Institución Universitaria

www.itm.edu.co

RESOLUCIÓN 0000478

06 JUN 2014

Por medio de la cual se adoptan las Políticas de Seguridad de la información institucional.

LA RECTORA DEL INSTITUTO TECNOLÓGICO METROPOLITANO, Institución Universitaria –ITM-, en uso de sus atribuciones legales, estatutarias, y

CONSIDERANDO

- Que la resolución 831 del 10 de septiembre de 2012 reglamentó el uso de todos los recursos informáticos.
- Que el ITM suministra para uso académico, funciones institucionales o para cumplir con productos establecidos en los contratos de prestación de servicios, las herramientas o aplicaciones informáticas necesarias.
- Que todos los usuarios de la plataforma tecnológica son responsables de la información que en ésta se manipula y que el uso de los Recursos Informáticos debe responder estrictamente a necesidades institucionales.
- Que es necesario asignar responsabilidades en el uso de la información institucional.
- Que es necesario propender por el cumplimiento de los cuatro pilares de la seguridad informática: Disponibilidad, Confidencialidad, Integralidad y No repudio.
- Que para el correcto y adecuado manejo de la información, es necesario definir las políticas de seguridad de información institucional.

RESUELVE

Artículo 1°. Adoptar en el ITM las Políticas contempladas en el documento **"Políticas de Seguridad de la Información"**.

Parágrafo 1. El Departamento de Sistemas dará a conocer a todo el personal administrativo y académico dichas políticas y suministrará el soporte y acompañamiento necesario para el adecuado cumplimiento de las mismas.

Artículo 2°. El incumplimiento de lo dispuesto en la presente resolución, podrá dar origen a las sanciones administrativas y disciplinarias a que haya lugar.

Artículo 3°. La presente Resolución rige a partir de la fecha de expedición y deroga todas las disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dada en Medellín 06 JUN 2014

LUZ MARIELA SORZA ZAPATA
Rectora

Políticas de *Seguridad de la Información*

ALCANCE

Las Políticas de Seguridad de la Información para el Instituto Tecnológico Metropolitano presentan las orientaciones generales para implementar un modelo de seguridad de la información confiable y flexible; define el marco básico de cualquier norma, proceso, procedimiento, estándar y/o acción, relacionados con el manejo de la seguridad de la información.

Éstas políticas aplican para todos los niveles de la Institución: Empleados, Docentes, Estudiantes, Egresados, Terceros, proveedores, que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación. Adicionalmente las presentes políticas aplican para toda la información creada, procesada o utilizada como soporte a las actividades académicas y administrativas, cualquiera sea el medio, formato, presentación o lugar en el cual se encuentre.

Las Políticas de Seguridad de la Información del Instituto Tecnológico Metropolitano, son una serie de mejores prácticas para el manejo de la información generada y trasmitida en la Institución, para la cual la información es considerada uno de sus activos más importantes.

OBJETIVO GENERAL

Brindar orientaciones generales en cuanto al manejo de la información generada en el Instituto Tecnológico Metropolitano, con el fin de prevenir cualquier alteración o acceso no autorizado a la información, buscando que ésta sea accedida solamente por su dueño y que esté siempre disponible cuando la requiera.

OBJETIVOS ESPECÍFICOS

- Orientar a las personas vinculadas con el ITM, sobre el uso de la información generada en la Institución.
- Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos tecnológicos suministrados por la Institución para el normal desarrollo de sus actividades académicas y administrativas.
- Establecer y comunicar la responsabilidad en el uso de los activos de información
- Establecer los canales de comunicación que le permitan a la Rectoría y a la Vicerrectoría General mantenerse informados de los riesgos y uso inadecuado de los activos de información, así como las acciones tomadas para su mitigación y corrección.
- Mantener el buen nombre del Instituto Tecnológico Metropolitano.

Manejo

LINEAMIENTOS

- La información de la Institución y de los clientes es un activo muy importante para el Instituto, por lo tanto debe ser protegida permanentemente garantizando su disponibilidad y confidencialidad.

- Cada dependencia y persona, tendrá un espacio en los servidores del Instituto Tecnológico Metropolitano donde debe guardar periódicamente la información generada en los equipos que fueron dispuestos para sus funciones.

- Se debe hacer una correcta evaluación de los riesgos a los que está expuesta la información para identificarlos, evaluarlos y mitigarlos.

- Toda persona vinculada el Instituto Tecnológico Metropolitano que utilice remotamente recursos de información del Instituto deberá acogerse a estas políticas

- La información del Instituto Tecnológico Metropolitano será utilizada únicamente para los fines que fue obtenida.

- Toda área física del Instituto Tecnológico Metropolitano debe contar con un nivel de seguridad acorde con el valor y la privacidad de la información que se procesa y administra en ella.

- Cada empleado de la Institución, debe suministrar la información propia de su cargo a quien sea necesario, en caso de un traslado o desvinculación de la misma.

- El Instituto Tecnológico Metropolitano debe vigilar el cumplimiento de la presente política y cuando exista una violación, informarla de inmediato al Jefe del Departamento de Sistemas.

EXCEPCIONES A LA POLÍTICA

No se aceptan excepciones a la definición de la política de Seguridad de la Información.

POLÍTICA:

Uso y Gestión de usuarios y contraseñas.

ALCANCE

La primera línea de protección en el acceso a los recursos informáticos es la contraseña. Es de vital importancia seleccionar una adecuada, que cumpla con las características mínimas de seguridad, una contraseña mal elegida puede ser la puerta de entrada de una persona externa al Instituto Tecnológico Metropolitano, razón por la cual es responsabilidad de todos los empleados velar por las seguridad de éstas, apoyados en las recomendaciones que da la presente política.

El solo hecho de tener una contraseña segura no garantiza su seguridad, ésta depende de que se mantenga en secreto, las directrices emitidas con esta política buscan mantener la confidencialidad de la contraseña.

El ámbito de esta política incluye a todos aquellos usuarios de los servicios y recursos informáticos de la Institución que tienen o son responsables de una cuenta de usuario o cualquier otro tipo de acceso que requiera una contraseña en cualquiera de los sistemas de la Institución.

OBJETIVO GENERAL

El objetivo fundamental de esta política es establecer un estándar para la creación de contraseñas seguras, la protección de dichas contraseñas, y el cambio frecuente de las mismas.

OBJETIVOS ESPECÍFICOS

- Brindar orientaciones generales sobre cómo crear una contraseña segura.
- Dar recomendaciones en la forma cómo se debe proteger las contraseñas y la frecuencia de cambio de las mismas.

LINEAMIENTOS

- Todas las contraseñas de sistema (root, administradores de servidores, cuentas de administración de aplicaciones, etc.) deben ser cambiados al menos una vez cada seis meses.

- Todas las contraseñas de usuario (cuentas de usuarios del dominio, cuentas de email, cuentas de servicios web, etc.) deben ser cambiadas al menos una vez cada seis meses.

- Las contraseñas no deben ser incluidas en mensajes de correo electrónico, chat o ningún otro medio de comunicación electrónico o escrito.

- Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.

- Las contraseñas serán generadas con las recomendaciones de esta política y se les comunicará a los usuarios su contraseña siempre en estado "Cambio en el próximo inicio de sesión" para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta o servicio.

- No se deben usar contraseñas completamente numéricas con algún significado (teléfono, fecha de nacimiento, patente del automóvil, etc.).

- Se debe elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas), numéricos y caracteres especiales (/ * @ etc).

- Deben contener como mínimo 8 caracteres con las combinaciones descritas anteriormente.

- La protección de la contraseña recae tanto sobre el administrador del sistema como sobre el usuario. Al comprometer una cuenta se puede estar comprometiendo todo el sistema.

- Por ninguna razón la contraseña debe compartirse con otro usuario

- No se permite ninguna cuenta sin contraseña.

- No se mantienen contraseñas por defecto de ningún sistema de información o telecomunicaciones.

- No se debe teclear la contraseña en presencia de otras personas. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.

- El sistema restringirá a 3 el uso de contraseñas repetidas, es decir, cuando se solicite cambio de contraseña, no se podrán utilizar las 3 últimas usadas.

RECOMENDACIONES

- Se recomienda cambiar la contraseña con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su contraseña pueda haber sido comprometida.

- Cree una sigla con una información que sea fácil de recordar. Por ejemplo, elija una frase que tenga significado para usted, como Mi hijo nació el 12 de diciembre de 2004. Con esa frase como guía, puede usar Mhne12/Dic,4 como contraseña

- Combinar palabras cortas con algún número o carácter de puntuación: toy5_yo4.

- Relacione la contraseña con un pasatiempo o deporte favorito. Por ejemplo, Me encanta el bádminton puede transformarse en Mn'kant6ehlB@dm1nt()n.

- Crear una frase no conocida: L a S emana P asada S e P erdio U n G ato -> LaSePasePeuGa

- Elegir una palabra sin sentido, aunque pronunciable: TorcanCi30, AloCatiJ, Wen2Mar0

- No utilice la característica de "Recordar Contraseña" existente en algunas aplicaciones (Outlook, Firefox, Chrome, Internet Explorer).

- Si alguien le pide la contraseña, refiérale a este documento o pídale que se comunique con el Departamento de Sistemas del Instituto Tecnológico Metropolitano.

- Si sospecha que una cuenta o su contraseña pueden haber sido comprometidas, cámbiela inmediatamente o comuníquese con el Departamento de Sistemas del Instituto Tecnológico Metropolitano.

EXCEPCIONES A LA POLÍTICA

No se aceptan excepciones a la definición de la política de Seguridad de la Información.

Manejo

POLITICA:

Uso de Internet, correo electrónico y mensajería instantánea.

ALCANCE

Los servicios telemáticos son una gran necesidad hoy en día, el Internet, correo electrónico y mensajería instantánea son unas de las herramientas más utilizadas, ya que acortan caminos y brindan un acceso a la información y a las personas, además ayuda a las instituciones a proyectarse en el medio. Internet es una excelente herramienta para mejorar la operatividad de todo negocio, crear nuevos productos o servicios, abrir nuevos mercados, y en definitiva, mejorar los procesos de comunicación empresarial. Pero como tal, es un medio que como puede ayudar a proyectar un negocio, puede llevar a las personas a incurrir en el desaprovechamiento de tiempo y recursos, lo que implica que se deben implementar controles que propicien un mejor uso de esta tecnología.

OBJETIVO GENERAL

Brindar orientaciones generales sobre lo que se puede o no hacer en Internet con los recursos que entrega el Instituto Tecnológico Metropolitano a sus empleados.

OBJETIVOS ESPECIFICOS

- Directrices sobre los sitios permitidos o no permitidos durante la jornada laboral.
- Directrices sobre la utilización del correo electrónico.
- Directrices sobre la utilización de la mensajería instantánea.

LINEAMIENTOS

- El uso de la información electrónica contenida en la mensajería debe cumplir con las políticas de seguridad de la información. Por lo anterior los usuarios de los servicios de mensajería electrónica son los responsables del contenido de las comunicaciones enviadas y recibidas.

- Está prohibida la suplantación, el enmascaramiento o la firma de otro usuario en el uso de cualquier recurso de información.

- Está prohibida la replicación de mensajes que son exclusivos para una persona en particular o de advertencias públicas hacia otros usuarios.

- Está prohibido el envío de mensajes cadena, pornografía, mensajes no solicitados, y bromas.

- Se deberá tener en cuenta y dar cumplimiento a los lineamientos emitidos en la resolución rectoral 831 del 10 de septiembre de 2012, por medio de la cual se reglamenta el uso corporativo de los servicios de correo electrónico, Internet y de telefonía en el Instituto Tecnológico Metropolitano y se asignan responsabilidades en su administración, así como la adquisición, seguridad y uso de todos los Recursos Informáticos.

- El Instituto cuenta y deberá asegurar la permanencia de un sistema de protección perimetral, que proteja la navegación en Internet y los mensajes de correo electrónico entrantes y salientes, contra virus, malware, spam y otros medios de ataque a los sistemas de cómputo y de información.

EXCEPCIONES A LA POLÍTICA

- Las contempladas en la Resolución Rectoral 831 del 10 de septiembre de 2012

POLITICA:

Uso de los recursos tecnológicos provistos por la Institución

ALCANCE

Los equipos de cómputo y recursos de información, son de vital importancia para la operacionalización de los diferentes procesos de la Institución. El Instituto dentro de sus políticas de inversión, se ha propuesto entregar los mejores recursos a sus empleados, estudiantes y docentes, para ayudar a que sus funciones y procesos sean llevados a cabo eficientemente y eficazmente. Esto implica además, controles para que su utilización sea acorde a las necesidades y políticas anteriormente descritas.

OBJETIVO GENERAL

Brindar orientaciones generales sobre la utilización de los recursos de cómputo y de información, para lograr su máximo aprovechamiento y cuidar el buen nombre de la Institución.

OBJETIVOS ESPECIFICOS

- Directrices sobre la utilización de los equipos de cómputo, y sistemas de información.
- Orientaciones sobre lo que se debe o no instalar en los equipos de cómputo
- Indicaciones sobre los traslados de equipos y su instalación.

LINEAMIENTOS

- Los recursos de cómputo y de información son provistos a sus empleados y proveedores para el uso exclusivo del Instituto Tecnológico Metropolitano.

- La propiedad intelectual sobre patentes, derechos de autor, invenciones o Información, permanecerá en el Instituto Tecnológico Metropolitano, de igual forma, el Instituto respetará los derechos de autor y licencias de uso, para lo cual solamente software aprobado, probado y autorizado por el Departamento de Sistemas debe ser instalado en los equipos y sistemas de la Institución.

- El área de soporte técnico será la encargada de instalar o desinstalar software, y de revisar periódicamente el software instalado en los equipos de cómputo, y reportar el software instalado no autorizado al jefe del Departamento de Sistemas.

- Todo equipo de cómputo o de comunicaciones, debe ser reportado al Departamento de Sistemas para su respectivo registro de inventario y adecuación física y lógica.

- Con el fin de cuidar el buen nombre de la Institución, y siendo respetuosos de las leyes sobre derechos de autor y demás temas legales y de licenciamiento, se prohíbe la instalación y la utilización de software ilegal o no licenciado.

- No se permite la utilización de los recursos de cómputo o información dispuestos por el Instituto, para trabajos o asuntos personales.

- Se prohíbe copiar por la red Institucional y almacenar información personal en los servidores tales como música, videos, fotos, documentos entre otros.

EXCEPCIONES A LA POLÍTICA

No se aceptan excepciones a la definición de la política de Seguridad de la Información.