 USPEC Unidad de Servicios Penitenciarios y Carcelarios	MANEJO DE CONTRASEÑAS	Código: A3-GU-01
		Versión: 01
		Vigencia: 13/09/2016

1. **PROCESO:** Gestión de las Tecnologías de la Información
2. **SUB PROCESO:** N/A
3. **OBJETIVO:** Establecer el marco de referencia para el uso, gestión y administración de las contraseñas de las credenciales o cuentas de acceso de los Sistemas de Información y aplicaciones de la Unidad de Servicios Penitenciarios y Carcelarios USPEC.
4. **CONTENIDO:**

El factor de autenticación más usado en los sistemas de información y aplicaciones de USPEC, es el de usuario y contraseña, para lo cual se hace necesario crear una guía de manejo de contraseñas en cumplimiento de las políticas del SGSI.

4.1 Alcance

Involucra a todos los roles definidos en las aplicaciones y sistemas de información de USPEC. No existen excepciones bajo ninguna circunstancia. Es de aclarar que el cumplimiento de esta guía es tanto para los Administradores, Directivos o Coordinadores, como para todo el personal de la Entidad. El incumplimiento de esta guía se cataloga como un incidente de seguridad que puede dar inicio a un Proceso disciplinario.

4.2 Reglas


Las reglas para el manejo de las contraseñas en el acceso a las aplicaciones y sistemas de información de USPEC son:

- ✓ Para los servidores y aplicativos críticos se debe cambiar las contraseñas de administrador por lo menos cada 60 días.
- ✓ Las contraseñas de usuarios para iniciar sesión en el directorio activo, serán configuradas para cambiarse automáticamente cada 2 meses.
- ✓ Todas las contraseñas de nivel de usuario por ejemplo para ingreso a los aplicativos, deben ser cambiadas por el usuario cada 2 meses. En los casos en que un aplicativo pueda configurarse para exigir este cambio de contraseña, se debe habilitar esta opción.
- ✓ Las contraseñas son personales e intransferibles, sin ninguna excepción. La solicitud de una contraseña de otro usuario, puede ser considerado un incidente de seguridad que debe reportarse.
- ✓ Las contraseñas no deben ser almacenadas ni transmitidas en medios digitales o físicos.
- ✓ Las contraseñas no pueden ser expresadas en conversaciones presenciales o telefónicas, sin ninguna excepción.
- ✓ El personal de soporte técnico cuenta con sus propias credenciales de acceso y la debida contraseña para la misma, en ningún caso un usuario debe suministrar por ningún medio su contraseña.
- ✓ Se recomienda no usar contraseñas de cuentas personales para las cuentas asignadas en USPEC.

4.3 Composición

A continuación las especificaciones que se deben seguir para la definición de contraseñas para los sistemas de información y aplicaciones de USPEC.

- ✓ Debe tener una longitud mínima de 8 caracteres.

 USPEC Unidad de Servicios Penitenciarios y Carcelarios	MANEJO DE CONTRASEÑAS	Código: A3-GU-01
		Versión: 01
		Vigencia: 13/09/2016

- ✓ Debe tener una longitud máxima de 12 a 100 caracteres dependiendo del sistema o aplicación.
- ✓ Contener tanto letras mayúsculas como minúsculas por ejemplo, a-z, A-Z.
- ✓ Contener números y/o caracteres especiales por ejemplo, - !@#\$%^&*()_+|~=-\`{}[]:;'\<>?,./.
- ✓ No se permite que la contraseña sea el nombre o parte del nombre del usuario.
- ✓ No deben contener números que hagan referencia a información personal como fechas de nacimiento, números de identificación, entre otros.
- ✓ Hacer uso de estructuras que no tengan una secuencia lógica, por ejemplo: ABCD1234.

4.4 Continuidad de la Seguridad de la Información durante contingencias

Considerando la integración con el plan de continuidad de USPEC, se establecen los siguientes controles para mantener la seguridad de la información durante eventos que puedan causar la interrupción de las operaciones:

- ✓ Las contraseñas de perfil de administrativo de las bases de datos, sistemas de información y aplicativos, serán almacenadas en un sobre sellado y este debe ser almacenado en un lugar seguro accedido solo por una persona. Una vez se declare el evento, la Dirección General o la Jefatura de Tecnología será quien autoriza la apertura del sobre con las contraseñas.

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	13/09/2016	Todos	Se crea el documento

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	Revisó:	Aprobó:
Firma: Original Firmado	Firma: Original Firmado	Firma: Original Firmado
Nombre: Fernando Aguilera	Nombre: Fernando Arturo Vargas	Nombre: Diana Lucia Pinilla Marín
Cargo: Consultor Externo Globaltek Security SAS	Cargo: Técnico Operativo	Cargo: Jefe Oficina de Tecnología
Dependencia: N/A	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología