RESOLUCIÓN RECTORAL 847
(14 diciembre de 2015)

Por medio de la cual se adopta las políticas de seguridad informática de la Institución Universitaria Pascual Bravo

El Rector en ejercicio de sus facultades legales y estatutarias y,

CONSIDERANDO

Que las tecnologías de la información y las comunicaciones (TIC), son en la actualidad una herramienta de uso prioritario para todas las entidades públicas. Al respecto, la Institución Universitaria Pascual Bravo, reconoce la importancia de éstas para el debido desarrollo de sus funciones y el cumplimiento de su misión institucional.

Que en concordancia se han diseñado herramientas que sirvan de guía para que los usuarios que accedan y utilicen los servicios tecnológicos que presta la Institución Universitaria puedan hacer un adecuado uso de los mismos, en términos éticos y legales. Siendo las políticas que a continuación se describen, los parámetros a seguir por la entidad en términos de uso de activos de programas.

Que con el fin de dar un uso adecuado a las nuevas tecnologías se establecen las Políticas de Seguridad Informática (PSI); las cuales se consolidan como herramientas organizacionales que le permiten a los usuarios obtener un mayor provecho, evitando un uso indebido de las mismas.

Que el manual de políticas y estándares informáticos es un conjunto de requisitos definidos por la Oficina Asesora de Planeación área de informática con respecto al manejo del software y al uso del hardware.

Que en mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO. Adoptar las políticas de seguridad informática de la Institución Universitaria Pascual Bravo, la cual estará integrada, así:

Objetivos

- Sensibilizar a los funcionarios y contratistas sobre la importancia de hacer un uso adecuado de los bienes y servicios informáticos que presta la entidad.
- Generar en los funcionarios y contratistas la cultura del autocontrol para acceder a los servicios informáticos de forma ética y legal.
- Posibilitar la mejora continua en los procesos informáticos que lleve a cabo la entidad.

Alcance: Con el manual, se describen las políticas y estándares informáticos para todos los usuarios que tienen a su cargo recursos informáticos, orientarlos a alcanzar los logros institucionales e informarles de las políticas que deben aplicar para el buen uso de los equipos de cómputo, aplicaciones y demás servicios informáticos.

Beneficios: El manual beneficiará a todos los usuarios que utilizan los servicios informáticos de la institución, ya que las políticas y estándares en materia informática son la base del buen funcionamiento, desempeño, seguridad y protección de los activos tecnológicos del Campus Universitarios.

DIRECTRICES GENERALES. El Proceso de Gestión TIC tiene como objetivo: Planear, ejecutar, y controlar todas las actividades relacionadas con la administración de hardware, software, redes, telecomunicaciones y sistemas de información institucional de manera que se vele por la adecuada prestación de los servicios misionales de la entidad soportados en tecnologías de información y comunicaciones.

Se han definido, como Políticas en materia de informática, sistemas y desarrollo tecnológico en general, las siguientes:

- Mantener funcionando constante y permanente toda su estructura computacional y plataforma tecnológica para garantizar la prestación ininterrumpida del servicio educativo y demás servicios complementarios apoyados por la tecnología.
- Mantener actualizados de manera permanente los equipos, software, sistemas operativos y sistemas de información institucional de manera que se correspondan con los desarrollos tecnológicos, los planes y proyectos de la entidad, los programas académicos y las políticas gubernamentales en materia de derechos de autor.
- Ejecutar de manera periódica, planes de renovación tecnológica de equipos, periféricos y sistemas de información de acuerdo con las actividades y presupuestos consignados en los proyectos institucionales.
- Revisar de manera permanente el estado, cantidades, calidades y cualidades de los equipos de cómputo y periféricos de las dependencias, salas de informática, laboratorios, cafés, y demás estaciones de trabajo que soportan los procesos misionales y de apoyo de la entidad, de manera que pueda garantizarse la suficiencia, funcionamiento, desempeño y características técnicas adecuadas de los mismos.
- Velar por la seguridad física y lógica de las redes y los sistemas de información a través de la implementación de políticas, estrategias y soluciones tecnológicas que eviten la intrusión a los sistemas, la interrupción de los servicios de red y la perdida de datos.
- Mantener controlados las fallas y daños presentados en la plataforma tecnológica (debidos a la operación normal de los equipos, virus informáticos, variaciones eléctricas, mala operación, etc.) a través de los planes de mantenimiento preventivo, correctivo y predictivo.
- Acatar las recomendaciones técnicas sustentadas por organismos gubernamentales, expertos, pares institucionales, empresas privadas y demás actores involucrados, en materia de procesos tecnológicos, sistemas de información, seguridad, licenciamiento, software, hardware y redes.
- Realizar las evaluaciones pertinentes y periódicas, a la plataforma tecnológica, utilizando herramientas y metodologías estándar y probabas por entidades del mismo nivel.

