POLÍTICA DE USO DE CREDENCIALES DE USUARIO

Este documento contiene el detalle de las políticas establecidas para el uso adecuado de credenciales de usuario.

Av. Jorge Guzmán Rueda y Av. Aurelio
Espinosa Pólit, Cdla "La Victoria"
Apartado postal: 100112
Telf.: (+593) 06 2615 500 / 2615 453
Ibarra– Ecuador www.pucesi.edu.ec

Información del Documento

TÍTULO:	POLÍTICAS DE USO DE CREDENCIALES DE USUARIO
SUBTÍTULO:	Gestión de la Seguridad
ARCHIVO:	politicaSegUsoCredenciales.docx
ESTADO:	Formal

Lista de Cambios

VERSIÓN	FECHA	AUTOR	DESCRIPCIÓN
1.0.0	04/01/2019		Emisión Inicial

Firmas y Aprobaciones

ELABORADO POR: Ing. Paúl Enríquez
Jefe del área de Redes

Firma: _____

ELABORADO Y REVISADO POR: Msc. Franklin Sanchez
Jefe Sistemas

Firma: _____

APROBADO POR: *PhD. María José Rubio*
Prorrectora PUCESI

Firma: _____

Pontificia Universidad Católica del Ecuador
PUCE
ÁREA DE REDES
Sede Ibarra

Pontificia Universidad Católica del Ecuador
PUCE
DIRECCIÓN DE SISTEMAS
Sede Ibarra

Pontificia Universidad Católica del Ecuador
PUCE
PRORRECTORADO
Sede Ibarra

ÍNDICE DE CONTENIDOS

POLÍTICAS DE SEGURIDAD PARA USO DE CREDENCIALES DE USUARIO

1 Información general

Debido al uso masivo de las tecnologías de la información por parte de sus actores: estudiantes, docentes, personal administrativo y grupos de interés que acceden a los servicios y recursos de TI que brinda la Universidad. Con la *"POLÍTICA DE SEGURIDAD PARA USO DE CREDENCIALES DE USUARIO"* se define los lineamientos y responsabilidades que todos los usuarios deben conocer y practicar para minimizar el riesgo de pérdida de confidencialidad, integridad y disponibilidad de la información debido a accesos no autorizados por terceras personas que buscan acceder a información confidencial para eliminar o modificar datos sensibles que podrían afectar seriamente la integridad de la información almacenada en las plataformas tecnológicas de la Universidad.

Finalmente, la presente política detalla el propósito, alcance, políticas, cumplimientos que todo usuario de la comunidad académica debe conocer con respecto a la generación, mantenimiento y uso de su cuenta de usuario.

2 Consideraciones

Que, el numeral 44 del Código de Ética de la Pontificia Universidad Católica del Ecuador, determina abstenerse de utilizar en su propio beneficio o de comunicar cualquier manera datos, documentos o información de carácter institucional, más aún si están calificados como confidenciales, a los que han tenido acceso durante el ejercicio de su actividad en la institución. El carácter de confidencialidad permanecerá una vez concluida su relación con la institución y comprenderá la obligación de no hacer uso de ellos después de su separación;

Que, el numeral 45 del Código de Ética de la Pontificia Universidad Católica del Ecuador, determina no tener derecho a acceder a información ajena a sus funciones o estamento de pertenencia. Solo se podrá obtener originales o copias de documentos o de archivos, si éstos se requieren para el debido cumplimiento de sus funciones o actividades o para el ejercicio de sus derechos;

Que, el numeral 47 del Código de Ética de la Pontificia Universidad Católica del Ecuador, establece que no está permitido acceder, sin la debida autorización, a datos o programas informáticos contenidos en un sistema o en parte del mismo en contra de la voluntad de quien tenga la legítima custodia de los mismos;

Que, el numeral 48 del Código de Ética de la Pontificia Universidad Católica del Ecuador, señala que no podrán ser accesibles a personas no autorizadas los

documentos y soportes de almacenamiento de datos utilizados en el lugar de trabajo y, por consiguiente, se guardarán con las medidas de seguridad adecuadas. Los ordenadores deberán protegerse mediante la utilización de contraseñas que deberá ser cambiadas con frecuencia. Es responsabilidad de quienes tienen a su cargo instrumentos y archivos informáticos observar minuciosamente las directrices técnicas que se impartan;

Que, el numeral 50 del Código de Ética de la Pontificia Universidad Católica del Ecuador, establece que no está permitido, en modo alguno, apoderarse, utilizar o modificar sin autorización, en perjuicio de la PUCE o de terceros, datos reservados de carácter personal o familiar de otra persona que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro, así como acceder por cualquier medio a los mismos eliminarlos, alterarlos o utilizarlos en perjuicio del titular de los datos o de un tercero;

Que, el apartado (12) Políticas Generales de Seguridad de la Información de las Políticas Generales de la PUCE, establece que se respetan los objetivos y principios de la seguridad de la información. Para este fin se destinan los recursos necesarios para el funcionamiento del Sistema de Gestión de Seguridad de la Información, SGSI. Este sistema tiene las siguientes características:

- **Integridad**: la información no puede ser alterada ni eliminada por cambios no autorizados o accidentales. Se debe garantizar su precisión, completitud, suficiencia y validez en los métodos de procesamiento y en todas las transacciones, de acuerdo con los valores y principios de la PUCE, evitando fraudes o irregularidades de cualquier índole que alteren la información.
- **Confidencialidad**: la información sólo debe ser conocida por el personal que la requiera para el desarrollo de sus funciones, quien debe protegerla del uso no autorizado o divulgación accidental, sabotaje, espionaje, violación de la privacidad y otras acciones que pudieran poner en riesgo la información.
- **Disponibilidad**: La información debe ser accesible a estudiantes, docentes, investigadores, autoridades, administrativos y trabajadores, usuarios internos, externos y entes reguladores de control de manera oportuna, según sus niveles de responsabilidad y autorización.
- **Confiabilidad**: La información institucional debe ser precisa, completa, relevante, accesible, oportuna, fácil de usar y orientada a las necesidades de la comunidad universitaria, de manera que contribuya a la consecución de los objetivos institucionales.

3 Propósito

Establecer la normativa del uso adecuado de las credenciales de usuario para el acceso a los servicios y recursos de TI que brinda la Universidad mediante la aplicación de buenas prácticas de seguridad de la información.

4 Alcance

Esta política se aplicará con observancia obligatoria a todos los usuarios administrativos, docentes, estudiantes y terceros con acceso a los servicios y recursos informáticos que brinda la universidad a través de su sistema de información.

5 Principios

La Política define los siguientes principios para todo usuario que cuente con acceso a los servicios y recursos informáticos que brinda la Universidad:

- Actuará de acuerdo a esta normativa y demás normas vigentes de la Universidad.
- Deberá utilizar el sistema informático que brinda la universidad con el cuidado y la responsabilidad que deviene del ejercicio de su función.
- Actuará en forma legal, honesta y responsable, para garantizar la integridad de los recursos de computación que la universidad pone a su disposición para el cumplimiento de sus funciones.
- Deberá respetar los derechos de otros usuarios, la integridad del sistema y sus métodos de control.

6 Políticas

Creación de credenciales

- La creación de las credenciales de usuario para el personal estudiante, docente y administrativo será creada por las aplicaciones laboral y de admisión o por otros métodos automatizados.
- Para el caso de los usuarios docentes y estudiantes el nombre de la cuenta estará conformada por las iniciales de los nombres junto con el primer apellido en caso de repetición se agregará al final un secuencial.
- Para el caso de los usuarios administrativos el nombre de la cuenta estará conformada por la inicial del primer nombre junto con el primer apellido en caso de repetición se agregará al final un secuencial.
- La creación de las credenciales de docentes y administrativos se realizará una vez se haya legalizado en la Dirección Administrativa su vinculación a la Institución.

- La creación de las credenciales de estudiantes se realizará una vez hayan legalizado la inscripción y se encuentre debidamente aprobado para ser admitido en la Universidad.
- El estudiante deberá obtener el carné institucional para realizar el cambio de contraseña.
- El personal administrativo y docente deberá realizar el cambio en el primer inicio de sesión.
- Las credenciales de usuario no se eliminarán, únicamente se deshabilitarán a los usuarios administrativos y docentes que se hayan desvinculado de la institución.
- Las credenciales de usuario de los estudiantes permanecerán siempre activas.

Deshabilitación de credenciales

- Las credenciales de usuario docente y administrativo se deshabilitarán únicamente por notificación expresa de la Dirección Administrativa luego de la desvinculación oficial del personal.
- La unidad de sistemas deshabilitará inmediatamente, sin el consentimiento del usuario, una cuenta de usuario al detectar alguna incidencia de seguridad reportada por las aplicaciones o centros de seguridad, como medida preventiva, sin embargo, se deberá informar al usuario por los canales internos de comunicación establecidos.

Habilitación de credenciales

- La habilitación de las credenciales de usuario del personal docente y administrativo que se han desvinculado de la institución será solicitada por notificación expresa de la Dirección Administrativa.

Cambio de contraseña

- Para el personal administrativo, docente y estudiante será de forma personal previa identificación que le acredite, en la unidad de sistemas en jornada laboral.
- El cambio se realizará cuando lo requiera el usuario, por olvido de la misma o por sospecha de que alguien ha logrado capturar su contraseña.
- Cuando el periodo de caducidad haya vencido el cambio de contraseña para el personal docente y administrativo es de manera obligatoria.

Propiedades de las contraseñas

- La complejidad de la contraseña estará establecida por mínimo 8 caracteres en combinación alfanumérica, carácter especial y mayúsculas.
- La caducidad de la contraseña será cada 6 meses.
- Cada 5 intentos fallidos se bloquearán las cuentas por seguridad frente a ataques de fuerza bruta.

- Mantener un historial de contraseña para evitar volver a escribir en forma total o parcial la misma al momento de la actualización.

Uso de credenciales

En el momento mismo que el usuario conoce sus credenciales pasa a ser el único responsable de todas las acciones que se realicen con la cuenta de usuario que le fue asignada, para ello es importante seguir las siguientes recomendaciones:

- Las credenciales deben ser de uso único para todos los servicios de tecnología de información.
- Evitar anotar o guardar las contraseñas en cualquier medio no seguro.
- Bajo ninguna circunstancia entregar las credenciales a otras personas, debido a que es responsabilidad absoluta del propietario todas las acciones que se realicen con la cuenta de usuario dentro de los sistemas a los que tiene acceso.
- No divulgar o exponer las credenciales.
- Cambiar la contraseña inmediatamente al detectar alguna sospecha de mal uso de la misma.
- No crear contraseñas fáciles u obvias, p.ej. fecha de nacimiento, nombre de mascotas, nombre de hijos, etc., Crear contraseñas que sean fáciles de recordar, pero difíciles de descifrar.
- Al máximo evitar el uso de las credenciales en dispositivos desconocidos, redes de datos públicas y abiertas, debido a que pueden contener software que captura las pulsaciones del teclado o captura de tráfico de red.
- Proteger el ingreso de las credenciales observando que alrededor no existan personas que puedan mirar lo que escribe.
- Evitar ingresar las credenciales en sitios web no seguros, solicitados vía correo electrónico o cualquier otro medio electrónico. La unidad de sistemas no solicita por estos medios el ingreso o actualización de credenciales.

7 Cumplimiento de política

La unidad de sistemas verificará el cumplimiento de esta política a través de diversos métodos, que incluyen entre otros, visitas periódicas, monitoreo de red, informes de herramientas de negocios, auditorías internas y externas de ser el caso.

Cualquier excepción a la política debe ser aprobada en Prorrectorado y ejecutada por la unidad de sistemas.

El incumplimiento de esta normativa puede resultar en la aplicación de medidas disciplinarias.

8 Definiciones y términos

Ataques de fuerza bruta. Es un método de prueba y error utilizado por los programas de aplicación para descodificar datos encriptados, como contraseñas.

Captura de tráfico. Captura automática de contraseñas enviadas en claro y nombres de usuario de la red.

Credenciales. Las credenciales están conformadas por la cuenta de usuario y una contraseña.

Historial de contraseña. Determina el número de nuevas contraseñas únicas que deben asociarse con una cuenta de usuario antes de que se puede reutilizar una contraseña anterior.

Medio Electrónico. Cualquier tipo de dispositivo que almacena y permite la distribución o el uso de información electrónica.

Servicios tecnológicos. Son servicios profesionales diseñados para facilitar el uso de la tecnología por parte de las organizaciones y los usuarios finales. Estos brindan soluciones especializadas orientadas a la tecnología al combinar los procesos y funciones de software, hardware, redes, telecomunicaciones y electrónica.

Sistema informático. Es un sistema que permite la gestión de la información de forma automatizada mediante el uso de recursos tecnológicos y humanos.

Terceros. Persona u organización ajena a la universidad

TI. Departamento de tecnología de información.

Unidad de Sistemas
Firmado digitalmente por Unidad de Sistemas
Fecha: 2019.01.04 16:00:38 -05'00'