DIRECCIÓN DE
INFORMÁTICA

Normas de uso del sistema de autenticación[1] con contraseña única

El sistema de autenticación con contraseña única permite que los usuarios de los servicios de información proporcionados por unidades de la PUCP como la DIRINFO, la DIA y la DCI utilicen el mismo mecanismo de ingreso. Los servicios que utilizan este sistema se encuentran en http://intranet.pucp.edu.pe/directorio-servicios.html

El sistema:

1.- Permitirá usar una sola contraseña para todos los servicios, con la consiguiente ventaja de no exigir al usuario recordar más de una contraseña.
2.- Permitirá usar una sola vez el proceso de autenticación para acceder a varios servicios a la vez, con la consiguiente ventaja de no exigir al usuario autenticarse varias veces (una por cada vez que desee usar un servicio). Esto se conoce, por sus siglas en inglés, como SSO (Single Sign-On).
3.- Permitirá usar una sola vez el proceso de cierre de sesión para terminar las sesiones a varios servicios a la vez (Single Sign-Out), con la consiguiente ventaja de evitar el olvido de cierre de sesión de algún servicio por parte del usuario.
4.- No impedirá que el servicio de información pueda usar procesos adicionales de identificación.
5.- No impedirá que el servicio de información pueda usar procesos adicionales de autorización[2].

El ***identificador de usuario*** es aquel dato del usuario que es único para cada persona, y que se encuentre registrado en nuestra base de datos, permitirá que sea utilizado en el proceso de autenticación. El identificador de usuario, o simplemente **USUARIO-PUCP**, que podrá usarse, indistinta e independientemente del servicio requerido, es cualquiera de los siguientes datos:

- Código de personal (8 dígitos)
- Código de alumno regular de pregrado y posgrado (8 dígitos)
- Código de inscrito en una actividad PUCP. P.e. prospecto, alumno de formación continua, etc.
- Dirección de correo electrónico institucional (parte inicial de la dirección sin el dominio @pucp.edu.pe o @pucp.pe)
- Dirección de correo electrónico externo usado para una inscripción o para recuperación de contraseña (dirección completa, p.e. micorreo@dominio.com)
- DNI validado con la RENIEC (11 caracteres: 3 letras ‘dni’ + 8 dígitos del número del DNI).

Para autenticarse en el **sistema de autenticación con contraseña única** será necesario el ingreso de la combinación de usuario-pucp y la contraseña.

---

1 La ***autenticación*** es el proceso mediante el cual se garantiza que una persona es quien dice ser. Como el costo de usar un proceso de ***identificación*** (ubicar una identidad en base a datos biométricos) dentro de un proceso de autenticación tiene, aún, una relación costo/beneficio demasiado alta, se suele usar el método de una contraseña conocida sólo por la (auténtica) persona. Con esto, sin llegar a una garantía absoluta, se disminuye el riesgo de no lograr la autenticación.

2 La ***autorización*** es el proceso mediante el cual se controla el acceso a sub-servicios conformados por aplicaciones, transacciones y/o conjuntos de datos.

Esta facilidad de acceder a múltiples servicios de información a través de una sola sesión de autenticación requiere que el usuario tenga presenta las siguientes consideraciones para que la experiencia con este sistema sea confiable y segura.

1. La sesión de autenticación es válida solo para las ventanas y pestañas del navegador web (Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Safari, etc.) desde donde se invoque al sistema de autenticación con contraseña única.
2. Cuando finalice la sesión mediante el enlace o botón “Cerrar sesión” en cualquiera de los servicios de información que esté utilizando, finalizarán las sesiones de todos los servicios de información que tenga en ese navegador web.
3. Si no cierra la sesión mediante el enlace o botón “Cerrar sesión” y mantiene el navegador web activo, podrá ingresar nuevamente a cualquiera de los servicios autenticados por el sistema de autenticación con contraseña única invocando la ruta de cada servicio de información.
4. Si utiliza una computadora personal que puede ser utilizada por muchas personas es importante que finalice la sesión en cualquier de los servicios y cierre completamente el navegador web (esto incluye todas las ventanas existentes del navegador) si ya no desea trabajar con ninguno de los servicios de información autenticados por el sistema de autenticación con contraseña única, pues en caso contrario su sesión permanecerá activa y los servicios pueden ser invocados nuevamente sin necesidad de solicitar usuario-pucp ni contraseña.
5. Solo puede existir una sesión del sistema de autenticación con contraseña única por cada tipo y versión de navegador web.
6. La duración de las sesiones es de 4 horas. Si no se hace uso del sistema de autenticación con contraseña única durante ese lapso de tiempo, automáticamente se cierra la sesión para todos los servicios, excepto el Campus Virtual y el GMail PUCP, y será necesario autenticarse nuevamente para ingresar a ellos. El ingresar a un servicio por primera vez reanudará la duración de la sesión.
7. Al cerrar sesión en el sistema de autenticación con contraseña única, se cerrará la sesión de GMAIL PUCP (si se estaba utilizando) y de todas las sesiones para cuentas GMAIL externas en ese navegador.

La PUCP no se hace responsable por las consecuencias del mal uso que se le pueda dar al sistema, como el uso ilícito de sesiones de otras personas debido al cierre incorrecto de la sesión.