ÁREA METROPOLITANA DE BUCARAMANGA

POLÍTICA DE USO DE CONTRASEÑAS

ÁREA METROPOLITANA DE BUCARAMANGA

Apoyo tecnológico y de información - Gestión Corporativa Año 2019

Tabla de Contenido

1. INTRODUCCIÓN

Para el Área Metropolitana de Bucaramanga es de gran importancia el manejo que se le dé a las contraseñas asociadas a los sistemas y servicios informáticos. Estas representan las bases sobre la cual se construyen la confidencialidad, integridad y disponibilidad de la información en la entidad, puesto que la seguridad está directamente ligada a la fortaleza de las contraseñas, entre más simples sean, mayor será la posibilidad que sean vulneradas. Por lo que todos los usuarios deben comprometerse contribuyendo personalmente en la protección de la información de la entidad, implementando las directrices definidas en la presente política.

2. OBJETIVO

Establecer los aspectos a tener en cuenta para una adecuada creación y administración de contraseñas en el Área Metropolitana de Bucaramanga, de tal manera que no sean fácilmente vulnerables como parte de un control de acceso seguro y efectivo a los dispositivos informáticos.

3. ALCANCE

Esta política está dirigida y encaminada a la creación y administración de contraseñas empleadas para el acceso y uso de los recursos informáticos tales como: servicios de colaboración (correo, agenda), red corporativa, sistemas de información, Internet e Intranet, por parte de todo el personal que labora en el Área Metropolitana de Bucaramanga.

4. DEFINICIONES

Activos de información: Son elementos de información que la entidad produce en el ejercicio de sus funciones incluye información impresa, escrita, digital o transmitida por cualquier medio electrónico o de almacenamiento en equipos de cómputo incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, base de datos, videos e imágenes.

Acceso a la información: Se refiere al conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema: bases de datos, bibliotecas, archivos, Internet. Es un término estrechamente relacionado con la informática, la bibliotecología y la archivística, disciplinas que estudian el procesado automatizado, clasificado y custodia de la información respectivamente. Asimismo, el acceso a la Información involucra a muchos otros temas, como los derechos de autor, el Código abierto, la privacidad y la seguridad.

Alfanumérico: Es un término colectivo que se utiliza para identificar letras del alfabeto latino y de números arábigos. Es un vocablo híbrido (derivado de: a) «alfa» (primera letra del alfabeto griego), aféresis de la dicción «alfabeto»; b) el sustantivo latino «número»; c) el sufijo «ico»: relativo a.

Contraseña: Es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

Dispositivos informáticos: Son componentes que leen o escriben datos en medios o soportes de almacenamiento y juntos conforman la memoria o almacenamiento secundario de la computadora.

5. POLÍTICA

Como lo establece la política de seguridad y privacidad de la información todas las contraseñas de nivel de usuario y de nivel de sistema inicialmente deben ser asignadas por el área de tics o de apoyo tecnológico y de la información además deben ser creadas teniendo en cuenta algunos de los siguientes parámetros:

- La contraseña no debe estar asociada al ID de inicio de sesión, nombre, fecha de nacimiento, teléfonos, número de cédula o datos de familiares (hijos, padres, etc.).
- Utilizar contraseñas diferentes para los distintos servicios que utiliza dentro de la entidad.
- El usuario debe notificar oportunamente cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.
- Estar compuesto por lo menos de 8 caracteres.
- Un carácter no debe ser usado secuencialmente más de 2 veces.
- La contraseña debe incluir por lo menos 2 caracteres numéricos y 2 caracteres alfabéticos.
- Contener caracteres alternados en mayúsculas y minúsculas.
- No se podrá reutilizar hasta 3 contraseñas ya empleadas anteriormente.
- Definir periodicidad de cambio de contraseñas.
- El soporte, mantenimiento, renovación o actualización de credenciales o contraseñas estarán a cargo del personal de apoyo tecnológico y de la información.
- Todas las contraseñas deberán ser tratadas como información confidencial.
- Nunca deberán ser escritas en papeles, ni stickers, ni deberán ser guardados en línea usando las opciones de autocompletado y agentes de manejo de contraseñas que ofrecen el sistema operativo, bases de datos, aplicaciones o sistemas de información.
- Las contraseñas no deben ser guardadas en ningún sistema computarizado sin cifrado.

6. RECOMENDACIONES

- Se recomienda escoger una palabra, después mezclarla con algunos números al azar (ejemplo, caracoles se convierte en c4r4c02es).
- Convertir una frase fácil de recordar a su acrónimo con símbolos también es una buena estrategia. “Es un día muy bello” puede abreviarse a eudmb, y después se le agregan caracteres no alfanuméricos y mayúsculas. eUnMb04 sería una contraseña válida.
- Cambiar periódicamente el método para generar su contraseña.
- Debe ser fácil de recordar, pero difícil de adivinar.
- No estar basados en información personal, ni de trabajo (no usar nombres de familiares, fechas, palabras de uso común.