UNAB
BUCARAMANGA

Resolución No. 267

(Noviembre 4 de 2004)

(Por la cual se expide la Política General de Seguridad Informática -UNAB)

El Rector de la Universidad Autónoma de Bucaramanga, en ejercicio de sus funciones estatutarias consagradas en el literal "a" del artículo 31 y, CONSIDERANDO

1. Que es indispensable crear un reglamento donde se describe las normas para la utilización de servicios, el cuidado y el uso de los recursos informáticos.

2. Con el fin de hacer efectiva la correcta administración y prestación de las obligaciones y responsabilidades de usuarios y administradores,

RESUELVE

Artículo Único. Promulgar el Reglamento de la Política General de Seguridad Informática.

Comuníquese y cúmplase.

GABRIEL BURGOS MANTILLA
Rector

MARIA VICTORIA PUYANA SILVA
Secretaria General

DOCUMENTO POLÍTICA GENERAL DE SEGURIDAD INFORMÁTICA
UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA

DEFINICIÓN DE TÉRMINOS

· Administración de aulas: Conjunto de actividades, reglamentos y procedimientos necesarios para mantener utilizables las aulas de cómputo.
· Administración de infraestructura tecnológica: Conjunto de actividades, reglamentos y procedimientos necesarios para mantener en operación las comunicaciones internas y externas y los servicios electrónicos ofrecidos a los usuarios. Se divide en tres áreas: la administración de servidores, la administración de servicios y administración de la red de comunicaciones, cada una con sus respectivas funciones, procesos técnicos, operativos y administrativos.
· Administración de usuarios: Conjunto de actividades, reglamentos y procedimientos necesarios para guiar y autorizar a las personas en el uso de los servicios ofrecidos.
· Ataque: Acción cuyo objetivo es causar daño a un sistema, robar información o utilizar un recurso informático de forma no autorizada.
· Aula de cómputo: Espacio físico en el cual existen computadores personales conectados a la red LAN UNAB para uso de los usuarios. Actualmente existen las aulas mixtas, aulas de clase y aulas de servicio.
· Autenticación: Mecanismo mediante el cual un usuario se identifica ante un servicio electrónico.
· Autorización: Permisos que posee un usuario para poder tener acceso a la información. La autorización es otorgada luego de una autenticación satisfactoria.
· Backup o respaldo: Copia de seguridad de la información en medio magnético o disco duro que esta disponible para recuperar la información en caso de desastre.
· Canal seguro: Comunicación encriptada entre un cliente y un servidor.
· Centro de cómputo: Espacio físico en el cual se encuentran

ubicados servidores institucionales, equipos de comunicaciones y otros que forman parte de la infraestructura tecnológica.
· Clave, password o contraseña: Palabra secreta de mínimo 8 caracteres que autentica a los usuarios ante un servicio electrónico.
· Confidencialidad: Propiedad de la información que hace referencia a la privacidad de esta. Establece que la información sólo puede ser accedida por quien tiene derecho.

Control de acceso físico: Mecanismo utilizado para restringir el acceso de personal no autorizado a un espacio físico.
· Control de acceso lógico: Mecanismo utilizado para restringir el acceso de personal no autorizado a la información. La UNAB utiliza un mecanismo de control de acceso factor 1, el cual consiste en "algo que se sabe", en nuestro caso una clave o contraseña
· Control: Mecanismos que permiten o facilitan el cumplimiento de las políticas establecidas. Por ejemplo: Instalación de certificados digitales - Permite asegurar que la información que se intercambia entre un usuario y un servidor está cifrada.
· Cuenta de usuario: Cuenta que habilita a un usuario a conectarse a la red de datos UNAB y a hacer uso de todos sus servicios. La cuenta de usuario inicialmente autentica al usuario ante el servicio electrónico (le otorga acceso) y posteriormente según su perfil y derechos asignados le autoriza para hacer uso de este (asigna privilegios).
· Disponibilidad: Propiedad de la información que hace referencia a que la información pueda ser accedida siempre que se necesite.
· Elementos periféricos: Son considerados elementos periféricos de las estaciones de trabajo: el teclado, el mouse, los parlantes, la webcam, el monitor y la impresora.
· Estación de trabajo: Equipo de cómputo de escritorio o portátil que utilizan los usuarios para conectarse a la red LAN UNAB. Se incluyen también los equipos de cómputo personales que los empleados ingresen a las instalaciones de la UNAB.
· Granja de servidores: Espacio físico en el cual se encuentra ubicado un grupo de servidores institucionales.
· Incidente: Es el resultado de la materialización de una amenaza. Un evento que pone en riesgo la seguridad de un sistema de cómputo.
· Integridad: Propiedad de la información que hace referencia a que los datos no han sido alterados.
· Nombre de usuario o login: Nombre que identifica a los usuarios para autenticarse ante los servicios electrónicos o la red.
· Plan de recuperación de desastres (DRP): Su principal objetivo es proteger a la organización en el evento de que todas o parte de sus operaciones y/o servicios computacionales se vuelvan inutilizables.
· Recursos informáticos: Conjunto de elementos de hardware y software que la universidad ofrece a la comunidad universitaria para cumplir con sus funciones.
· Sistema de cómputo: Es un conjunto de Hw y Sw que se utiliza para el procesamiento de datos. La interconexión de varios sistemas de cómputo forman un sistema más grande un ejemplo de esto es la Internet.
· Usuario: Persona que puede hacer uso de los recursos informáticos con los que cuenta la universidad.

INTRODUCCIÓN

El presente documento describe claramente las normas para utilización de servicios, el cuidado y el uso de los recursos informáticos, y especifica los derechos, obligaciones y responsabilidades de usuarios y administradores.

Estas normas deben ser adoptadas como política general de seguridad informática, la cual es creada manteniendo los principios democráticos, que propenden a la tolerancia, el respeto por las creencias y derechos de los demás, la cátedra libre y la libertad de expresión, tal y como se menciona en la Misión de la UNAB.

La seguridad informática o seguridad computacional como se le llama en la mayoría de los textos comprende los mecanismos utilizados para crear un ambiente seguro a los sistemas de cómputo y para el uso correcto y adecuado de los recursos informáticos teniendo como premisa en primera instancia la seguridad de las personas, seguida por la seguridad de la información y del hardware.

POLÍTICAS

POLÍTICAS PARA CUENTAS DE USUARIO

Considerando que es importante contar con un sitio centralizado de autenticación de los usuarios y que se debe llevar un control de acceso lógico de los posibles usuarios de la red LAN, la universidad desea implementar un mecanismo que permita identificar a cada uno de los usuarios, con el fin de autorizar o negar servicios según el papel que juega dentro de la universidad. Igualmente garantizar el uso de un mismo nombre de usuario y contraseña facilitando la autenticación para los diferentes servicios electrónicos y al usuario el manejo de contraseñas. Teniendo en cuenta lo anterior se deberá cumplir con las siguientes normas para las cuentas de usuario:

· Estar formadas por un nombre de usuario o login y una contraseña o password únicas e intransferibles.
· Las personas vinculadas oficialmente con la universidad deben poseer una única cuenta de usuario que les permitirá conectarse a la red de datos UNAB, y deben autenticarse con ésta ante los servicios electrónicos con los privilegios, roles y perfiles a que tenga derecho. Los servicios electrónicos, que por su plataforma tecnológica no lo permitan, conservarán el método de autenticación propio, manteniendo el nombre de usuario y respetando las políticas para uso de contraseñas de este documento.
· El proceso de autenticación debe ser de máximo tres intentos para una autenticación satisfactoria, después de éste número de intentos la cuenta debe ser bloqueada.
· Estar respaldadas por una solicitud y deben tener una vigencia de acuerdo a la fecha de vencimiento de la vinculación de su dueño con la universidad. Finalizada su vigencia, deben ser eliminadas todas las autorizaciones relacionadas con la cuenta.

Son responsables de aplicar estas políticas los administradores de servicios electrónicos, los administradores de la red y los administradores de servidores.

POLÍTICAS PARA LAS CONTRASEÑAS O PASSWORD

El medio de autenticación utilizado por todos los servicios electrónicos de la UNAB consiste en un nombre de usuario, asociado a una contraseña, se proyecta realizar una unificación de ésta información de tal manera que un mismo nombre de usuario y contraseña autentiquen al usuario en varias aplicaciones, por ésta razón se hace necesario que tanto usuarios como administradores se aseguren de cumplir con las siguientes normas de seguridad para la creación de contraseñas y uso de las mismas:
· Deben tener una longitud de mínimo ocho caracteres y deben ser de tipo alfanumérico, es decir, estar formadas por la combinación de números, letras mayúsculas, letras minúsculas y caracteres especiales.
· Por ningún motivo una contraseña puede ser el mismo nombre de usuario, espacio en blanco o enter, igualmente no puede estar compuesta de caracteres constantes y otros que cambien de manera predecible, palabras que aparezcan en un diccionario, nombres propios, fechas especiales, nombres de familiares, variaciones del nombre del empleado, del nombre de usuario, del nombre del servidor, del nombre de la universidad, nombres de mascotas, y en general que sean fáciles de adivinar por un tercero.
· En ningún caso se deben construir contraseñas idénticas o parecidas a la anterior.
· Tener una vigencia máxima de 30 días y deben ser de cambio obligatorio.
· Los cambios de contraseña en caso de olvido o autenticación errónea, deben ser efectuados únicamente en forma personal para usuarios locales (empleados) y se debe utilizar un mecanismo que permita disminuir el riesgo de entrega de contraseñas a personas no autorizadas para los usuarios no locales (estudiantes), si se llegase a presentar el caso de un usuario que pertenezca a ambos grupos tendrá prelación el procedimiento de cambio de contraseñas establecido para usuarios locales. El cambió será realizado por la persona del área tecnológica autorizada para dicha labor.
· Las conexiones vía web deben garantizar el envío de contraseñas y nombres de usuario de forma segura.
· Deben ser almacenadas en forma segura en las bases de datos de los servicios electrónicos, impidiendo la consulta de las mismas.
· Únicamente el personal de seguridad informática está autorizado para utilizar software que permita descifrar las contraseñas y comprobar que se está cumpliendo con las políticas establecidas al respecto.
· Son de carácter privado, el cambio de éstas no debe ser realizado en presencia de otras personas. Excepto cuando el usuario requiera el cambio de forma personal, en cuyo caso estarían presentes el dueño de la contraseña (usuario) y el técnico que realiza la nueva asignación de contraseña.

Es responsable de verificar el cumplimiento de éstas normas la oficina de Seguridad Informática, y es deber de los administradores de servicios electrónicos colocar los controles para el cumplimiento de las mismas.

POLÍTICAS PARA LOS USUARIOS

Las buenas prácticas en seguridad informática de los usuarios logran manejar los riesgos por mal uso de los recursos informáticos. La Unab ha definido las siguientes normas básicas que deben seguir los usuarios:

· Son responsables por el cuidado y buen uso de los recursos informáticos entregados para realizar sus funciones.
· Deben informar cualquier requerimiento de soporte informático o irregularidades en el normal funcionamiento de las estaciones de trabajo a la oficina de Helpdesk.
· Son responsables de la cuenta de usuario que se les entregue.
· Deben almacenar únicamente información relacionada con sus actividades laborales en el espacio institucional asignado para ello. Otro tipo de información debe ser almacenada localmente en su estación de trabajo dentro de una carpeta especifica, facilitando así a los técnicos realizar copias de seguridad rápidamente en caso de necesitar asistencia.

· Asegurarse que el software de antivirus de su estación de trabajo esté actualizado y habilitado, si recibe algún tipo de advertencia del software antivirus o sospecha que su antivirus no ha sido actualizado en los últimos 30 días, debe avisar inmediatamente a la oficina de Helpdesk.

Cualquier irregularidad en el cumplimiento de estas normas debe ser reportado a Seguridad Informática, quien debe realizar revisiones periódicas o en el caso que se sospeche el incumplimiento de las mismas.

POLÍTICAS PARA EL MANEJO DE LA INFORMACIÓN

Se han identificado dos grandes grupos de información a proteger como son la información institucional y la información local. La información institucional hace referencia a los datos involucrados en los procesos académicos y administrativos de la universidad, la cual es almacenada en los servidores institucionales de la UNAB. La información local hace referencia a la información almacenada en las estaciones de trabajo de la universidad.

Es responsabilidad de los administradores de servicios electrónicos, garantizar la integridad y la confidencialidad de la información institucional.

Es responsabilidad de los usuarios garantizar la confidencialidad de la información almacenada en las estaciones de trabajo.

Información Institucional:
· Se deben manejar los derechos de lectura, escritura y modificación para usuarios, teniendo en cuenta preservar siempre los principios de integridad, confidencialidad y disponibilidad de la información.
o Entiéndase escritura como la acción de ingresar nuevos datos y, modificación como la acción de cambiar los datos existentes.
· El acceso a la información estará basado en derechos, perfiles y roles de usuario, de la siguiente manera:
o Usuario de nivel 1: Tendrá todos los derechos sobre la información.
o Usuario de nivel 2: Tendrá los derechos de lectura y modificación.
o Usuario de nivel 3: Tendrá los derechos de lectura y escritura.
o Usuario de nivel 4: Tendrá los derechos de lectura.

Información local:
o Los usuarios de las estaciones de trabajo son responsables por la información contenida en estas, los mecanismos que se utilicen para respaldo y recuperación de la información en caso de incidentes y de mantener su confidencialidad.
o Los usuarios de las estaciones de trabajo son responsables por los riesgos que corren al compartir archivos y/o carpetas en la red.
· La clasificación de información, tipos de usuarios y perfiles, de cada servicio electrónico debe ser presentada a Seguridad Informática con la finalidad de realizar las observaciones y recomendaciones necesarias para mantener seguridad, e implementar esta en los desarrollos.

POLÍTICAS PARA LOS SERVICIOS ELECTRÓNICOS

Los servicios electrónicos ofrecidos por la UNAB están descritos en el anexo No. 1. Se han definido unas normas básicas para garantizar el buen desempeño de los servicios electrónicos, la disponibilidad de éstos y la recuperación en caso de desastres:

· En lo posible en cada servidor debe existir un solo servicio electrónico, se permite la instalación de otros siempre y cuando sean dependientes.
· Deben contar con los siguientes manuales: de usuario, de administración y documento de políticas de seguridad.
· Los servicios electrónicos que vayan a ser utilizados en la Red LAN de la UNAB, deben cumplir con las políticas establecidas para contraseñas o password y cuentas de usuario.
· Deben cumplir con un periodo de prueba antes de su implementación definitiva.
· Deben tener un responsable de su administración técnica.
· El software para gestión administrativa aprobado por Desarrollo Tecnológico es considerado software de servicios electrónicos institucionales.
· Deben tener su clasificación de usuarios cumpliendo con las políticas establecidas para manejo de la información.
· La adaptación de un software externo que involucre desarrollo, debe ser realizada por el proveedor con el fin de recibir soporte y las actualizaciones respectivas en la adquisición de nuevas versiones.

En cuanto a la administración de servicios electrónicos
· Los servicios electrónicos se clasifican según su criticidad en: o Servicio critico: Servicio que al no estar disponible imposibilita cumplir con los objetivos de la universidad de enseñanza, investigación y extensión, incluyendo su gestión administrativa.
o Servicio medianamente crítico: Servicio que al no estar disponible dificulta cumplir con los objetivos de la universidad, incluyendo su gestión administrativa.

o Servicio no critico: Servicio que al no estar disponible no impide ni dificulta la gestión administrativa de la universidad ni afecta el cumplimiento de sus objetivos.

· Para los servicios institucionales en producción, los administradores no pueden entregar las claves de administración a ninguna persona. Cualquier actividad que se requiera hacer sobre estos servicios debe ser realizada directamente por el administrador y nunca por otra persona.
· La administración de los servicios electrónicos institucionales debe ser realizada por personal de Desarrollo Tecnológico.
· Deben tener un esquema de respaldo y recuperación para casos de desastre.
· La revisión y aplicación de parches y actualizaciones liberadas por los fabricantes, para las aplicaciones que soportan servicios electrónicos deben realizarse en intervalos de máximo tres meses.

Son responsables de cumplir dichas normas los administradores de servicios electrónicos y servidores.

POLÍTICAS PARA SERVIDORES

Los equipos servidores en una red la exponen a ataques por virus, gusanos, troyanos, hackers, entre otros, debido a la cantidad de servicios de carácter público que en ellos pueden ser habilitados y a vulnerabilidades de seguridad de los diferentes software y sistemas operativos. Para disminuir éste tipo de riesgo la universidad define:

· Los equipos con dirección IP pública son clasificados como servidores y deben estar ubicados en la Red Institucional y tener un responsable de su administración.
· Los equipos que soporten software para gestión administrativa o servicios ofrecidos a la comunidad universitaria, aprobado por Desarrollo Tecnológico deben estar ubicados en la Red Institucional y son clasificados como servidores institucionales. En éstos no podrá ser instalado ningún otro tipo de software.
· Cada servidor debe tener su hoja de vida registrada en seguridad informática con la siguiente información: sistema operativo, servicios, nombres de dominio, direcciones IP, puertos que debe tener abiertos y responsable de su administración. Cualquier modificación debe ser reportada oportunamente a Seguridad Informática y a los administradores de servicios electrónicos. Son responsables de suministrar esta información los administradores de cada servidor y el responsable de revisar que se cumpla con las especificaciones entregadas es Seguridad Informática.
· Deben estar ubicados en un espacio físico adecuado manteniendo los estándares definidos para centros de cómputo y granja de servidores. Ver anexo No. 2.
· Los servidores que sean conectados a la red LAN, deben cumplir con la siguiente configuración:
o En caso de sistema operativo windows
· Pertenecer a un dominio de windows (Pueden presentarse dominios independientes).
· Antivirus institucional local con actualizaciones descargadas directamente de la red UNAB.
· Parches actualizados a la fecha de instalación, del sistema operativo y aplicaciones.
· Aplicaciones propias para su administración local o remota de forma segura
· Inhabilitar los servicios propios del sistema operativo que no se requieran para su funcionamiento.
· Protocolo TCP/IP
· Servicio de NETBIOS sobre TCP/IP
· Usuarios invitado, administrador y guest deshabilitados
· Usuario con privilegios de administración con contraseña fuerte (Ver políticas para claves y contraseñas)
· Solamente los servidores de dominio pueden tener una base de datos de usuarios local. De existir usuarios locales estos deben tener contraseñas fuertes.

o En caso de sistema operativo unix
· Parches actualizados a la fecha de instalación, del sistema operativo y aplicaciones.
· Aplicaciones propias para su administración local o remota de forma segura
· Inhabilitar los servicios electrónicos y de sistema operativo que no se requieran para su función.
· Protocolo TCP/IP
· Los usuarios deben tener su respectiva contraseña fuerte (Ver políticas para claves y contraseñas).
· Adicionalmente la criticidad de los servidores se medirá por el servicio que soportan y su importancia en la función de operación de la universidad. Ver anexo No. 3. Esto será tenido en cuenta en el momento de crear Planes de Recuperación de Desastres (DRP) en caso de contingencia.

En cuanto a la administración de servidores

· La administración de los servidores que soportan servicios institucionales debe ser realizada por la Red Institucional.
· No se puede acceder local ni remotamente a los servidores con sistema operativo basado en unix utilizando en primera instancia el usuario root o equivalente.
· La administración remota de los servidores debe realizarse utilizando un canal seguro.

· Los servidores deben tener un esquema para mantener registros digitales de acceso y operación.
· Los servidores deben tener un esquema de copias de respaldo y recuperación para casos de desastre.
· La revisión y aplicación de parches y actualizaciones liberadas por los fabricantes, para el sistema operativo de los servidores deben realizarse en intervalos de máximo tres meses.
· Para los servidores en producción, los administradores no podrán entregar la clave de root o equivalente a ninguna persona. Cualquier actividad que se requiera hacer sobre estas máquinas deberá ser realizada directamente por el administrador y nunca por otras personas.

Son responsables de cumplir todas las políticas relacionadas con servidores los administradores de servidores. Seguridad informática debe realizar revisiones periódicas a los mismos, con la finalidad de mejorar la seguridad o detectar fallas.

POLÍTICAS PARA USO DE LA INFRAESTRUCTURA DE RED

La infraestructura de red comprende todo el cableado que permite realizar la conexión con la red telefónica y la red de datos. El buen funcionamiento de esta infraestructura depende de varios factores, entre ellos la configuración y uso de las estaciones de trabajo, el medio ambiente de los centros de cableado, los trabajos que afecten el tendido de cableado, el control en el uso de ancho de banda de la misma, entre otros. Con el fin de mantener la infraestructura y utilizar de la mejor forma los recursos existentes, se definen las siguientes normas:

Relacionado con el uso de ancho de banda para Internet
· La red UNAB no debe permitir el tráfico de protocolo ICMP con redes externas.
· No descargar música o vídeos utilizando la red de datos UNAB.

Relacionado con el direccionamiento IP

· El direccionamiento IP de las estaciones de trabajo debe ser privado. Las estaciones de trabajo que requieran dirección pública para acceder a un servicio específico, deben ser asignadas mediante NAT estático.
· Las estaciones de trabajo con IP pública tipo NAT se consideran como servidores potenciales, por tanto deben ser revisadas periódicamente por Helpdesk con el fin de disminuir los riegos por vulnerabilidades de sus servicios activos y sistema operativo. La Red Institucional puede suspender este servicio si se comprueba que está afectando la operación de la red UNAB.
· Se asignará direccionamiento público únicamente para los servidores cuyos servicios lo requieran.

Relacionado con la infraestructura física:

· Los proyectos relacionados con la infraestructura de telecomunicaciones deben ser avalados por la Red Institucional antes de su desarrollo y esta será la interventora de los mismos.
· Los centros de cómputo deben tener de forma independiente: red eléctrica, aire acondicionado de precisión, UPS de respaldo, mecanismos de detección y extinción de incendios, sistema de monitoreo y control de acceso.
· La Red Institucional es la responsable de la administración y mantenimiento de la infraestructura de los centros de cómputo, de los equipos activos y pasivos de red, centros de cableado y cableado estructurado de voz y datos.
· Los centros de cableado deben tener acceso restringido, y el acceso es autorizado únicamente por personal de la Red Institucional.

La Red Institucional es responsable de hacer cumplir las normas establecidas para la infraestructura de red, uso del ancho de banda y direccionamiento IP.

Relacionado con las estaciones de trabajo:

Los computadores personales son herramientas de trabajo que entrega la universidad a sus empleados, y son estos quienes deben responder por el buen uso de los mismos y por cuidar la información almacenada en ellos. La instalación de software se restringe para asegurar que la universidad cumpla con las leyes de licenciamiento de software, evitar las incompatibilidades y asegurar el cumplimiento del soporte por parte de los proveedores y el personal de Helpdesk. La administración de hardware se restringe para evitar la perdida de las garantías.

Se han definido las siguientes políticas para el cuidado de las estaciones de trabajo:

· La revisión y aplicación de parches y actualizaciones liberadas por los fabricantes, para el sistema operativo debe ser en intervalos de máximo 30 días.
· Las estaciones de trabajo de la universidad que vayan a ser conectadas a la red de datos UNAB, deben cumplir con la siguiente configuración:

o Pertenecer a un dominio de windows
o Navegadores Netscape e Internet Explorer en sus últimas versiones. Ver anexo No. 4.
o El navegador debe ser configurado para que no utilice el proxy para buscar direcciones locales.
o Cliente para manejo de correo electrónico definido por la universidad. Ver anexo No. 4.
o Antivirus local institucional con actualizaciones descargadas automáticamente de la red UNAB. Ver anexo No. 4.
o Parches actualizados a la fecha de instalación de sistema operativo y aplicaciones.
o Aplicaciones propias para la administración de los equipos. Ver anexo No. 4.
o Desactivar los servicios no requeridos. Ver anexo No. 4.
o Protocolo TCP/IP
o Servicio de NETBIOS sobre TCP/IP
o Usuario local con privilegios de administración con contraseña fuerte (Ver políticas para claves y contraseñas), conocida únicamente por los técnicos de Helpdesk.
o Deshabilitar los usuarios locales, incluidos los creados por defecto.

· Helpdesk debe llevar una hoja de vida de cada una de las estaciones de trabajo de la universidad.
· Toda estación de trabajo que vaya a ser conectada en la red UNAB, debe registrar la dirección física de su tarjeta de red en la Red Institucional antes de ser conectada.
· Los cambios en la configuración de las estaciones de trabajo deben ser realizados únicamente por la oficina de Helpdesk. Cualquiera de las siguientes actividades es considerada como cambios en la configuración de las estaciones de trabajo:
o Cambiar el computador de punto de red.
o Usar un disco extraíble para iniciar la estación de trabajo.
o Quitar la cubierta de los equipos y/o cambiarle, sustraer o agregar partes.
o Intercambiar los elementos periféricos de las estaciones de trabajo.
o Instalar software, sin la debida autorización de la oficina de helpdesk.

La oficina de Helpdesk es la responsable de hacer cumplir las normas para estaciones de trabajo.

POLÍTICAS PARA AULAS DE CÓMPUTO

La creación de aulas de cómputo sin ninguna supervisión, pone en riesgo la seguridad de la red UNAB, debido a que no se efectúa una administración de las estaciones de trabajo aumentando la posibilidad de que en cualquier momento una o varias de ellas se conviertan en atacantes de la red o puertas abiertas para llegar a todas las demás estaciones de trabajo de la universidad, adicionalmente el personal de desarrollo tecnológico no tiene conocimiento del estado de las mismas lo que complica la atención en caso de un siniestro.
· Las aulas de cómputo deben ser administradas y supervisadas por la dependencia Aulas de Informática. La administración como mínimo debe cumplir con lo siguiente:
o Control y registro del acceso y la asignación de estaciones de trabajo.
o No ingresar alimentos ni bebidas.
· En el proceso de creación de un aula de cómputo se debe contar con la participación y aprobación de Aulas de Informática dependencia encargada de su administración y la Red Institucional dependencia encargada de la infraestructura de comunicaciones.

ANEXO No. 1

SERVICIOS ELECTRÓNICOS OFRECIDOS POR LA UNAB

Servicios de Red
· Proxy
· DNS
· DHCP
· Wins
· Transferencia de archivos
· Impresión

Sistemas de Información y/o aplicaciones
· Correo electrónico
· Sitios Web: www.unab.edu.co, unabvirtual.unab.edu.co, www.unabvirtual.edu.co
· Portales Web: Intranet, Docente, Estudiantes, Futuros Universitarios, Egresados.
· Grupo de noticias
· Mensajería instantánea
· Aleph
· Sara
· Cosmos

ANEXO No. 2

ESTANDARES PARA CENTROS DE CÓMPUTO Y GRANJA DE SERVIDORES

Los centros de cómputo o granja de servidores deberán contar mínimo las siguientes protecciones:

· Espacio físico adecuado para la ubicación de las máquinas y equipos.

· Pisos falsos.
· Ductos para cableado.
· Sistema de vigilancia.
· Sistema de detección y contención de incendios.
· Sistema de control de acceso al sitio para personal autorizado.
· Ubicación en sitios no propensos a inundaciones.
· Aire acondicionado para una temperatura de mínimo 18 grados centigrados con todas las máquinas encendidas y control de humedad.
· Adecuaciones eléctricas independientes.
· UPS de respaldo y con sistema de contingencia para casos extremos.
· Iluminación adecuada de día y de noche.
· Planta eléctrica con un tiempo máximo de 30 segundos de arranque.
· No debe almacenarse material inflamables.

ANEXO No. 3

MATRIZ DE CLASIFICACION DE SERVIDORES Y SERVICIOS

El archivo que contiene la información y clasificación de servidores y servicios se considera de uso exclusivo del personal del área técnica y por lo tanto sólo éste tendrá accedo a dicha información.

ANEXO No. 4

DEFINICIONES VARIAS

Este anexo contiene las especificaciones para realizar la instalación y configuración de una estación de trabajo, según las políticas de seguridad informática existentes, y las aplicaciones y software autorizados por Desarrollo Tecnológico.

Aplicaciones colaborativas: La configuración mínima de las estaciones de trabajo contempla la instalación de las siguientes aplicaciones:

Navegadores
· Internet Explorer a partir de la versión 5.0 y el Netscape versión 4.7 o 7.0. Se han escogido los anteriores navegadores, teniendo en cuenta la facilidad para el usuario de acceder a todo el contenido web existente en Internet y a las características técnicas de las estaciones de trabajo que soportan dicho software. Para mayor información ver manuales de configuración de equipos del departamento de Helpdesk.

Clientes de correo
· El cliente de correo autorizado es Netscape en sus versiones 4.7 y 7.0. Se ha escogido debido a su facilidad de manejo, administración y tipo de licenciamiento.
· El cliente Microsoft Outlook será utilizado únicamente con fines académicos en las aulas de clase. Se debe deshabilitar la opción del Outlook Express del Sistema Operativo Windows.

Antivirus
· El antivirus institucional configurado en todas las estaciones de trabajo es el e-trust de Computer Associates versión 7.0.139.

Herramienta ofimática
· Word 97/2000/XP
· Excel 97/2000/XP
· Power Point 97/2000/XP

Aplicaciones académicas: El software académico autorizado para utilizar en la universidad se encuentra descrito detalladamente en el archivo SOFTWARE ACADEMICO.pdf adjunto a éste documento.

Adicionalmente en las aulas de clase y de servicio actualmente se utiliza el siguiente software:

Sistemas operativos
· LINUX REDHAT 7.....
· MICROSOFT WINDOWS 2000 SERVER
· MICROSOFT WINDOWS NT SERVER 4.0

Multimedial (sm)
· MACROMEDIA DIRECTOR 8
· MACROMEDIA DREAMWEAVER MX
· MACROMEDIA DREAMWEAVER ULTRADEV FOR WINDOWS
· MACROMEDIA FIREWORKS MX
· MACROMEDIA FLASH 5.0 FOR WINDOWS
· MACROMEDIA FLASH MX
· MACROMEDIA STUDIO MX 1.1

Diseño gráfico (sdg)
· ADOBE PHOTOSHOP 8.0
· CORELDRAW 8.0
· FRONTPAGE2000

Estadístico, matemático y financiero (semf)
· MATHLAB 5.2
· STATGRAPHICS FOR WINDOWS 4.0
· WINQSB FOR WINDOWS
· SPSSS

Gestion (sg)
· ACROBAT 5.0
· MICROSOFT OFFICE 2000 PROFESIONAL
· SIIGO
· WINZIP 8.0

Lenguajes de programación (slp)
· BORLAND TURBO C++ 1.01
· BORLAND TURBO PASCAL 6.0
· VISUAL . NET

Manejadores base de datos (smbd)
· ORACLE 8i

Simulación (sds)
· POWER SIM STUDIO 2002

Soporte a usuario final (ssu)
· ANTIVIRUS ETRUST 7.0

Diseño asistido por computador (scad)
· SOLID EDGE 2002
· SOLID WORKS 2000

Administración hotelera (sah)
· FIDELIO

Composición musical (scm)
· FINALE 2002

Aplicaciones de producción: Sólo deben estar instaladas en las estaciones de trabajo autorizadas y donde se necesiten para cumplir con las funciones de los cargos.

· Cliente para el sistema de información COSMOS: BANNER
· Cliente para SIAA
· Cliente para SIAC
· Cliente para ACADEMIA
· Cliente para AS400
· Cliente para SINCA
· Cliente para ESCORPIO (Únicamente Dependencias Licenciadas - Consultar con Helpdesk)
· Cliente para SARA

Herramientas ofimáticas:
· OFFICE 97/2000/XP
· STAROFFICE 5.2
· LOTUS SMART SUITE
· ACROBAT READER
· WINZIP