ALCANCE DE LAS POLÍTICAS

Las políticas definidas el presente documento aplican a toda la comunidad Universitaria de la Institución Universitaria Antonio José Camacho.

DEFINICIONES

Entiéndase para el presente documento los siguientes términos:

IES: Instituto de Educación Superior

Política: son instrucciones mandatorios que indican la intención de la alta gerencia respecto a la operación de la organización.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en si misma, sea o no protegida por reserva legal.

Criptografía de llave publica: es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Cifrar: quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama `descodificar" o `descifrar". Los sistemas de ciframiento se llaman sistemas criptográficos".

DESCRIPCIÓN DE LAS POLITICAS

POLITICA 1: ACCESO A LA INFORMACIÓN

Todos los funcionarios públicos, contratistas, IES, que laboran para la Institución Universitaria Antonio José Camacho deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la Institución Universitaria Antonio José Camacho, Los jefes de cada proceso responsables de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Entidad.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

POLITICA 2: ADMINISTRACION DE CAMBIOS

Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazar la solicitud.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por la Institución Universitaria Antonio José Camacho, de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

POLITICA 3: SEGURIDAD DE LA INFORMACION

Los funcionarios públicos, contratistas, IES y pasantes de la Institución Universitaria Antonio José Camacho son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios públicos, contratistas, IES y pasantes no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

POLITICA 4: SEGURIDAD PARA LOS SERVICIOS INFORMATICOS

El sistema de correo electrónico, grupos de charla y utilidades asociadas de la entidad debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas y pasantes.

La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, el funcionario o contratista autorizará a la entidad para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

Los funcionarios públicos, contratistas IES y pasantes que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

En cualquier momento que un trabajador publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de

información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la entidad.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la oficina de Servicios informáticos, no utilizar el computador y desconectarlo de la red.

El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información. Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de "no repudio".

POLITICA 5: SEGURIDAD EN RECURSOS INFORMATICOS

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el Administración de usuarios.

Plan de auditoria: Hace referencia a las pistas o registros de los sucesos relativos a la operación.

Las puertas traseras: Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptar la existencia de las mismas en la mayoría de los sistemas operacionales, bases de datos, aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.

El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos , contratistas IES, y pasantes de la Institución Universitaria Antonio José Camacho son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a el.

Antes de que un nuevo sistema se desarrolle o se adquiera, los jefes de oficina, en conjunto con el Director de la oficina de servicios informáticos, deberán definir las especificaciones y requerimientos de seguridad necesarios.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

POLITICA 6: SEGURIDAD EN COMUNICACIONES

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información confidencial.

Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documento de formalización.

POLITICA 7: SOFTWARE UTILIZADO

Todo software que utilice la Institución Universitaria Antonio José Camacho será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Todo el software de manejo de datos que utilice la Institución Universitaria Antonio José Camacho dentro de su infraestructura informática, deberá contar con las técnicas más avanzadas de la industria para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios públicos, contratistas IES, y pasantes de las implicaciones que tiene el instalar software ilegal en los computadores de la Institución Universitaria Antonio José Camacho.

Existirá un inventario de las licencias de software de la Institución Universitaria Antonio José Camacho que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

La programación del mantenimiento preventivo está a cargo del coordinador de infraestructura, este se programa una vez por semestre tanto para la comunidad académica (final de semestre), como para la comunidad administrativa (después de la 5 semana de iniciado el semestre).

En el caso del mantenimiento correctivo, este es informado por la comunidad en general al coordinador de infraestructura y es él quien lo programa.

La ejecución de estos mantenimientos la realiza los auxiliares de laboratorio, bajo la supervisión del coordinador de infraestructura quien revisa los servicios atendidos y lleva un control de indicadores de servicio.

Las personas encargadas de la instalación del hardware y del software son los auxiliares de laboratorio, bajo la supervisión del coordinador de infraestructura; estos equipos en el caso de ser para el área administrativa se le entrega al usuario final y se capacita si es necesario en el uso del mismo. Para el caso del área académica se ubican en el espacio designado para estos.

El mantenimiento preventivo y correctivo deberá ser realizado por los auxiliares de laboratorio de sistemas, de acuerdo a la programación del plan de mantenimiento, cuando se requieren solicitar garantía de equipos se gestiona directamente con el proveedor, en caso de necesitarse repuestos o cambios en elementos de hardware estos se gestionan a través del proceso de planeación tecnológica como compras directas.

En casos de que, como parte componente de contratos de adquisición de bienes y/o servicios, se incluyan equipos informáticos, como parte complementaria de otro tipo de equipos, o como parte componente de servicios contratados, se deberá contar previa a la contratación, con un informe favorable de la Oficina de Servicios informáticos en lo referente a activos informáticos y de comunicaciones, con el fin de que cumplan con los estándares tecnológicos para la Institución, vigilando, particularmente su compatibilidad con la infraestructura instalada y su posibilidad de mantenimiento y

soporte técnico por parte de los fabricantes o de los distribuidores autorizados de la marca en el país.

El soporte técnico en sitio de activos informáticos y de comunicaciones que no tienen garantía vigente por el fabricante, será brindado por el personal de apoyo de la Oficina de Servicios Informáticos.

Los activos informáticos de misión crítica (servidores, equipos de comunicación, etc.) deberán estar ubicados en áreas que cumplan con los requerimientos de seguridad física, condiciones ambientales (aire acondicionado, control de humedad, etc.) apropiados, alimentación eléctrica controlada y regulada, servicio de energía eléctrica ininterrumpida.

La Oficina de Servicios Informáticos tiene la responsabilidad de controlar y llevar un inventario detallado de la infraestructura de hardware de los activos de la Institución. La persona encargada de ingresar los equipos de computo al formato de control de inventario de hardware son lo auxiliares de laboratorio, bajo la supervisión del coordinador de infraestructura; estos obtienen un inventario detallado de cada computador tanto de software como de hardware por medio de un software freeware llamado AIDA32.

La Oficina de Servicios Informáticos llevará un inventario detallado del software instalado en la infraestructura de hardware de la Institución. Este control se llevará tanto para la infraestructura centralizada administrativa como para equipos de laboratorio de microinformática.

Los activos informáticos corporativos y centralizados serán custodiados por la Oficina de Servicios Informáticos En los casos que se requiera equipos especializados de servicio de telecomunicaciones. Serán custodiados por la misma área encargada de su operación.

Los Custodios deberán ser funcionarios nombrados de la universidad, a quienes se asignan los activos informáticos y son responsables pecuniariamente de su buen uso e integridad. Los usuarios son quienes utilizan para su labor diaria o eventual el activo informático y pueden ser empleados regulares de la empresa o no (empleados de outsourcing, contratistas externos, consultores, etc.)

La asignación de equipos informáticos a Custodios/Usuarios la hace la Oficina de Servicios Informáticos en base a los requerimientos que reciba de las otras áreas de la Universidad.

Todo el Software instalado en la Institución Universitaria Antonio José Camacho, deberá estar legalmente licenciado. No se permitirá la instalación de software que no cuente con la respectiva licencia de uso.

La custodia y almacenamiento de todos los medios que contengan componentes de software se hará en la Oficina de Servicios Informáticos bajo la custodia del coordinador de infraestructura. Solamente en casos debidamente justificados se podría permitir que copias de los medios se entreguen y estén en custodia de los usuarios finales.

La Oficina de Servicios Informáticos, deberá propender a realizar contratos de licenciamiento de software a nivel corporativo, obteniendo las mejores condiciones económicas para la Institución. Salvo casos emergentes debidamente justificados lo deba realizar un área en particular, siempre y cuando las adquisiciones estén contemplados en el plan operativo y presupuesto, y cumplan la normativa y estándares establecidos por la Oficina de Servicios Informáticos.

Las licencias de los software adquiridos al igual que los medios de instalación son archivados y están bajo la custodia del coordinador de infraestructura. El licenciamiento de Software está regido por las leyes de propiedad intelectual antes mencionadas.

La Administración y Fiscalización de Contratos deberán seguir las normas establecidas por la universidad, logrando que todos los contratos se cumplan en los plazos definidos y bajo las especificaciones técnicas contratadas. Esta labor está a cargo del director de Oficina de Servicios Informáticos

Se verifica por parte del coordinador de infraestructura que se realicen los trabajos de acuerdo a la programación y que se hagan las respectivas entregas a conformidad del usuario final.