



Pontificia Universidad Católica del Ecuador

Oficina de Seguridad de la Información

E-MAIL:
lapazmino@puce.edu.ec
Av. 12 de Octubre 1076 y Roca
Apartado postal 17-01-2184
Telf: 593 – 2 – 299 15 10
Quito - Ecuador

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR VICERRECTORADO OFICINA DE SEGURIDAD DE LA INFORMACIÓN	
POLÍTICA DETALLADA DE USUARIO FINAL PARA LA SEGURIDAD DE LA INFORMACIÓN	
OSI-PDUF	VERSIÓN: 1.0: Aprobada
Marzo de 2011	VIGENCIA: Desde fecha de divulgación

1.- Objetivo

El objetivo de la presente política es alcanzar un grado aceptable y sostenido de seguridad de los computadores personales, de la información almacenada en ellos y el uso de los servicios de correo electrónico e Internet, en función del perfil de riesgos tecnológicos y las vulnerabilidades, para lo cual se requiere normar los aspectos relacionados con las seguridades físicas y lógicas que deben precautelar los usuarios finales de los equipos, servicios y aplicaciones tecnológicas.

En particular, se proporciona una guía a los usuarios para la utilización segura, eficiente y efectiva de los computadores personales, y de los servicios de correo electrónico e Internet, con el fin de racionalizar y optimizar el uso de dichos recursos y servicios y asegurar una mayor calidad en el desarrollo de las funciones.

2.- Políticas Macro Relacionadas

- Política General de Seguridad de la Información: OSI-PGSI

3.- Audiencia

Pontificia Universidad Católica del Ecuador.- personal docente y administrativo que tenga un computador personal portátil o de escritorio de dotación oficial y los servicios de aplicaciones, correo electrónico y acceso a Internet.

OSI – Política de usuario final

Incluyen los personales y los del equipamiento docente?

.Página 1 de 6



Pontificia Universidad Católica del Ecuador

Oficina de Seguridad de la Información

E-MAIL:
lapazmino@puce.edu.ec
Av. 12 de Octubre 1076 y Roca
Apartado postal 17-01-2184
Telf: 593 – 2 – 299 15 10
Quito - Ecuador

4.- Detalle

4.1 Seguridades lógicas

4.1.1 De las contraseñas de usuario

La contraseña es uno de los medios más utilizados en tecnología informática para garantizar que solamente personal autorizado, de acuerdo con sus perfiles y roles, tenga acceso a la información. La política de contraseñas se basa en que éstas sean de carácter personal, se mantengan en secreto y por lo tanto sean intransferibles, por ello:

- a) Se prohíbe a los usuarios dar a conocer a terceras personas su contraseña, quien así lo hiciere debe tomar en cuenta que sigue siendo el único responsable de las actividades que se realicen con su identificación de usuario (ID) y contraseña;
- b) El usuario debe asegurarse que al digitar su contraseña no esté siendo observado por ninguna persona;
- c) En caso de que el usuario sospeche que su contraseña ha sido comprometida deberá solicitar a la Dirección de Informática (DI) inmediatamente su cambio;
- d) En caso de olvido o bloqueo de su contraseña, el usuario deberá coordinar el restablecimiento de la misma con la Unidad de Soporte al Usuario de la DI;
- e) Se debe cambiar la contraseña en un período definido de acuerdo con la criticidad y la sensibilidad de la información a la que se tiene acceso. La DI deberá dar las facilidades para ello a través de las aplicaciones y los servicios. **Al cambiar la contraseña no se podrá utilizar una ya utilizada en al menos tres períodos anteriores.**
- f) No se deben utilizar contraseñas que resulten obvias, fáciles de adivinar o descubrir, o predecibles para un atacante: (el mismo identificador de usuario, palabras de diccionario, fechas o nombres de personas allegadas, secuencias de números repetidos o consecutivos). Para que las contraseñas cumplan con su función de seguridad de la información, en aplicaciones que manejen información crítica, deberán tener una longitud mínima de 8 caracteres, de entre los cuales debe incluir letras mayúsculas y minúsculas, mínimo 2 números o símbolos;
- g) No se debe escribir ni registrar en medio alguno la contraseña y dejarla en sitios fácilmente accesibles.

