1. **PROCESO:** Gestión de las Tecnologías de la Información.

2. **SUBPROCESO:** N/A.

3. OBJETIVO

Definir los lineamientos asociados con la estructuración y el uso de contraseñas seguras, necesarios para el fortalecimiento de las acciones tendientes a disminuir la posibilidad de acceso no autorizado a la información que se encuentra alojada en activos tipo software o servicios, mitigando el riesgo asociado con la pérdida de disponibilidad, integridad o confidencialidad de la información de la Unidad de Servicios Penitenciarios y Carcelarios USPEC.

4. ALCANCE

Aplica para las contraseñas de acceso a los sistemas de información, servicios y la administración de todos los equipos y dispositivos que conforman la plataforma tecnología de la USPEC.

5. LINEAMIENTOS GENERALES

- Cumplir con la estructuración y gestión de contraseñas seguras es deber de todo el personal vinculado a la Entidad. Por lo tanto, es responsabilidad de cada servidor público la gestión de cada usuario y contraseña que le sea asignado para el cumplimiento de sus funciones o actividades contractuales, cualquier desviación en este protocolo, puede llevar a la materialización de riesgos de seguridad de la información.

- El usuario y su contraseña asociada, es el único mecanismo de identificación de cada servidor público que le da autorización para el uso de los recursos tecnológicos y acceso a la información institucional, este mecanismo, permite manejar los perfiles y permisos de los usuarios, hacer seguimiento y llevar trazabilidad de las gestiones y acciones que sean ejecutadas por este.

- Cada servidor público al que se le asigne un usuario de acceso a un sistema de información y/o a los servicios de la plataforma tecnológica, es responsable de garantizar la seguridad de la información a su cargo, la cual está disponible en medios electrónicos, cumpliendo estrictamente cada uno de los documentos enmarcados en el Sistema de Gestión de la Seguridad de la Información - SGSI, particularmente lo indicado en esta guía.

- Esta guía toma como referencia los estándares y componentes de uso libre determinados por la NTC/ISO 27002:2013 los siguientes numerales:

  Numeral 9.2.4: Gestión de información de autenticación secreta de usuarios literales d, f.
  Numeral 9.3.1: Uso de información de autenticación secreta

- El incumplimiento de esta guía se cataloga como un incidente de seguridad.

6. ESTRUCTURACIÓN Y GESTIÓN DE CONTRASEÑAS SEGURAS

6.1 CREAR UNA CONTRASEÑA SEGURA

- Las contraseñas deben contener mínimo 8, y no más de 16, caracteres intercalados de tal forma que se combinen letras minúsculas y mayúsculas, números y símbolos, (sólo caracteres basados en el estándar ASCII), no puede contener tildes, ni caracteres acentuados o espacios. A continuación, se relacionan los caracteres especiales no permitidos, por ser incompatibles con algunos sistemas:
  - Espacio.
  - "Comilla Doble".
  - ‘Comilla Sencilla’.

- El método de generación de contraseña segura seleccionado por la USPEC es el denominado contraseña pseudoaleatoria. La contraseña se deriva de una frase fácil de recordar. Por ejemplo:

  Frase Personal: " Somos la Entidad pública que facilita las condiciones físicas, espacios seguros y medios adecuados para la protección de los derechos …". Es válido, el título o frases de un libro que tenga mayor recordación, la letra de una canción, lo más importante es que sea una frase que no se olvide.
  Método: Elija las dos primeras letras de cada palabra, hasta un mínimo de 8 caracteres, y cambie algunas letras por números y caracteres, tomando como referencia, la misión de la USPEC, tendríamos, SolaEnpuqu, cambiando la letra “o” por el número “0”, la letra “l” por el número “1”, la letra “E” por el número “3”, la letra “u” por el signo “?”, e incluyendo aleatoriamente mayúsculas, obtendremos una contraseña segura.
  Contraseña: S01a3nP?qU

- Como alternativa, se podrá generar la contraseña segura de un sitio web especializado, siempre y cuando se configure de tal forma que la longitud sea de 8 caracteres e involucre todo tipo de caracteres válidos, se recomienda el uso del portal LastPass[1].

