de la información y los datos.
- c) Evitar el comportamiento inescrupuloso y uso indiscriminado de los recursos.
- d) Cuidar y proteger los recursos tecnológicos de la Universidad.
- e) Concientizar a la comunidad sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.

 <b>Universidad del Atlántico</b>	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 5 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

## 2. ALCANCE

La presente política de seguridad informática y uso de los sistemas tecnológicos y comunicaciones de la Universidad del Atlántico, aplica para los estudiantes, contratistas, cuerpo académico, funcionarios de la Universidad, personal de apoyo y terceros no vinculados directamente a la universidad pero que presten su servicio y utilicen tecnología de información, en lo que sigue, la palabra “usuario” y/o “usuarios” se referirá a cualquiera de estas personas. La política aplica a los equipos propios de la Universidad o arrendados y a los equipos de personas externas que sean conectados a la red de la Universidad del Atlántico.

## 3. DOCUMENTOS DE REFERENCIA

- Seguridad en la información ISO/IEC 27001
- Estatuto de propiedad intelectual de la Universidad del Atlántico
- Ley 527 de 1999 - Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
- Ley 1273 de 2009 - “De la Protección de la información y de los datos”

## 4. GLOSARIO

**Hardware.** El hardware está formado por los componentes físicos. Es la parte "dura", es decir, las partes que configuran la máquina y que le dan una serie de características.

**Software.** El software está compuesto por los programas que dirigen el funcionamiento de un ordenador. Es la "parte lógica" de la máquina que permite enlazar todos los elementos de hardware de la manera más efectiva posible, permitiéndole realizar cualquier tipo de trabajo.

**Comunicación:** Es cuando se transmite información desde un equipo a cualquier otro. Para que se pueda realizar una transmisión de información, son necesarios tres elementos: El emisor, quien origina la información; el medio de transmisión:

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 6 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

que permite la transmisión de esa información; el receptor: quien recibe la información.

**Servicio:** Son programas que están disponibles en los servidores y que son utilizados por los usuarios de la red bajo una solicitud.

**Correo electrónico** También conocido como “E-mail”. Es un software que puede utilizarse para el envío y recepción de mensajería entre usuarios, entendiendo por mensajería cualquier texto, archivo, programa, etc.

**Virus:** Son pequeños programas de computadora cuya principal cualidad es la de poder auto replicarse, está escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este para producir efectos dañinos.

**LAN (Local Area Network):** Se refiere a redes de computadoras que no traspasan de un ámbito delimitado por un área física determinada, como por ejemplo un edificio, una compañía, etc.

**Red de computadoras:** A nivel más elemental una red no es más que un conjunto de máquinas (computadoras, impresoras y otros recursos), un medio compartido (tal como un cable con el que se interconectan todas las computadoras y las impresoras), junto con una serie de reglas (protocolo) que rigen el acceso a dicho medio.

**WAN (Redes de Área Extensa).** Al ampliarse el alcance de las LAN, traspasando las fronteras que delimitan su espacio físico, se convierten en una red de área extensa (WAN). Generalmente se denomina WAN a un conjunto de redes LAN situadas en espacios físicos distantes, que se interconectan entre sí mediante medios de transmisión de datos (enlaces de radio, fibra óptica, microondas, cable, MODEM, etc.).

**Usuarios:** Se refiere a todos los empleados, estudiantes, contratistas, consultores, trabajadores temporales, y cualquier otra persona o entidad que por razón de su trabajo se le permita acceso, se le asignen derechos de uso y utilicen los recursos

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 7 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

que componen los medios electrónicos de almacenamiento y transmisión de datos de la universidad del Atlántico.

Igualmente se clasifica como usuario a cualquier empleado, contratista, consultor, o trabajador temporal de compañías asociadas a la universidad del Atlántico, a quienes se les preste cualquier tipo de servicio que implique la utilización de los medios electrónicos de transmisión de datos de la universidad del Atlántico.

**Red Internet:** Conjunto de computadoras y entidades alrededor del mundo, interconectadas entre sí, con el propósito de intercambiar correo e información de carácter general.

**Backup:** Son copias de respaldo o de seguridad del sistema o de los datos, que puede ser utilizada en caso de producirse un fallo generalizado, caída del sistema, o el daño o eliminación accidental de archivos. Gracias a la información contenida en el backup, se podrá restaurar el sistema al estado en que se encontraba en el momento de realizar la copia de seguridad.

**Comprimir:** Proceso que compacta archivos para guardarlos en una unidad de almacenamiento limitada. Al comprimir un archivo con un programa de compresión de archivos como PowerArchiver, Winzip o Winace, se crea un archivo que contiene toda la información del original, pero en un tamaño más reducido.

**Descomprimir:** Proceso inverso a la compresión, en la que en un archivo comprimido se restablece toda la información de la misma forma y tamaño original.

**Acceso lógico:** Provee medios técnicos para controlar la información que los usuarios pueden utilizar, los programas que pueden ejecutar y las modificaciones que pueden hacer. Los controles pueden estar en el sistema operativo, aplicaciones, bases de datos, dispositivos de red y utilerías.

**Acceso físico:** Restringen la entrada y salida de personal, equipos y medios de áreas como edificios, centros de datos o cuartos de servidores.

**Comunidad Universitaria:** La comunidad universitaria está integrada por estudiantes matriculados en cualquiera de las enseñanzas que se impartan en las

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 8 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

universidades del sistema universitario, el personal investigador, el personal docente, el de administración y servicios, contratistas, proveedores y terceros que tengan relación directa o indirecta con la universidad, en conclusión todos los grupos de interés.

**Switch:** es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos, Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro.

**Routers:** Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.

**Antena:** Permiten conexiones desde otros dispositivos sin cable como pueden ser las NICs (network interface cards - tarjetas de red), repetidores wireless, puntos de acceso inalámbrico (WAP o AP), y puentes wireless.

**Puntos:** Los puntos de acceso son dispositivos de red “wireless” que funcionan de forma equivalente a los “hubs” o concentradores, permitiendo que varios clientes “wireless” se comuniquen entre sí. A menudo se utilizan varios puntos de acceso para cubrir un área determinada como una casa, una oficina u otro tipo de localización delimitada.

**Redes sociales:** Las Redes son formas de interacción social, definida como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos.

 <b>Universidad del Atlántico</b>	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 9 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

## 5. POLITICAS Y CONDICIONES DE OPERACIÓN

### 5.1 Control de acceso a la información y los sistemas

#### 5.1.1 Generalidades

El acceso a los recursos de información que provee la Universidad del Atlántico, tales como internet, sistemas de información y redes avanzadas es suministrado a los usuarios de la universidad del Atlántico como herramientas de soporte para obtener la información necesaria para realizar de manera óptima sus actividades mediante el uso de herramientas tecnológicas de punta, para lo cual debe cumplirse con los siguientes aspectos:

- a) Todo tipo de información que provenga, sea transmitida o recibida por un sistema computacional de comunicación es considerada parte de los registros oficiales de la universidad del Atlántico y, por ende, está sujeta a cumplir las normas y restricciones consignadas en este documento. Como consecuencia de esto, el usuario, deberá siempre asegurarse que la información contenida en los mensajes de e-mail y en otras transmisiones es precisa, apropiada, ética y constructiva.
- b) Los equipos, servicios, y tecnologías proporcionadas a los usuarios para hacer uso del Internet son en todo momento propiedad de la universidad del Atlántico. Por este motivo, la universidad del Atlántico se reserva el derecho a monitorear el tráfico de Internet, y retirar, leer o verificar cualquier documento enviado o recibido a través de conexiones en línea y que sea guardado en los computadores de la Universidad.

#### 5.1.2 Prohibiciones

Está prohibido a los usuarios de los sistemas de información de la Universidad, realizar las siguientes acciones:

- a) El acceso físico y/o manipulación de los servidores, switches, routers, antenas, puntos y elementos activos de red y las bases de datos que almacenan información privilegiada y transacciones propias de la universidad. Estas

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 10 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

acciones serán realizadas única y exclusivamente por el personal de la Oficina de Informática AUTORIZADO para realizar estas labores.

- b) El ingreso físico al centro de cómputo principal y demás centros de comunicaciones. Excepto para el personal de la Oficina de Informática autorizado para tal fin.
- c) Redactar, Transmitir, acceder o recibir vía Internet, haciendo uso de las redes o equipos de cómputo de la Universidad información con contenido que pudiera ser discriminatorio, ofensivo, obsceno, amenazante, intimidante o destructivo para cualquier individuo u organización. Ejemplos de contenido inaceptable incluyen, entre otros, comentarios en general o imágenes con contenido sexual, discriminación racial, otro tipo de comentarios o imágenes que pudieran ofender a algún individuo con base en su raza, edad, orientación sexual, creencias religiosas, orientación política, nacionalidad, limitaciones físicas o cualquier otra característica especial protegida por la ley.
- d) El acceso físico o lógico a los servidores, switches, routers, antenas, puntos y elementos activos de red y las bases de datos que almacenan información privilegiada y transacciones propias de la universidad mediante el uso de herramientas lógicas tales como programas de computación que pudieran ocasionar daños permanentes en la información allí almacenada.

## 5.2 Uso del correo Institucional

### 5.2.1 Generalidades

Para acceder a la cuenta de correo institucional que establezca la Universidad del Atlántico los usuarios deberán hacerlo a través de su plena identificación y utilizando la contraseña correspondiente. Las cuentas de los usuarios cumplirán con los siguientes aspectos:

- a) Los usuarios deben utilizar la dirección de correo asignada por la universidad única y exclusivamente para enviar/recibir mensajes de correo electrónico relacionados con asuntos laborales.
- b) Revisar el correo electrónico es de carácter obligatorio ya que estos han reemplazado para muchos efectos la papelera de entrada.
- c) Las cuentas de correo son personales e intransferibles. El propietario de la cuenta es el UNICO responsable de la privacidad de la clave de acceso a su

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 11 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

cuenta, cualquier acción efectuada desde ésta cuenta será atribuida a dicho propietario.

- d) Los correos masivos institucionales que por necesidades específicas de un área requieran ser enviados a toda la comunidad universitaria deben ser solicitados a la Oficina de Informática y autorizados por la misma.
- e) La apertura de archivos adjuntos debe hacerse siempre y cuando se conozca con claridad el remitente y el asunto. Es responsabilidad del usuario el cuidado de ejecutar archivos de fuentes desconocidas, o ciertos archivos como fotos o imágenes reenviadas vía email.
- f) Los usuarios de los correos electrónicos institucionales que adjunten documentos que no son propios deberán citar siempre la fuente de origen con la finalidad de respetar los derechos de propiedad intelectual.
- g) La Universidad del Atlántico a través de la Oficina de Informática se reserva el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para su seguridad.
- h) La creación de los correos electrónicos institucionales es responsabilidad de la Oficina de Informática quien define los nombres, estructura y plataforma que se utilizará.

### 5.2.2. Prohibiciones

Está prohibido a los usuarios del correo institucional de la Universidad, realizar las siguientes acciones:

- a) El uso de cuentas ajenas, así como la cesión de la cuenta propia a terceros.
- b) Iniciar o reenviar mensajes encadenados o el envío de correo masivo.
- c) Uso de seudónimos y envío de mensajes anónimos.
- d) Envío de mensajes que atenten contra la dignidad humana y las garantías fundamentales.
- e) Usar el correo corporativo para fines personales, comerciales, publicitarios, religiosos o políticos.
- f) Generar o enviar correos electrónicos a nombre de otra persona o suplantándola.
- g) Enviar archivos adjuntos de tamaño mayor a 5 MB y/o archivos ejecutables.

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 12 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

## 5.3 Uso de las redes e internet

### 5.3.1 Generalidades

La Internet es el método más común de contagio y de riesgo informático que una compañía puede enfrentar. Es por esto que deben seguirse las siguientes acciones para proteger la integridad de la información y los sistemas y proteger el ancho de banda con que cuenta la Universidad del Atlántico:

- a) El internet de la Universidad del Atlántico, únicamente puede ser usado con fines institucionales.
- b) El Internet institucional debe emplearse como una herramienta para investigación, desarrollo, consulta y comunicación de actividades relacionadas con los procesos de la Universidad del Atlántico.
- c) El Internet de la Universidad del Atlántico puede llegar a tener fines didácticos permitiéndole a los usuarios tomar cursos de capacitación por Internet en temas que enriquezcan su labor dentro de la organización.
- d) El Internet es el medio de difusión de la página Web de la universidad y por lo tanto toda la comunidad universitaria tendrá acceso a ella.
- e) Se restringe el uso e instalación sin previa autorización de la Oficina de Informática, de programas de Chats tales como: MSN Messenger, YAHOO Messenger o Similares, excepto los autorizados para chat interno. En adelante, para que este servicio sea instalado en algún equipo, los jefes de área/facultad deberán pasar la solicitud a la Oficina de Informática explicando los motivos por lo que necesitan este tipo de sistemas en sus áreas.
- f) Se restringe el acceso a las redes sociales Facebook, Myspace, HI5 o similares en los horarios de 6:00 A.M. a 12:00 P.M. y de 2:00 P.M. a 9:00 P.M.

### 5.3.2 Prohibiciones

Está prohibido a los usuarios de la red e internet de la Universidad, realizar las siguientes acciones:

- a) Ingresar a páginas de dudoso contenido o autoría
- b) El acceso a sitios pornográficos, sitios religiosos dedicados a difundir las creencias de alguna religión o secta en particular, acceso a sitios web de alzados en armas o de grupos terroristas a nivel nacional o internacional dedicados a difundir temas relacionados con violencia.

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 13 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

- c) Utilizar el canal de conexión a Internet para descargar e instalar música, videos y archivos ejecutables mediante programas tales como KAZAA.com, Ares, Lime Ware y similares.
- d) Bajar programas (software), sin la debida autorización de la Oficina de Informática, tales como: Shareware, Freeware, software de evaluación, etc. Archivos de música (MP3, WAV, etc.) ya que estos no poseen licencia para su uso en la Universidad.
- e) Usar el Internet para realizar llamadas internacionales (Dialpad, NET2PHONE, FREEPHONE, etc.).

## 5.4 Infraestructura de la red

### 5.4.1 Generalidades

La Universidad del Atlántico cuenta con la infraestructura de red que comprende todo el cableado, switches, routers, antenas y sistemas inalámbricos que permiten realizar la conexión.

La Oficina de Informática definirá el manejo de la infraestructura de la red dependiendo de las necesidades del servicio, con el fin de mantenerla y utilizar de la mejor forma los recursos existentes.

- a) Pruebas de Chequeo de Vulnerabilidades: La Oficina de Informática realizara estudios periódicos a la red para evaluar la vulnerabilidad de la misma.
- b) Para efectos de realizar mantenimiento de la red y seguridad, la Oficina de Informática, podrá monitorear equipos, sistemas y tráfico de red en cualquier momento.

### 5.4.2 Prohibiciones

Está prohibido a los usuarios de la red e infraestructura tecnológica de la Universidad, realizar las siguientes acciones:

- a) Utilizar la infraestructura de tecnología de información y redes de la universidad para conseguir o transmitir material con ánimo de lucro excepto cuando se trate de cumplir con fines institucionales; igualmente está

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 14 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

prohibido su utilización para hacer algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil en contra de miembros de la comunidad universitaria y en general de cualquier persona o institución.

- b) Ejecutar cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada.
- c) Burlar los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
- d) Desconectar o manipular los elementos de red tales como swiches, routers, antenas, racks y demás elementos pertenecientes a la infraestructura de red de la Universidad.
- e) Modificar la configuración de red establecida en los equipos de cómputo de cualquier dependencia o sala.

## 5.5 Uso de los equipos de cómputo y el procesamiento de la Información

### 5.5.1 Generalidades

La información almacenada y el manejo de las estaciones de trabajo o los equipos portátiles de la Universidad del Atlántico deberán cumplir con las siguientes pautas:

- a) Los equipos asignados a cada uno de los usuarios de la Universidad del Atlántico se consideran propiedad de la institución y por lo tanto, esta última es la encargada de decidir las aplicaciones que se han de manejar en cada equipo, la instalación o desinstalación de aplicaciones de software por parte de usuarios queda restringida mediante esta política.
- b) El uso de los recursos informáticos debe limitarse única y exclusivamente a fines institucionales.
- c) Todas y cada una de las máquinas de la Universidad del Atlántico se encuentran trabajando en red y deben ser validadas por un dominio.
- d) Cada usuario es el único responsable de la administración y el buen uso de su nombre de usuario y contraseña de red y por lo tanto, será responsable de las acciones realizadas por terceros quienes conozcan su clave de ingreso a las redes corporativas.

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 15 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

- e) La Vicerrectoría Administrativa y Financiera por medio del departamento de gestión del Talento Humano, deberá mantener informada a la Oficina de Informática de la rotación de los funcionarios/contratistas con el fin de mantener actualizada la base de datos como la eliminación de cuentas de correos, claves de acceso entre otros de personas que ya no tengan vínculos con la institución y evitar accesos no autorizados.
- f) Los antivirus serán instalados, actualizados y habilitados continuamente.
- g) Utilizar software licenciado o libre en las estaciones de trabajo de la Universidad del Atlántico debidamente autorizado por la Oficina de Informática de la Universidad del Atlántico.

### 5.5.2 Prohibiciones

Con respecto al almacenamiento de información:

- a) Almacenar información de índole personal como videos, fotos, música entre otros.
- b) El uso de equipos, redes, espacio en servidor, impresoras, entre otros para almacenar o realizar labores de índole personal.
- c) Alterar o copiar un archivo perteneciente a otro Usuario sin el previo consentimiento del dueño del archivo.

### 5.6 Administración de servidores

#### 5.6.1 Generalidades

La administración de los servidores de la Universidad del Atlántico debe cumplir con los siguientes criterios:

- a) Los servidores deben tener un esquema de copias de respaldo y recuperación para casos de desastre.
- b) Los servidores deben tener un esquema para mantener registros digitales de acceso y operación.
- c) Los administradores de servidores son responsables de cumplir todas las políticas, la Oficina de Informática debe realizar revisiones periódicas a los mismos con la finalidad de mejorar la seguridad o detectar fallas.

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 16 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

## 5.6.2 Prohibiciones

Está prohibido a los usuarios de la tecnología de procesamiento de información y redes de la Universidad del Atlántico lo siguiente:

- a) Violación de los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier forma de propiedad intelectual.
- b) Realizar copia no autorizada de material protegido por derecho de autor que incluye, pero no está limitado a, digitalización y distribución de imágenes y fotografías de cualquier origen, música, audio, video, distribución o instalación de software sin licencia ni autorización de la universidad.
- c) Exportar software o información técnica sin la autorización expresa de la Universidad.
- d) Introducir software malicioso en la red o en los servidores (virus, Worms, correo no deseado, spam, etc).
- e) Revelar la clave o contraseña de sus cuentas de los sistemas de información de la Universidad a otros, o permitir su uso a terceros para actividades ajenas a la misión institucional.
- f) Proporcionar información confidencial a personas o entidades sin la debida autorización o violando las políticas sobre manejo de la información confidencial.

## 6. POLITICA Y REGLAMENTO PARA LA OPERACIÓN DEL SITIO WEB DE LA UNIVERSIDAD DEL ATLANTICO

### 6.1 Generalidades

La Universidad del Atlántico entiende el sitio web como un medio de comunicación en todo lo relativo a contenidos e imagen gráfica, entendidos estos como: el carácter institucional de la Universidad y la comunicación externa e interna, reconoce y asume el valor de este espacio virtual como herramienta de promoción, comunicación y apoyo permanente a los procesos de enseñanza, aprendizaje, investigación, proyección social, administración y gestión.

Es por esto que se establece la presente política institucional así:

- a) La Oficina de Informática como proceso de Gestión tecnológica y comunicaciones, tiene la responsabilidad de la operación de los servidores que albergan las páginas web, para lo cual; administra el servidor, se ocupa de la parte de programación y desarrollo utilizando tecnología de vanguardia en todo lo relacionado con Web y establece los estándares y lineamientos de diseño, publicación, comunicación y procedimientos de revisión para todas las páginas web institucionales, por lo tanto es la dependencia encargada de desarrollar, diseñar y mantener el portal de la Universidad.
- b) Todos los contenidos que aparecen en los diferentes sitios, portales o páginas electrónicas de cada una de las instancias universitarias con presencia en la página Web, son responsabilidad del área que los emite.
- c) El nombre de dominio "www.uniatlantico.edu.co" y todos aquellos que sirvan para acceder de forma directa al sitio oficial de la Universidad del Atlántico son de titularidad exclusiva de la Universidad del Atlántico. La indebida utilización de los mismos supondría una infracción de los derechos conferidos por su registro y será perseguido por los medios previstos en la Ley.
- d) Las páginas web que se publiquen en los servidores de la Universidad del Atlántico deben respetar los lineamientos institucionales y las indicaciones gráficas definidas en la guía gráfica de la web establecida por la Oficina de Informática y en el manual de imagen corporativa de la Universidad.
- e) Los contenidos, textos, fotografías, diseños, logotipos, imágenes, sonidos, vídeos, animaciones, grabaciones, programas de computador, códigos fuente y, en general, cualquier creación intelectual existente en el sitio oficial, así como el propio sitio en su conjunto como obra artística multimedia están protegidos como derechos de autor por la legislación en materia de propiedad intelectual.
- f) Quedan exceptuados de esta protección aquellos archivos o programas de computador que no sean de titularidad de la Universidad del Atlántico y de acceso gratuito o aplicaciones que tienen el carácter de dominio público por voluntad de sus autores.
- g) Cualquier link o vínculo a páginas externas a la Universidad del Atlántico, deberá ser autorizado por la Oficina de Informática.
- h) Toda información incluida en páginas web de servidores de la Universidad debe cumplir con todas las leyes de derechos de copia y propiedad intelectual, no ir contra política o reglamento de la Universidad y no ser usada para actividades comerciales o de lucro excepto cuando se trate de cumplir con fines institucionales.
- i) Para la publicación imágenes, videos y audios en las páginas sociales a las que pertenece la Universidad oficialmente, es indispensable contar con la autorización de la Oficina de Informática.
- j) Toda solicitud para realizar cambios o publicaciones en la página web debe estar sustentada por un comunicado escrito, correo electrónico o enviado a

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 18 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

través de la herramienta help desk CAU( Centro de Atención a Usuarios), dirigido a la Oficina de Informática

- k) Cada área de la Universidad del Atlántico con presencia en la página web es responsable de la información que publica, y designará a una persona como responsable operativo y contacto con la Oficina de Informática. Esta persona estará encargada de la edición, revisión de estilo y pertinencia de cada artículo. La actualización de la información publicada por cada unidad académica o administrativa es responsabilidad de la misma.
- l) Los docentes, investigadores y administrativos de la Universidad pueden crear páginas web para su uso en proyectos y deberes académicos o administrativos propios de la Universidad y pueden instalarlas en servidores web de la Universidad. El contenido de las páginas web publicadas por los mismos en servidores de la Universidad del Atlántico debe cumplir con las reglas generales de contenidos indicados en estas políticas y los contenidos serán de responsabilidad del área a la que pertenecen.

## 6.2 Prohibiciones

Los contenidos publicados en el sitio web de la Universidad del Atlántico, deberán reflejar la actividad que cada área desarrolla, siempre apegados a la Misión, Visión, filosofía educativa y principios de la propia Universidad del Atlántico. Para garantizar esto se establecen las siguientes prohibiciones:

- a) La Universidad no autoriza publicación en otros dominios diferentes a los de los Servidores oficiales de la Universidad del Atlántico.
- b) Hacer proselitismo de ideas políticas, gremiales o religiosas.
- c) Publicar contenidos que promuevan intolerancia, violencia, racismo o vicios.
- d) Publicación de links o vínculos a páginas externas a la Universidad del Atlántico que vayan en contra de los principios y valores de la propia Universidad del Atlántico.
- e) Comercialización de espacios dentro de la página Web de la Universidad del Atlántico.

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 19 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

## 7. POLITICA Y REGLAMENTO PARA LA ADMINISTRACIÓN Y OPERACIÓN DE LAS SALAS DE CÓMPUTO

El presente capítulo tiene como objetivo, establecer las normas de funcionamiento de las salas de cómputo de la Universidad del Atlántico, cuyas disposiciones son de obligatorio cumplimiento para todos los usuarios.

### 7.1 Usuarios

Podrán hacer uso de las Salas de cómputo, los siguientes usuarios teniendo alta prioridad las actividades de tipo académico:

- a) Estudiantes con matrícula académica y/o financiera vigente.
- b) Egresados de los programas de la Universidad.
- c) Docentes.
- d) Personal administrativo que requiera uso de las salas de cómputo.

La administración de los recursos y funcionamiento de las salas de cómputo es responsabilidad de la Oficina de Informática a través del personal designado como administradores, supervisores y monitores de sala.

### 7.2 Servicios

Los servicios de cómputo ofrecidos por las salas de la Universidad son los siguientes:

- a) Uso de los computadores con programas (software) necesarios para el desarrollo de clases, trabajos académicos y de investigación.
- b) Acceso a Internet
- c) Asesoría en el uso de equipos y programas.

### 7.3 Horarios

El horario normal de uso de las salas de computo, es desde las 6:30 a.m. a las 9:30 p.m. de lunes a viernes de forma continua, y los sábados desde las 6:30 a.m. a las 6:00 p.m. durante el semestre en curso. En periodo de vacaciones se reservaran las salas para mantenimiento de programas y equipos.

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 20 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

La programación de horarios de clases en las salas será asignada por la Vicerrectoría de Docencia.

#### 7.4 Suspensión del servicio

El servicio será suspendido en caso de mantenimiento urgente, siniestro, o cuando las condiciones lo ameriten a consideración de la Oficina de Informática.

#### 7.5 Reserva de las salas

Las reservas para el uso de las salas de computo de la Universidad, se realizará según programación de horarios realizado al inicio del semestre académico.

Para las reservas extraordinarias durante el semestre, se deberá efectuar la solicitud por escrito con ocho días hábiles de anticipación, a la Vicerrectoría de docencia quien asigna los horarios de clases y la Oficina de Informática especificando la fecha y hora, las aplicaciones (software) requeridas y el uso para el que requiere la sala. Esta reserva, estará sujeta a la disponibilidad de las salas.

#### 7.6 Deberes de los usuarios

Son deberes de los usuarios de las salas de cómputo de la Universidad los siguientes:

- a) Cumplir y respetar lo establecido en el presente manual.
- b) Respetar el horario de servicio.
- c) Contribuir a mantener el buen estado de las instalaciones y los equipos.
- d) Observar una conducta adecuada para la convivencia universitaria, incluyendo el respeto al personal de las Salas de cómputo.
- e) Exclusivamente se utilizarán las salas de cómputo para actividades de tipo académico.
- f) Los archivos del usuario deberán ser guardados de manera temporal en la carpeta Mis Documentos de cada equipo. Es deber del usuario sacar copias de sus archivos cuando finalice la utilización del equipo.
- g) La Sala de cómputo deberá ser entregada en perfecto orden al finalizar la clase por parte del profesor o monitor designado.
- h) Durante el desarrollo de las clases, no se permitirá el ingreso de personas ajenas a ella.
- i) La utilización de los equipos y redes estará sujeto a la política de seguridad informática de la Universidad.

	<b>VERSIÓN:</b> 0
	<b>CÓDIGO:</b> MAN-GT-001
	<b>PÁGINA:</b> 21 DE 21
<b>MANUAL DE SEGURIDAD Y POLITICAS DE INFORMATICA</b>	

- j) Todo incumplimiento a las obligaciones de los usuarios acarreará sanciones de acuerdo con lo establecido en el Reglamento Estudiantil y Reglamento docente.

## 7.7 Prohibiciones

Está prohibido a los usuarios de salas de informática de la Universidad del Atlántico lo siguiente:

- a) Instalar software sin la aprobación de la Oficina de Informática, que estará sujeta a la legalidad del mismo.
- b) Cambiar la configuración del equipo de cómputo.
- c) Instalar juegos o utilizarlos.
- d) Instalar o intercambiar los elementos de los computadores.
- e) Ingresar a páginas con contenido sexual o erótico.
- f) Consumir alimentos y bebidas.
- g) Fumar.

## 7.8 Sanciones

El incumplimiento a cualquiera de las políticas establecidas en el presente documento acarreará las sanciones de tipo disciplinario y legarles a que hubiera lugar.