Como se controla esto?

4.2 Prevención de virus y otros programas que causan daños

Los usuarios deben evitar cualquier actividad que comprometa la seguridad de la información en sus computadores personales en cuanto a la introducción de virus u otros programas maliciosos, para ello:



Pontificia Universidad Católica del Ecuador

Oficina de Seguridad de la Información

E-MAIL:
lapazmino@puce.edu.ec
Av. 12 de Octubre 1076 y Roca
Apartado postal 17-01-2184
Telf: 593 – 2 – 299 15 10
Quito - Ecuador

Capacitación?

- a) Se prohíbe introducir en los computadores personales cualquier tipo de medio de almacenamiento sin que previamente haya sido revisado para descartar la presencia de virus o cualquier otro programa dañino;
- b) Se prohíbe conectar en la red universitaria cualquier equipo de computación sin la autorización y revisión previa de la DI.
- c) Se prohíbe grabar en los dispositivos de almacenamiento de los equipos de computación personales cualquier tipo de archivo de dudosa condición o calidad que pueda ocasionar daños. Esto aplica a archivos procedentes de Internet o introducidos al PC por medio de almacenamientos extraíbles como “flash memories” o de cualquier otra índole acerca de los cuales no se tenga la certeza de que están libres de cualquier código malicioso;
- d) El usuario está en la obligación de comprobar que su equipo de computación dispone del software antivirus actualizado, en caso contrario, o en caso de duda, deberá acudir a la Unidad de Soporte a Usuarios de la DI para su inmediata actualización;
- e) El usuario deberá abstenerse de abrir o reenviar mensajes de correo electrónico que no provengan de fuentes conocidas y seguras, y de descargar anexos enviados por correo electrónico que puedan ser fuente de virus o similares o cuya procedencia y características desconozca;
- f) En caso de evidenciar la presencia de virus o similares en su equipo de computación, el usuario debe de inmediato terminar la ejecución de los programas que al momento esté utilizando, apagar el computador y notificar a la unidad de Soporte al Usuario de la DI.

4.3 Acerca del uso de Internet, correo electrónico y servicios relacionados

El Internet y sus servicios relacionados se han convertido en herramientas indispensables en las actividades de cualquier organización, no obstante, su utilización requiere estrictos controles para evitar riesgos ocasionados por su inadecuada utilización, por ello:

4.3.1 Acerca de Internet

- a) La utilización de Internet debe ser solamente para asuntos relacionados con las funciones de trabajo en la PUCE;
- b) Se prohíbe la utilización en horas laborables de sistemas públicos de correo electrónico como por ejemplo los provistos por Microsoft, Google, Yahoo, etc. La utilización de estos servicios en horarios extra - laborables está sujeta a la autorización de las altas autoridades institucionales;
- c) Se prohíbe a los usuarios suscribirse a foros de discusión, u otras agrupaciones ofrecidas por Internet ajenas a las funciones institucionales con la utilización de la cuenta de correo provista por la PUCE;
- d) Se prohíbe la utilización del servicio de Internet para establecer cualquier tipo de conexión no autorizada, o descargar o enviar por medio de la red cualquier tipo de información, programa o archivo magnético que no esté autorizado para el desarrollo de las funciones propias en la PUCE;



Pontificia Universidad Católica del Ecuador

Oficina de Seguridad de la Información

E-MAIL:
lapazmino@puce.edu.ec
Av. 12 de Octubre 1076 y Roca
Apartado postal 17-01-2184
Telf: 593 – 2 – 299 15 10
Quito - Ecuador

- e) Se prohíbe y se restringe por política implementada para el efecto, la navegación por sitios de Internet relacionados con temas tales como **sexo, racismo, guerra, violencia, fundamentalismo**, diversión, entretenimiento y en general sitios ajenos por completo a las actividades de los funcionarios de la PUCE. Sin atentar contra la privacidad de los funcionarios, la DI se reserva el derecho de reportar a la unidad competente la utilización de los recursos de la universidad en asuntos que evidentemente estén lejanos a las funciones propias. Si un usuario requiere para sus funciones acceso a un sitio restringido por la política, debe solicitarlo a través de su jefe inmediato a la DI;
- f) Se prohíbe la conexión a Internet dentro de la red institucional por medios y canales diferentes a los dedicados para el efecto por la DI, por lo tanto no se podrán establecer conexiones “dial – up” (a través de las líneas telefónicas) o conexiones inalámbricas no autorizadas;

y si es por educación

4.3.2 Acerca del correo electrónico

- a) Las cuentas de correo electrónico del personal docente y administrativo de la PUCE provistas por medio de la DI son solamente para uso en las funciones institucionales;
- b) Los usuarios del servicio de correo electrónico deben abstenerse de enviar por este medio información confidencial, privada, reservada, a menos que existan evidentes garantías y autorización para ello;
- c) En razón de que el correo electrónico es utilizado institucionalmente como medio de comunicación, es obligatorio para todos los usuarios mantenerse en línea diariamente y revisar su cuenta de correo institucional en los días y horas laborables para recibir, disposiciones o pedidos que deba atender y responder;
- d) Cada usuario es totalmente responsable de la utilización de su cuenta de correo electrónico, por lo cual, como se estipula en la política de contraseñas, éstas deben mantenerse estrictamente secretas;
- e) Se prohíbe enviar correos masivos para asuntos de índole personal a las cuentas individuales de la PUCE o, en general, a cualesquiera otras cuentas;
- f) El envío o recepción de archivos adjuntos a los mensajes de correo electrónico está restringido por política implementada para el efecto de evitar ataques de virus u otros códigos maliciosos;
- g) El usuario no debe abrir ni enviar o reenviar correo no deseado (“spam”) ni cadenas ni ningún otro mensaje que no esté relacionado con el normal ejercicio de sus funciones en la PUCE;
- h) Cada usuario del correo electrónico debe mantenerse dentro de límite máximo de almacenamiento de mensajes y anexos válidos, siendo de su responsabilidad borrar o descargar elementos innecesarios que puedan afectar su servicio por excesos. La capacidad de almacenamiento del buzón de correo para cada usuario es de 30 MB, y se revisará cuando sea pertinente;
- i) Es deber de cada usuario mantener periódicamente en su PC respaldo tanto de los mensajes como de los anexos de correo electrónico que pueda requerir en el futuro en el



Pontificia Universidad Católica del Ecuador

Oficina de Seguridad de la Información

E-MAIL:
lapazmino@puce.edu.ec
Av. 12 de Octubre 1076 y Roca
Apartado postal 17-01-2184
Telf: 593 – 2 – 299 15 10
Quito - Ecuador

desarrollo de sus actividades, en razón de que estos son borrados periódicamente del servidor.

5 De las seguridades físicas y uso de computadores personales

5.1 De los computadores personales portátiles y de escritorio

Los computadores personales dotados por la PUCE al personal docente y administrativo para el desempeño de sus actividades son un importante activo de información institucional, cuyo valor intrínseco es alto, y se incrementa si se considera que allí se guarda información que puede ser clasificada. Por ello cada funcionario debe tomar una serie de precauciones para precautelar la integridad tanto del computador como de la información y programas en él contenidos, por ello:

- a) El computador personal portátil o de escritorio es para uso exclusivo en las actividades propias de las labores desarrollada en ejercicio de las funciones en la PUCE, por lo que está prohibido almacenar o procesar información ajena a dichas funciones. La información y programas almacenados en los computadores personales son de propiedad de la Universidad;
- b) En caso de pérdida del computador personal, se debe reportar de inmediato a la DI;
- c) Los computadores portátiles y sus accesorios, una vez terminadas las actividades propias de las funciones debe ser apagado guardado con todas las seguridades que prevengan su pérdida o daño. Deben ser guardados bajo llave en un sitio libre de humedad, exceso de calor u otros factores ambientales o no que puedan afectarlos;
- d) Los computadores de escritorio deben ser apagados una vez terminada la jornada de trabajo y dejar la oficina con las debidas seguridades de accesos;
- e) Durante el transporte se deben tomar todas las precauciones para evitar que los computadores portátiles sufran golpes o caídas, sean sustraídos o utilizados por terceras personas;
- f) Cada usuario es responsable de coordinar, de acuerdo con las instrucciones que para el efecto da la Unidad de Soporte a Usuarios de la DI, las actividades relacionadas con el mantenimiento preventivo y correctivo de los PC's y de actividades de instalación o actualización de software básico, parches o software de seguridad, aplicaciones, respaldos, etc.;
- g) Para efectos de proteger la información y los programas almacenados en el PC, los usuarios deben propender a la utilización de contraseña de encendido y de red, así como de protectores de pantalla con clave que impiden que personas no autorizadas accedan a la información almacenada. La DI deberá dar la capacitación necesaria para la utilización de las funciones de seguridad;
- h) Todas las contraseñas que utilice el funcionario en la operación del PC y sus servicios y aplicaciones deberán ser puestas en conocimiento de su jefe inmediato con las debidas seguridades y en la forma que se determine para el efecto, para ser utilizadas solamente en casos de necesidad institucional certificada por el titular del área;



Pontificia Universidad Católica del Ecuador

Oficina de Seguridad de la Información

E-MAIL:
lapazmino@puce.edu.ec
Av. 12 de Octubre 1076 y Roca
Apartado postal 17-01-2184
Telf: 593 – 2 – 299 15 10
Quito - Ecuador

- i) Cada usuario es responsable por la información almacenada en su computador personal y por lo tanto está en la obligación de realizar periódicamente respaldos de dicha información. La periodicidad estará en función de la criticidad de los datos almacenados y de las vulnerabilidades;
- j) Se prohíbe realizar cualquier cambio a la configuración física interna del computador personal, esto es extraer o colocar módulos de memoria, tarjetas, puertos, procesadores, unidades internas de almacenamiento, y en general cualquier cambio que altere en aumento o disminución los componentes físicos del computador personal;
- k) Se prohíbe realizar cualquier cambio a la configuración lógica del computador personal, esto es, **instalar o desinstalar software o componentes de software básico**, de seguridades o aplicativo; configurar o des configurar servicios, o cualquier otra actividad que altere la configuración lógica del computador personal. Estas actividades deben realizarse exclusivamente en coordinación y bajo la revisión de la Unidad de Soporte al Usuario de la DI;
- l) En caso de fallas o malfuncionamiento de los componentes de hardware o de software del computador personal, el usuario deberá acudir a la Unidad de Soporte al Usuario de la DI, única autorizada para revisar el equipo y corregir las fallas o remitirlo al proveedor en ejercicio de la garantía si está vigente;
- m) Los usuarios de computadores portátiles que deban conectarlos a redes diferentes a la red institucional, deben tomar las precauciones para evitar ataques de virus u otros códigos malignos. En caso de duda, antes de volver a conectar el computador en la red institucional, es necesario que acuda a la Unidad de Soporte al Usuario de la DI para verificación del equipo;
- n) El funcionario en uso de licencia por vacaciones, enfermedad o por asuntos personales, deberá entregar para su resguardo el computador personal portátil a su jefe inmediato, si este así lo requiere.