- No se deben utilizar datos personales, tales como: nombres, el nombre del usuario en el sistema (ID), números de identificación, fechas, o cualquier información de tipo personal. Es responsabilidad de cada servidor público el no uso de las siguientes contraseñas:
  - En blanco o con palabras como: “contraseña”, “amor”, “súper”, “uspec”, etc.
  - Su nombre, el de su cónyuge, hijo(s), mascota(s), amig@s, compañer@s de trabajo, personajes favoritos, lugares y en general de cualquier tipo de nombre.
  - Cadenas de números o letras como: 12345678, abcdefgh, números de teléfono o celular, número de identificación, fecha de nacimiento.
  - Una palabra en un diccionario sin importar el idioma.
  - Contraseñas con una sola letra repetida como “aaaa”, patrones simples de letras en el teclado, como “asdfgh”.

- Cada vez que un administrador funcional o técnico, que cambie su función o cargo, o se desvincule de la Entidad, es indispensable que el dueño del activo haga seguimiento al ajuste del perfil, la desactivación de su usuario o el forzado del cambio de todas las contraseñas a las que tuviera acceso mientras adelantaba la administración del sistema, aplicación o servicio de TI. Quien reciba las gestiones de administración debe adelantar de manera prioritaria el cambio de contraseñas en todos los sistemas que le sean entregados

[1] https://www.lastpass.com/es/password-generator

para administración, estas gestiones deben articularse con los subsistemas asociados para evitar desincronizaciones o fallos en servicios automáticos, lo por cual se debe realizar la debida planeación y documentación de la actividad conforme el Control de Cambios.

6.2. USO DE LA CONTRASEÑA SEGURA

- Utilizar contraseñas diferentes para cada servicio, aplicación o sistema externo a los que se tenga acceso autorizado, estas contraseñas deben cumplir los lineamientos de la presente guía o en el caso de los servicios externos se deberán tener en cuenta los lineamientos establecidos por las Entidades u organizaciones responsables para la gestión de contraseñas. Es decir, no utilizar la contraseña que se tiene configurada para acceder a los servicios internos dispuestos en la plataforma tecnológica de la USPEC.

- Renovar periódicamente cada una de las contraseñas. En el contexto institucional, las contraseñas tendrán un periodo de vigencia máximo de 60 días. Esto implica que se requerirá el cambio atendiendo las mejores prácticas asociadas con esta temática y con lo consagrado en las políticas de seguridad. El tiempo de caducidad será parametrizable según las determinaciones que se tomen en el marco de acción del SGSI.

- Cada cuenta de usuario en el directorio se parametriza para que automáticamente requiera el cambio de contraseña según lo indicado anteriormente y dado cumplimiento al numeral 4.2.1 Crear una contraseña segura.

- La contraseña segura es un código único, personal e intransferible, que no debe ser divulgado o compartido, el incumplimiento de este lineamiento equivale a un incumplimiento a las políticas del SGSI.

- No está permitido utilizar credenciales de acceso diferentes a las asignadas para acceder a los Sistemas de Información y a los servicios de la plataforma tecnológica, el acceso debe ser exclusivamente a través del usuario asignado.

- Si por necesidad del servicio, se requiere el uso de un usuario y contraseña asignado a un servidor público que no se encuentra en las instalaciones de la USPEC, únicamente el jefe inmediato o supervisor, previa solicitud escrita a la OTEC, autorizará la asignación de una contraseña temporal, con una duración específica, e indicará el servidor público que la utilizará; el solicitante será responsable de lo que suceda con los activos de información y la seguridad por la duración del evento. Una vez el funcionario retorne, debe actualizar la contraseña.

- Si se digita consecutivamente 3 veces una contraseña errónea para acceder al sistema o herramienta la cuenta debe ser bloqueada automáticamente. Será necesario, a través de la herramienta de gestión de soporte técnico, solicitar la reactivación de la cuenta al personal de soporte, o esperar a la reactivación automática para que esta vuelva a estar habilitada.

- En caso de olvido de la contraseña, se debe solicitar formalmente al soporte técnico o al administrador funcional del sistema de información, el restablecimiento de la contraseña, para lo cual se debe asignar una contraseña temporal con petición de cambio en el primer o siguiente inicio de sesión, el usuario es responsable de cambiarla de manera obligatoria.