La Institución Universitaria Pascual Bravo ha adquirido copias debidamente licenciadas de programas para PC, obtenidas de proveedores autorizados. Dichas copias son instaladas en los PC de la entidad y se han hecho reproducciones de seguridad en concordancia con los acuerdos de las licencias y las políticas de la institución. Al respecto, no pueden hacerse

copias de los programas o de su documentación sin el consentimiento expreso por escrito de quien provee el programa y de Microsoft.

1. **PROGRAMAS DE OTRAS FUENTES.** La Institución Universitaria Pascual Bravo proveerá copias de los programas que han sido adquiridos legalmente, el uso de los programas que se obtienen a partir de otras fuentes, puede implicar amenazas legales y de seguridad para el Instituto, por lo que dicho uso está estrictamente prohibido.

2. **COPIAS ADICIONALES.** En algunos casos, el acuerdo de la licencia para un programa en particular, puede permitir una copia adicional, para ser instalada en un portátil o en un PC, posibilitando que un usuario utilice ambas copias. Los empleados y contratistas no están autorizados para hacer copias adicionales del programa o de su documentación sin previa aprobación de la Oficina Asesora de Planeación. De ser posible, la aprobación para hacer las copias mencionadas será autorizada, siempre que existan razones de necesidades válidas.

3. **COPIAS NO AUTORIZADAS.** La duplicación no autorizada de programas o de su documentación, implica una violación a la ley, además de ir en contravía con los estándares de conducta establecidos por la Institución Universitaria. En consecuencia, aquellos funcionarios y/o contratistas que hagan, adquieren o utilizan copias no autorizadas de programas para PC y su respectiva documentación, se les desinstalara dicho programa y se verificará que estos programas no sean instalados de nuevo.

4. **CONTROLES.**
   a) **La Institución Universitaria Pascual Bravo** se reserva el derecho de proteger su reputación y sus inversiones en programas para PC, fomentando controles estrictos, para prevenir el uso y la fabricación de copias no autorizadas de los programas. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorias anunciadas y no anunciadas a los PC con el fin de asegurar su buen uso.
   b) La subdirección de planeación área de informática, podrá limitar el acceso a determinadas páginas de internet horarios de conexión y servicios ofrecidos por la red, cuando estos no sean en cumplimiento de las funciones laborales
   c) Corresponde a la Oficina Asesora de Planeación área de informática el control y resguardo de las licencias de programas de cómputo (software) por lo que se debe mantener un registro (inventario) del software.
      - Programas de cómputo con licencia.
      - Programas de cómputo de uso libre y autorizado por la subdirección de planeación área de informática.
      - Programas o aplicaciones desarrollados por la entidad.

5. **MANEJO DE LA INFORMACION.**
   a) Todo acto realizado por funcionarios y/o contratista utilizando su usuario y contraseña es de su responsabilidad.
   b) Los equipos de cómputo contarán con particiones de discos duros, donde el disco C será utilizado para el sistema operativo y los programas y las demás particiones para el almacenamiento de la información propia de sus funciones. Esto Con el objeto de crear

carpetas de trabajo específicas para facilitar el almacenamiento, respaldo, protección y localización de la información en los equipos de cómputo.

6. USO, INSTALACIÓN Y DESINSTALACIÓN DE SOFTWARE Y HARDWARE. El uso adecuado de los recursos tecnológicos asignados por la Institución Universitaria Pascual Bravo**,** a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

a. La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la Institución Universitaria Pascual Bravo, es responsabilidad del área de informática y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por e la Institución a través del área de informática.
b. Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla institucional, entre otros. Estos cambios pueden ser realizados únicamente por el área de informática.
c. El área de informática, debe definir y actualizar, de manera periódica, la lista de Software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
d. Únicamente los funcionarios y terceros autorizados por el área de informática, previa solicitud escrita por parte de la dependencia que lo requiera, pueden conectarse a la red Inalámbrica de la Institución Universitaria Pascual Bravo.
e. La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de la Institución, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de informática.
f. Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la Institución Universitaria Pascual Bravo; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidas por el área de informática.
g. La sincronización de dispositivos móviles, tales como PDA, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Institución, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con el área de informática y podrá llevarse a cabo sólo en dispositivos provistos por la organización, para tal fin.
   Toda instalación de software deberá ser autorizada por la Subdirección de Planeación área de informática, a través del funcionario competente, a fin de dar cumplimiento a las políticas y directrices aprobadas para el manejo del software.
h. No se permite la instalación de programas con carácter de juego pornografía, video, y música en ningún caso.
i. Solo se encuentran autorizados para realizar cambios en la configuración original de los equipos, así como para destapar, agregar o retirar partes o el pc, los funcionarios designado por la Subdirección de Planeación área de informática.
j. Los equipos se deben apagar correctamente en las ausencias prolongadas y al final de la jornada laboral.

k. Toda solicitud de requerimiento técnico debe realizarse a través de la Intranet institucional, según el formato establecido para el efecto en el software de la mesa de ayuda.
l. La Oficina Asesora de Planeación área de informática llevarán un registro de los servicios de mantenimiento preventivo, correctivo, y asesorías en materia de tecnología de información.
m. Se entregarán a cada usuario de la Institución, los equipos tecnológicos con su respectiva acta, la cual se archivara en las bases de datos de la institución, con el fin de llevar el control para las garantías y el mantenimiento respectivo.
n. Cuando se quiera trasladar un bien informático por parte del funcionario responsable del mismo, deberá ser reportado previamente al personal autorizado de la Oficina Asesora de Planeación área de informática; el cual igualmente procederá con el traslado del equipo y la anotación respectiva en el inventario.
o. Para las Aulas informáticas se realizara 2 programas de mantenimiento preventivo anual, para garantizar el correcto funcionamiento de las tecnologías de la información y las comunicaciones y para el área administrativa se programara un mantenimiento preventivo anual el cual será realizado por personal del área de informática.

7. USO DEL INTERNET INSTITUCIONAL. El servicio de internet suministrado por la Institución Universitaria es una herramienta de apoyo a las funciones, y su uso será responsabilidad de todas las personas que laboran en él, por lo cual se debe controlar, verificar y monitorear de acuerdo con las siguientes directrices.

El servicio de internet institucional únicamente puede ser utilizado para el desarrollo de actividades directamente relacionadas con el cumplimiento de las funciones de sus servidores o para la misión de la institución dentro de la red administrativa y en la red académica para uso de la comunidad estudiantil.

a) No está permitido

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- No se permitirá el uso de internet para enviar o descargar archivos de video, audio, música, texto, fotos, etc., y todas aquellas actividades que no sean propias del cumplimiento de los propósitos institucionales o de las funciones laborales.
- No se permite el uso de chat con fines personales.
- El uso de herramientas de comunicaciones, como Facebook o Twitter, Messenger, o cualquier otra aplicación no se encuentra autorizada para ningún funcionario de la Institución, excepto que se trate del cumplimiento o fines institucionales.
- No se permite el intercambio no autorizado de información de propiedad de la Institución Universitaria Pascual Bravo, de sus clientes y/o de sus funcionarios, con terceros.

b) La Institución Universitaria Pascual Bravo, debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

c) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

8. **CORREO ELECTRÓNICO INSTITUCIONAL.** El correo electrónico institucional es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta para agilizar las comunicaciones oficiales que apoyen la gestión institucional, es por esto que los funcionarios y terceros autorizados a quienes la Institución Universitaria Pascual Bravo les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a. La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de la Institución Universitaria Pascual Bravo, así mismo podrá ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.
b. Los mensajes y la información contenida en los buzones de correo son propiedad de la Institución Universitaria Pascual Bravo, y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva.

c. El envío de información Institucional debe ser realizado exclusivamente desde la cuenta de correo que la Institución Universitaria Pascual Bravo, proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.
d. El envío masivo de mensajes publicitarios Institucionales deberá contar con la aprobación de la Oficina Asesora de Comunicaciones. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe por alguna circunstancia realizar envío de correo masivo de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o Servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.
e. Todos los mensajes enviados deben respetar el estándar de formato e imagen Institucional definido por la Institución Universitaria Pascual Bravo, y deben conservar en todos los casos el mensaje legal Institucional.

9. **RESPALDO DE LA INFORMACIÓN [ISO/IEC 27001:2005 A.11.1].** El contar con respaldo de la información permite a las dependencias y a los usuarios en algún momento dado

recuperar información que haya sido dañada por virus, fallas en el equipo o accidentes. Por lo tanto se deben tener en cuenta los siguientes parámetros en cuanto a este tema:

a) La Oficina Asesora de Planeación área de informática es la única dependencia autorizada para realizar copias de seguridad del software licenciado por la entidad, el cual no debe ser copiado para uso personal o suministrado a terceros.
b) Los usuarios deberán hacer copia de seguridad de la información de los procesos y/o proyectos a su cargo en los servidores de archivos asignados por la Oficina Asesora de Planeación área de informática. Esta información será respaldada de forma periódica por el área de informática.
c) Cada área de gestión, usuaria de sistemas de información específicos, será responsable de respaldar la información procesada de acuerdo con sus necesidades, en concordancia con las políticas de manejo y uso de la información, según el ciclo de vida de la información, el movimiento de ésta y el histórico que proporcione el sistema.

10. SERVICIO DE ANTIVIRUS. La Institución Universitaria Pascual Bravo contará con licencias de Antivirus para uso en todos los computadores de la institución, tanto clientes como servidores. Para lo cual se tienen las siguientes directrices:

a) Es obligatorio el uso y actualización de programas antivirus en todos aquellos equipos de cómputo y servidores, propiedad del Pascual Bravo donde las plataformas soporten y prevean su utilización.
b) Los equipos que ingresen al Instituto por un determinado periodo como el caso de los equipos de los contratistas deben tener un programa antivirus activo y actualizado antes de conectarse a la red de la institución.
c) Es responsabilidad de los usuarios realizar análisis de las memorias USB y/o discos portátiles antes de utilizarlos.
d) En caso de detectar virus en cada computador, el usuario debe desconectar el equipo de la red y solicitar soporte técnico de forma inmediata.

POLITICAS DE SEGURIDAD INFORMATICA, DE DATOS Y DE SISTEMAS:

DE SEGURIDAD DEL SITIO WEB: Las políticas de seguridad básicas para el sitio Web se divide en:

1. **Acceso físico al servidor:** Controladas por autorización directa del responsable de Informática y del Data Center de servidores.
2. **Acceso a través de escritorio remoto o terminal server:** Controlada por un usuario y contraseña, autorizada por el administrador de los servidores.
3. **Acceso a través de cuenta FTP:** Controlada por usuario y contraseña, autorizado por el administrador de los servidores.
4. **Acceso a la Base de Datos:** Controlada por un usuario y contraseña, autorizada por el administrador de los servidores, que depende de la BD a la que se desea acceder
5. **Acceso al contenido del sitio Web:** Controlada por un usuario y contraseña, autorizada por el administrador del sistema, que define el perfil y el alcance al que se tiene acceso con la información, estos perfiles son desde el CMS Joomla son:
   - Superadministrador
   - Administrador

- Gestor
- Publicador
- Autor
- Usuario registrado
- Usuario visitante

6. **Acceso a la información de trámites:** Controlada por un usuario y contraseña, autorizada por el administrador del sistema, que define el perfil y alcance al que se tiene acceso con cada trámite:
   - Administrador
   - Docente
   - Empleado
   - Estudiante
7. **Ingreso de contenido al sitio Web:** El contenido debe ser ingresado por el Webmaster, autorizado por Comunicaciones, cumpliendo con los estándares de accesibilidad.
8. **Ingreso y publicación de Información en Redes Sociales:** Este contenido debe ser ingresado por el Social Media Manager o Webmaster, con autorización de la persona responsable en comunicaciones.
9. **Ingreso de Notas al Sistema:** Estas deben ser ingresadas por los docentes, en las fechas estipuladas para ello.
10. **Ingreso y publicación de Noticias y Novedades:** El contenido de Noticias y novedades debe ser ingresado por el Webmaster, y aprobados por el área de comunicaciones.

POLÍTICAS DE DESARROLLO DE SOFTWARE:

BASADA EN METOLOGÍA UML.

Lenguaje Unificado de Modelado (LUM o **UML**, por sus siglas en inglés, *Unified Modeling Language*) es el lenguaje de modelado de sistemas de software más conocido y utilizado en la actualidad; está respaldado por el OMG (Object Management Group). Es un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema. UML ofrece un estándar para describir un "plano" del sistema (modelo), incluyendo aspectos conceptuales tales como procesos de negocio, funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y compuestos reciclados.

JUSTIFICACIÓN. Debido a la importancia de controlar la información en cada uno de los procesos que la institución requiere y minimizar los riesgos en el desarrollo del software, se hace necesario entonces implementar una metodología de desarrollo que garantice el buen funcionamiento de los procesos en la Institución Universitaria Pascual Bravo, permitiendo estructurar cada uno de ellos.

OBJETIVOS DE LA IMPLEMENTACIÓN DE LA METODOLOGÍA

- Registrar los requisitos de un sistema de información
- Proporcionar un método de desarrollo
- Permitir construir un sistema de información en un tiempo apropiado, bien documentado y fácil de sostener
- Implementar e identificar cualquier cambio en el menor tiempo posible

1. **Investigación preliminar.** La solicitud para recibir ayuda de un sistema de información pueden originarse por una persona, cuando se formula la solicitud comienza la primera actividad del sistema. Esta actividad tiene tres partes:

   Aclaración de la solicitud. Antes de considerar cualquier investigación de sistemas, la solicitud de proyecto debe examinarse para determinar con precisión lo que el solicitante desea; ya que muchas solicitudes que provienen de empleados y usuarios no están formuladas de manera clara.

   Estudio de factibilidad. En la investigación preliminar un punto importante es determinar que el sistema solicitado sea factible. Existen tres aspectos relacionados con el estudio de factibilidad, que son realizados por lo general por analistas capacitados o directivos:
   - Factibilidad técnica.

   Estudia si el trabajo para el proyecto, puede desarrollarse con el software y el personal existente, y si en caso de necesitar nueva tecnología, cuales son las posibilidades de desarrollarla (no solo el hardware).
   - Factibilidad económica.

   Investiga si los costos se justifican con los beneficios que se obtienen, y si se ha invertido demasiado, como para no crear el sistema si se cree necesario.
   - Factibilidad operacional:

   Investiga si será utilizado el sistema, si los usuarios usaran el sistema, como para obtener beneficios.

   Aprobación de la solicitud. Algunas organizaciones reciben tantas solicitudes de sus empleados que sólo es posible atender unas cuantas. Sin embargo, aquellos proyectos que son deseables y factibles deben incorporarse en los planes. En algunos casos el desarrollo puede comenzar inmediatamente, aunque lo común es que los miembros del equipo de sistemas estén ocupados en otros proyectos. Cuando esto ocurre, la administración decide qué proyectos son los más importantes y el orden en que se llevarán a cabo.

   Después de aprobar la solicitud de un proyecto se estima su costo, el tiempo necesario para terminarlo y las necesidades de personal

2. **Determinación de los requisitos del sistema.** Los analistas, al trabajar con los empleados y administradores, deben estudiar los procesos de una empresa para dar respuesta a ciertas preguntas claves.

   Para contestar estas preguntas, el analista conversa con varias personas para reunir detalles relacionados con los procesos de la empresa. Cuando no es posible entrevistar, en forma personal a los miembros de grupos grandes dentro de la organización, se emplean cuestionarios para obtener esta información.

Las investigaciones detalladas requieren el estudio de manuales y reportes, la observación en condiciones reales de las actividades del trabajo y, en algunas ocasiones, muestras de formas y documentos con el fin de comprender el proceso en su totalidad.

Reunidos los detalles, los analistas estudian los datos sobre requerimientos con la finalidad de identificar las características que debe tener el nuevo sistema.

3. **Diseño del sistema. (Diseño lógico).** El diseño de un sistema de información responde a la forma en la que el sistema cumplirá con los requerimientos identificados durante la fase de análisis.

   Es común que los diseñadores hagan un esquema del formato o pantalla que esperan que aparezca cuando el sistema está terminado, se realiza en papel o en la pantalla de una terminal utilizando algunas de las herramientas automatizadas disponibles para el desarrollo de sistemas.

   También se indican los datos de entrada, los que serán calculados y los que deben ser almacenados. Los diseñadores seleccionan las estructuras de archivo y los dispositivos de almacenamiento. Los procedimientos que se escriben indican cómo procesar los datos y producir salidas.

   Los documentos que contienen las especificaciones de diseño representan a éste mediante diagramas, tablas y símbolos especiales.

   La información detallada del diseño se proporciona al equipo de programación para comenzar la fase de desarrollo de software.

   Los diseñadores son responsables de dar a los programadores las especificaciones de software completas y claramente delineadas.

4. **Desarrollo de software (diseño físico).** Los encargados de desarrollar software pueden instalar software comprado a terceros o escribir programas diseñados a la medida del solicitante. La elección depende del costo de cada alternativa, del tiempo disponible para escribir el software y de la disponibilidad de los programadores.

   Los programadores son responsables de la documentación de los programas y de explicar su codificación, esta documentación es esencial para probar el programa y hacer el mantenimiento.

5. **Prueba de sistemas.** Las pruebas se harán en un ambiente de pruebas, controlado y que no tiene conexión alguna con la información de producción, durante esta fase, el sistema se emplea de manera experimental para asegurarse que el software no tenga fallas, es decir, que funciona de acuerdo con las especificaciones y en la forma en que los usuarios esperan que lo haga. Se alimentan como entradas conjuntos de datos de prueba para su procesamiento y después se examinan los resultados. En ocasiones se permite que varios

usuarios utilicen el sistema, para que los analistas observen si tratan de emplearlo en formas no previstas, antes de que la organización implante el sistema y dependa de él.

Las pruebas son conducidas por personas ajenas al grupo que escribió los programas originales; para asegurarse de que las pruebas sean completas e imparciales y, por otra, que el software sea más confiable.

6. **Implantación y evaluación.** La implantación es el proceso de verificar e instalar nuevo equipo, entrenar a los usuarios, instalar la aplicación y construir todos los archivos de datos necesarios para utilizarla.

   Cada estrategia de implantación tiene sus méritos de acuerdo con la situación que se considere dentro de la empresa. Sin importar cuál sea la estrategia utilizada, los encargados de desarrollar el sistema procuran que el uso inicial del sistema se encuentre libre de problemas.

   Los sistemas de información deben mantenerse siempre al día, la implantación es un proceso de constante evolución.

   La evaluación de un sistema se lleva a cabo para identificar puntos débiles y fuertes. La evaluación ocurre a lo largo de cualquiera de las siguientes dimensiones:

   Evaluación operacional. Valoración de la forma en que funciona el sistema, incluyendo su facilidad de uso, tiempo de respuesta, lo adecuado de los formatos de información, confiabilidad global y nivel de utilización.

   Impacto organizacional. Identificación y medición de los beneficios para la organización en áreas como finanzas (costos, ingresos y ganancias), eficiencia operacional e impacto competitivo.
   - Opinión de los administradores

   Evaluación de las actitudes de directivos y administradores dentro de la organización así como de los usuarios finales.
   - Desempeño del desarrollo

   La evaluación del proceso de desarrollo de acuerdo con criterios tales como tiempo y esfuerzo de desarrollo, concuerdan con presupuestos y estándares, y otros criterios de administración de proyectos.

   Cuando la evaluación de sistema se conduce en forma adecuada proporciona mucha información que puede ayudar a mejorar la efectividad de los esfuerzos cuando la evaluación de sistemas se conduce en forma adecuada proporciona mucha información que puede ayudar a mejorar la efectividad de los esfuerzos de desarrollo de aplicaciones subsecuentes.

La importancia de las Contraseñas. Desde la Oficina Asesora de Planeación, gestión de Informática y con el fin de ser diligentes y transparentes con el manejo de la información y la aplicación de buenas prácticas les hacemos las siguientes sugerencias.

Las contraseñas son el punto de entrada a los recursos tecnológicos de información con que cuenta la Institución Universitaria. Proteger el acceso a nuestros recursos computacionales resulta esencial para asegurar que los sistemas y la información que contienen permanezcan segura, en este sentido debemos ser diligentes en resguardar el acceso a nuestros recursos y protegerlos de posibles amenazas a nuestra organización.

Sobre el manejo de las Contraseñas

- No pueden ser transmitidas verbalmente, escritas, enviadas por correo electrónico, sugeridas, o compartidas de cualquier otra forma conocida a personas distintas que no sean el responsable de dicha contraseña. Esto incluye jefaturas y personal asistente.
- Las contraseñas no pueden ser compartidas con la finalidad de "reemplazar" a alguien que se encuentra fuera de la oficina (con licencia médica, por ejemplo). Para tal caso se deben seguir los conductos regulares para solicitar una cuenta temporal con los permisos y acceso a recursos necesarios para que pueda realizar la labor de reemplazo.
- No hacerlas visibles en el escritorio.
- No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el número de teléfono.
- Al momento de levantarse de su puesto de trabajo, se recomienda dejar el equipo bloqueado.
- En el manejo de los usuarios y claves de acceso que le sean asignados para el ingreso a los distintos aplicativos son de su entera responsabilidad (esta información no debe prestarse.), es decir sus datos son personales e intransferibles usted es el único responsable de las acciones que se hagan con su usuario y contraseña.

ACTUALIZACION DE LAS POLÍTICAS DE USO Y MANEJO DE INFORMACIÓN. Es responsabilidad de la Oficina Asesora de Planeación área de TIC, liderar la actualización de las presentes políticas de acuerdo a las necesidades de la entidad y al avance tecnológico del medio, dicha actualización será por versiones para garantizarla vigencia de las mismas en el tiempo.

ARTÍCULO SEGUNDO. La presente resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Medellín, a los 14 de diciembre de 2015

Original Firmado
MAURICIO MORALES SALDARRIAGA
Rector

Proyectó: JJPA	Elaboró: Berta C.	Revisó: JPAG
Firma:	Firma:	Firma: