TABLA DE CONTROL

| VER | FECHA | ELABORÓ | REVISO Y APROBÓ | DESCRIPCIÓN |
|---|---|---|---|---|
| 0 | Mayo 2011 | Mauricio Vengoechea | | VERSIÓN ORIGINAL |
| 1 | Sept 2017 | Cesar Vásquez | | Actualización |

## 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

6. **POLITICA Y REGLAMENTO PARA LA OPERACIÓN DEL SITIO WEB DE LA UNIVERSIDAD DEL ATLANTICO** ..... 17
7. **POLITICA Y REGLAMENTO PARA LA ADMINISTRACIÓN Y OPERACIÓN DE LAS SALAS DE CÓMPUTO** ..... 20

7.1 Usuarios ..... 20

7.2 Servicios ..... 20

7.3 Horarios ..... 20

7.4 Suspensión del servicio ..... 21

7.5 Reserva de las salas ..... 21

7.6 Deberes de los usuarios ..... 21

7.7 Prohibiciones ..... 22

7.8 Sanciones ..... 22

## 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.

## 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.

## 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:

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 Área 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 ha 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 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 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.

# 5. POLITICAS Y CONDICIONES DE OPERACIÓN

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

### 5.1.1 Generalidades

a) Todo funcionario, docente, contratista, estudiante o usuario con acceso a la información, aplicaciones o sistemas de la Universidad del Atlántico, tiene la obligación de adoptar todas las medidas de control establecidas, así como los ordenamientos legales aplicables para la protección de la información o sistemas a los que tenga acceso, preservando su naturaleza confidencial y evitando su transferencia, modificación, destrucción o divulgación a entidades no autorizadas.

b) La infraestructura tecnológica y la información de la Universidad del Atlántico (sistemas, aplicaciones, programas, y en general todos los recursos de cómputo e información que reside o se transmite a través de ellos, PC, escritorios, portátiles, teléfonos celulares y cualquier dispositivo tecnológico en general) son propiedad de la Universidad del Atlántico, por tanto ningún funcionario, docente, contratista, estudiante o usuario puede copiar, duplicar, transmitir o divulgar dicha información, el conocimiento de la misma debe ser únicamente para fines del cumplimiento de sus funciones o deberes.

c) El usuario de dominio y la contraseña asignada para el acceso a los sistemas, aplicaciones y en general a la infraestructura tecnológica e información, son personales, intransferibles y confidenciales; por tanto el titular de la misma es responsable por el uso que se haga de ella, así como de la información y provecho que a través de ella obtenga, para sí o para terceros y de los daños y perjuicios que se ocasionen sin menoscabo de las responsabilidades y sanciones de naturaleza civil y penal que resulten.

d) El acceso a la infraestructura tecnológica de la Universidad del Atlántico que se haga mediante el usuario distinto al asignado para el desempeño de sus funciones, se considera como un uso no autorizado de información confidencial.

e) Se considera una falta grave, la introducción, tráfico o envío de información, el desarrollo, almacenamiento, uso (ejecución) de programas, aplicaciones u

otros mecanismos que puedan dañar, alterar o impactar en el desempeño de los componentes de software de una computadora o sistema de cómputo o comunicaciones propiedad de la Universidad del Atlántico, con el fin de molestar a otros usuarios, infiltrarse en un sistema, y en general, intentar violar los estándares de seguridad definidos para la Universidad del Atlántico por parte de la Oficina de Informática.

f) La infraestructura tecnológica debe ser utilizada únicamente para los fines propios de la entidad. En virtud de ello, no debe ser usada para provecho personal, tales como entretenimiento, grupos de conversación, juegos recreativos, entre otros.

g) En ningún caso, los usuarios de dominio pueden ser reasignados o puestos a nombre de otras personas. Los usuarios de la Universidad del Atlántico no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Universidad del Atlántico, sin la previa autorización por escrito de la Oficina de Informática.

h) El funcionario debe obligarse a impedir fugas de información confidencial o secreta o evitar la sustracción o utilización indebida de la documentación e información clasificada o confidencial a la cual tiene acceso y que le corresponde custodiar por razón de su cargo o función.

i) Los funcionarios de la Universidad del Atlántico, se obligan con toda información clasificada como confidencial a: administrarla, guardarla, custodiarla y conservarla bajo la más estricta reserva.

j) No se permite utilizar programas, herramientas o mecanismos de mensajería instantánea (chats internos o públicos) para el envío y recepción de información confidencial.

k) No se permite utilizar programas, herramientas o mecanismos que pudieran analizar información confidencial en los dispositivos, sin previa autorización de la Oficina de Informática.

l) Al imprimir información confidencial de cualquiera de la Universidad del Atlántico, el usuario debe proteger la información contra robo y acceso no autorizado.

m) El usuario final debe recoger sus listados confidenciales en el menor tiempo posible, no dejándolos olvidados en impresoras, salas de reuniones, entre otros y no utilizándola como papel reciclable.
n) Está prohibida la definición y asignación de usuarios genéricos para uso compartido (usuarios que no están a cargo de un funcionario, docente, o contratista).
o) La transmisión de archivos vía FTP es restringida en la Universidad del Atlántico. En caso de excepciones se debe hacer el análisis correspondiente y avalarlo por la Oficina de Informática.
p) Todos los funcionarios, docentes y contratistas están obligados a bloquear su terminal de trabajo cuando se ausenten de su puesto.
q) La ejecución de operaciones no autorizadas al cargo específico que desempeña se considera falta grave y es sancionada disciplinariamente.
r) Está prohibido compartir carpetas de los discos duros de los equipos propios o unidad "C", entre usuarios.
s) El servicio de acceso a internet se autoriza a funcionarios, docentes, contratistas y terceros que requieran dicho acceso para el cabal ejercicio de sus funciones.
t) Cualquier intento de acceso exitoso o no exitoso a páginas fuera de las autorizadas se considera una falta grave y se aplica las sanciones establecidas en el régimen disciplinario correspondiente.
u) La Oficina de Informática en la Universidad del Atlántico establece los estándares y procedimientos necesarios para control de reportes de acceso y actividad en internet.
v) La autorización para inspección y monitoreo del uso de internet se presume desde el momento de asignación de acceso.
w) Los usuarios y contraseñas asignados por la Oficina de Informática para el acceso a los sistemas de la Universidad del Atlántico, son de carácter personal y bajo ninguna circunstancia deben ser notificados (correo electrónico, WhatsApp, o cualquier medio de comunicación usado por la universidad) a informática o cualquier otra dependencia que presuma su requerimiento; si duda de la veracidad o procedencia del requerimiento comuníquese con la Oficina de Informática.

**Correo electrónico Institucional**

a) La dirección del buzón de mensajería de la Universidad del Atlántico, es creado únicamente por el administrador del sistema contratado por la Oficina de Informática.
b) La revisión del correo institucional asignado por la Universidad del Atlántico es de carácter obligatorio.
c) Está estrictamente prohibido realizar afirmaciones que produzcan pánico general, cualquiera sea su intención (económico, social, político o natural).
d) Es prohibida la utilización de este medio para el envío de mensajes de tipo religioso, político, humorístico, de azar o cualquier otro que no aporte a la eficiencia, productividad y eficacia en el cumplimiento de las funciones y responsabilidades de cada cargo.
e) Está prohibido el uso indebido de la extensión o el nombre de dominio en la dirección electrónica.
f) El servicio de correo electrónico corporativo es un instrumento o herramienta de trabajo, cuya propiedad corresponde a la Universidad del Atlántico y cuyo uso se vincula a la existencia de la relación laboral.
g) Se restringirá el ingreso de archivos anexos en los correos electrónicos que tengan extensiones consideradas como peligrosas.
h) El correo institucional es de uso privativo y solo con fines laborales.
i) Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la Universidad del Atlántico. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
j) Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó la Oficina de Informática.
k) 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.
l) 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.

**Manejo de contraseña del correo electrónico institucional**

a) La contraseña debe ser mínimo de ocho (8) caracteres alfanuméricos.
b) La contraseña debe ser personal e intransferible.
c) En el caso de un correo genérico asignado por la Universidad del Atlántico, el líder del proyecto o coordinador se hace responsable por la información saliente de dicha cuenta de correo.
d) La recuperación de contraseñas del correo electrónico se debe realizar como primera instancia siguiendo los pasos del manual de Recuperación de Contraseñas publicado y socializado por la oficina de Informática, el cual podrá encontrar en la página web de la Universidad del Atlántico; en caso de no tener éxito seguir las indicaciones de los numerales e. y f. según sea su caso.
e) La recuperación de la contraseña del correo electrónico institucional para el personal docente y administrativo se realiza en la oficina de Informática de carácter personal.
f) La recuperación de la contraseña del correo electrónico institucional de los estudiantes se debe solicitar al correo electrónico soporte@mail.uniatlantico.edu.co donde se les dará respuesta en el tiempo establecido mediante la plataforma Campus.
g) El tiempo establecido para responder la solitud de recuperación de contraseñas es de dos (2) días hábiles.
h) En caso de existir una razón justificada de no uso del correo institucional (licencia, incapacidad, vacaciones, permiso, entre otros), el jefe inmediato debe notificar a la oficina de informática, para que se realice el respectivo bloqueo del usuario durante el tiempo que se encuentra fuera de su labor.

**Manejo de contraseña del CAU**

a) La contraseña debe ser mínimo de ocho (8) caracteres variado entre mayúsculas, minúsculas, números y caracteres especiales.
b) La contraseña debe ser personal e intransferible.

**Internet**

a) Está estrictamente prohibido el uso del servicio de internet para realizar negocios personales o transacciones financieras electrónicas, salvo los expresamente autorizados por la Universidad del Atlántico.
b) La Universidad del Atlántico establecerá los estándares y procedimientos necesarios para control de reportes de acceso y actividad en internet.
c) Es prohibido, salvo aprobación expresa, el uso o habilitación de módems, adaptador o cualquier dispositivo externo de almacenamiento y/o transmisión de datos.
d) La autorización para inspección y monitoreo del uso de Internet se presume desde el momento de asignación de acceso.
e) Queda expresamente prohibido el encadenamiento de proxies externos a la Universidad del Atlántico para la navegación por Internet. La Universidad del Atlántico dispondrá de programas antivirus de obligatoria ejecución al momento de recepción de archivos externos por cualquier vía y en cualquier estación de trabajo móvil o fija.
f) Pro aplicabilidad el consumo de recursos viene ligado con el buen uso de las páginas y su contenido, en el caso de páginas de videos y juegos se aplicarán las políticas descritas en el literal anterior que sugieren el buen uso y utilización de la red.
g) La utilización de páginas web inapropiadas dentro de la organización facilita al desorden de los usuarios en pro de la calidad y el desempeño que se puede lograr, además de esto facilita la infección por malware y virus que adicionarían vulnerabilidades de seguridad de la información a la Universidad del Atlántico.
h) La navegación estará restringida exclusivamente para las labores institucionales y las conexiones que lo requieran, si existiera una página bloqueada a la que sea necesario entrar se deberá solicitar la Oficina de Informática, la debida autorización.
i) El acceso a internet provisto a los usuarios de la Universidad del Atlántico es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine la Alta dirección.
j) La asignación del servicio de internet, deberá solicitarse mediante el procedimiento establecido por la Oficina de Informática. Esta solicitud deberá contar con el visto bueno del Jefe Inmediato.
k) Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por la Oficina de Informática.
l) Los usuarios con acceso a Internet de la Universidad del Atlántico tienen que reportar todos los incidentes de seguridad informática a la Oficina de

Informática, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

**Copyright**

a) La realización de copias no autorizadas de software o material bajo protección de copyright está expresamente prohibida, tanto mediante el uso de los Sistemas de la Universidad del Atlántico como si el material está licenciado o es propiedad de la Universidad del Atlántico.

**Pruebas de seguridad**

b) Está estrictamente prohibida la recogida de información sobre configuraciones de redes, sistemas, software base, aplicativos y controles internos o mecanismos de seguridad asociados a los mismos tanto para aquellos pertenecientes a la Universidad del Atlántico para los ajenos a los mismos, salvo los efectuados por motivos de trabajo por las diferentes áreas en las que es parte de su responsabilidad como la Oficina de Informática, Control Interno y Auditoría.
c) Están estrictamente prohibidos los intentos de acceso no autorizado mediante monitorización de tráfico de datos, y las pruebas de vulnerabilidades o deficiencias de seguridad en los Sistemas de Información tanto para aquellos pertenecientes a la Universidad del Atlántico, salvo los aprobados por la Oficina de Informática, Control Interno y Control Disciplinario.
d) No se considerará acceso no autorizado la monitorización de tráfico necesaria e imprescindible para la resolución de incidencias siempre que sea efectuada por los departamentos técnicos responsables y bajo las normas y procedimientos de seguridad específicos que puedan estar establecidos.

**Escritorio Limpio**

a) Todos los funcionarios internos y externos que presten servicios a la Universidad del Atlántico, adoptarán una política de escritorio limpio con el objeto de prevenir el acceso no autorizado a activos de información cuando estos fuesen desatendidos. De esta manera se evitará la manipulación, pérdida o daño de información que se encuentre en soporte electrónico o en papel.
b) Es responsabilidad de todo usuario guardar los soportes electrónicos y documentos en papel cuando se tenga conocimiento de largos periodos de

tiempo lejos del escritorio, como en la hora de almuerzo, reuniones en otras locaciones y al final de la jornada de trabajo, entre otros.

c) Todo usuario deberá guardar bajo llave aquellos soportes que contengan documentos clasificados como Confidencial o de Uso Interno de la Universidad del Atlántico, durante su ausencia.
d) Todo usuario deberá mantener un entorno de trabajo ordenado para evitar la pérdida de soportes de información, ya sea en formato electrónico o en papel.

**Accesos de los Usuarios**

a) Las Estaciones de trabajo, Servidores y Aplicativos que se tengan al interior de la Universidad del Atlántico deben ser protegidos mediante usuario y contraseña. Se debe establecer una caducidad específica para la contraseña, la cual será asignada inicialmente de forma confidencial y segura al usuario, quien debe realizar cambio en el primer inicio de sesión, además, tendrá una longitud mínima de 8 caracteres y será alfanumérica.
b) Debe quedar registrado en el log los logins/logoff con sus correspondientes horarios y los cambios de contraseña de todos los usuarios del sistema/aplicación.
c) Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
d) Cada usuario deberá contar con su respectivo código para acceder a los sistemas de información, la generación de usuarios genéricos deberá estar restringida.
e) Toda clave de acceso debe estar personalizada, lo cual implica que la clave Administrador del sistema debe ser usada solo en situaciones predeterminadas.
f) La cuenta administradora NUNCA debe ser utilizada para actividades cotidianas, debe permanecer en custodia.
g) Se limitará el otorgamiento de privilegios administrativos para instalación, configuración, monitorización o soporte por parte de personal ajeno al personal designado para tal fin.
h) Para prevenir infecciones por virus informáticos, los usuarios de tecnologías de la información, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Oficina de Informática.
i) Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Universidad del Atlántico, que no esté autorizado por la Oficina de Informática.

j) Los empleados que requieran de la instalación de software o aplicativos que no sean de propiedad de la Universidad del Atlántico, deberán justificar su uso y solicitar su autorización a la Oficina de Informática, a través de un documento firmado por el titular Jefe Inmediato, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software o normatividad que rigen su uso, esto con el fin de tener control sobre todos y cada uno de los programas instalados en la Universidad del Atlántico.

**Uso de impresoras, servicio de Impresión y documentos físicos**

a) Los documentos que se impriman en las impresoras de la Universidad del Atlántico deben ser de carácter institucional.
b) Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
c) Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la Oficina de Informática de la Universidad del Atlántico.
d) La documentación en papel no debe de ser accesible por personal no autorizado. Se evitará dejar documentos en las impresoras y fotocopiadoras, así como en sitios de paso o de atención al público.
e) Si la función no lo requiere, queda prohibida la impresión física de documentos que contenga información de la Universidad del Atlántico.

## 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 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.

# 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.

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.
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 acarreara las sanciones de tipo disciplinario y legarles a que hubiera lugar.