6.3 CAMBIAR O ACTUALIZAR LA CONTRASEÑA SEGURA

- La contraseña de red y de correo electrónico institucional, sistemas básicos asignados a un servidor público con vínculo vigente con la USPEC, debe ser actualizado así:
    - Presionar simultáneamente las teclas CTRL+ALT+SUPR, aparece la pantalla de Seguridad de Windows. Seleccione la opción de Cambiar Contraseña. Escriba la contraseña vigente. Cumpliendo lo indicado en el numeral 5.1 Crear una contraseña segura, digite la nueva contraseña segura dos (2) veces. El sistema indica que la contraseña ha sido cambiada con éxito. Si requiere soporte técnico, debe gestionar a través de la herramienta de gestión de soporte técnico.
    - Con la ejecución del anterior protocolo, simultáneamente se actualiza la contraseña del correo electrónico institucional.

6.4 CONTINUIDAD DEL SERVICIO DURANTE CONTINGENCIAS

- Exclusivamente, las contraseñas de administración de la plataforma tecnológica deben ser escritas, protegidas en un sobre sellado y almacenadas en un lugar seguro, con los datos de contacto de cada administrador técnico y funcional de cada sistema de información o equipo que conforme la plataforma tecnología de la USPEC, debe incluir, además, los datos de contacto de las mesas de soporte especializado que estén contratadas. Esta información será utilizada por el Jefe de la Oficina de Tecnología en caso de una contingencia, o por ausencia del líder del proceso del sistema o recurso afectado.

7. DEFINICIONES

ASCII [2]: acrónimo que corresponde a la expresión inglesa American Standard Code for Information Interchange, Código Estándar Americano para el Intercambio de Información, en español. Se trata de un patrón de codificación que se emplea en la informática y representa caracteres.

Activo: cualquier elemento que tiene valor para la organización y que para la gestión de riesgos de seguridad de la información se consideran los siguientes: hardware, información, software, servicios y recursos humanos.

Autenticación: si el usuario existe dentro de la plataforma tecnológica y en los sistemas de información, pasa la primera etapa de identificación del usuario, y posteriormente con la contraseña, que solo el usuario conoce, se pasa la segunda etapa de autenticación, si ambas etapas son válidas, el usuario finalmente puede acceder a la información y servicios informáticos permitidos.

Contraseña segura: palabra o expresión secreta, utilizada por verificar el acceso de una persona autorizada para acceder a los recursos o servicios tecnológicos de la USPEC; cadena de caracteres cuyo conocimiento se reduce a un usuario autorizado.

Credenciales: término usado para referirse al conjunto usuario y contraseña.

Cuenta de usuario: es el registro en el Directorio Activo de Windows que contiene toda la información del nombre real del usuario y sus derechos de acceso.

[2] ASCII (s.f.) (citado el 26 de junio de 2020) Recuperado de https://definicion.de/ascii/#:~:text=A-,Definici%C3%B3n%20de%20ASCII,el%20%C3%A1mbito%20de%20la%20inform%C3%A1tica.

Directorio Activo: componente de la plataforma Windows, que proporciona el mecanismo para administrar y gestionar las identidades de los usuarios, los recursos y las relaciones que organizan los entornos de red.

Servidor Público: Los funcionarios y contratistas con vinculación activa con la USPEC se consideran como servidores públicos, se incluyen en esta definición a los practicantes.

Equipo activo de red: corresponde a todos los equipos cuya función sea, o esté asociada con, la distribución de forma activa de información a través de la red de datos institucional.

Plataforma tecnológica: conjunto de elementos interrelacionados de tipo Hardware y Software que se han parametrizado para brindar acceso a servicios de TI y permitir la gestión institucional por parte de los usuarios autorizados.

Propietario del activo: persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

Riesgo: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización).

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	13/09/2019	Todos	Se crea el documento
02	30/06/2020	Todos	Se cambia el nombre “Guía Manejo de Contraseñas” por “Guía para Manejo de Contraseñas Seguras”. Se actualizan todos los numerales.
	04/10/2021	N/A	Se ajustan los códigos de los documentos de acuerdo con la actualización del Mapa de Procesos Institucional. La versión del documento se mantiene debido a que su contenido no se modificó.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma:	Firma:	Firma:
Nombre: Oscar Javier Suárez Ramos	Nombre: Diana Paola Cárdenas Mayra Alexandra Agudelo Fernando Arturo Vargas	Nombre: Oscar Javier Suárez Ramos
Cargo: Jefe Oficina de Tecnología	Cargo: Profesional Universitario Profesional Especializado Técnico Operativo	Cargo: Jefe Oficina de Tecnología
Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología