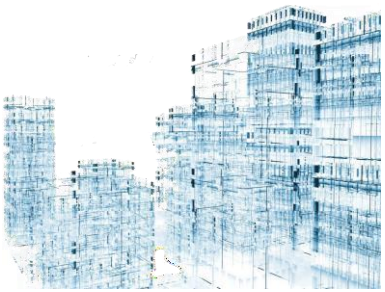
POLÍTICA DE USUARIOS Y CONTRASEÑAS

AREA DE TECNOLOGIA – IT

BOGOTA D.C.

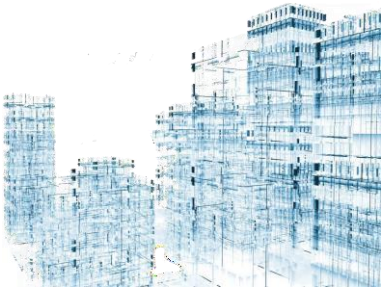


INFORMACIÓN PRELIMINAR DEL DOCUMENTO

Título	Lineamiento de Usuarios y Contraseñas (SGSI)
Área	Tecnología – IT
Autor	Ing. Herman Montenegro, Miguel Ángel Cano

CONTROL DE CAMBIOS

Versión	Fecha	Cambios realizados	Modificado por
1.0	27/06/23	Creación del documento	Herman Montenegro
1.1	27/08/25	Modifica políticas en longitud mínima de contraseña, caracteres especiales permitidos, reglas de reutilización	Herman Montenegro



LINEAMIENTOS POLITICA DE SEGURIDAD DE LA INFORMACIÓN

En la actualidad, la seguridad de la información es una de las principales preocupaciones de las empresas y organizaciones en todo el mundo. La información es uno de los activos más valiosos que posee una empresa, por lo que es necesario protegerla adecuadamente para evitar el robo, la pérdida o la filtración de datos.

Una de las medidas más importantes y eficaces para proteger la información es el establecimiento de políticas de seguridad de la información. Estas políticas establecen directrices y reglas claras para que los usuarios y empleados de Combuscol SA puedan manejar la información de forma segura y responsable.

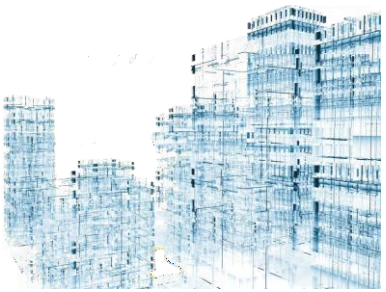
Uno de los aspectos más importantes de las políticas de seguridad de la información es el manejo adecuado de contraseñas. Las contraseñas son la primera línea de defensa contra el acceso no autorizado a la información. Una contraseña segura y única es la mejor forma de proteger las cuentas y los datos personales.

En este sentido, las políticas de seguridad de la información deben incluir reglas claras para la elección de contraseñas. Por ejemplo, es necesario que las contraseñas tengan cierta longitud y complejidad, con combinaciones de letras, números y símbolos. Además, las contraseñas deben ser únicas para cada cuenta y no se deben compartir con nadie más.

Otro aspecto importante de las políticas de seguridad de la información es la caducidad de las contraseñas. Es recomendable establecer una periodicidad para el cambio de las contraseñas, por ejemplo, cada tres meses. Es importante que esta medida se aplique no solo a los empleados, sino también a los usuarios en general, por ejemplo, en el caso de las cuentas de correo electrónico o las redes sociales.

Por último, es fundamental que las políticas de seguridad de la información incluyan medidas de protección contra el phishing y otros ataques cibernéticos. Los usuarios deben estar informados sobre todos los riesgos asociados al manejo de la información y deben estar capacitados para identificar y evitar cualquier intento de phishing o ataque similar.

En conclusión, las políticas de seguridad de la información son una herramienta fundamental para garantizar la protección de la información en Combuscol SA, y prácticas seguras en cuanto al manejo de contraseñas son fundamentales para evitar contratiempos o posibles filtraciones de información.



USUARIOS Y CONTRASEÑAS

La asignación de usuarios y contraseñas es un permiso que Combuscol SA concede a sus funcionarios, con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información.

La política de seguridad de usuarios y contraseñas tiene como objetivo principal establecer reglas y directrices para garantizar un uso seguro y protegido de los sistemas de información de Combuscol SA

OBJETIVOS ESPECÍFICOS

- ✓ El objetivo principal de la política de seguridad de usuarios y contraseñas es proteger la información de Combuscol SA contra accesos no autorizados, robos, hackers, virus y otras amenazas.

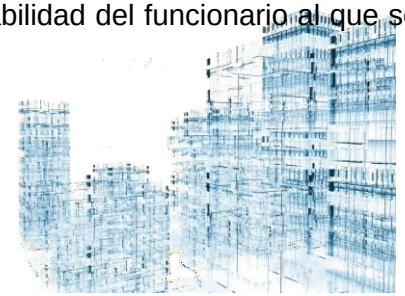
- ✓ Establecer contraseñas seguras y sólidas, capaces de proteger la información sensible y crucial de Combuscol SA.

- ✓ Fomentar la responsabilidad de los usuarios de la compañía, alertando sobre las implicaciones negativas que un mal uso de la información puede tener.

- ✓ Promover una cultura de seguridad de la información, educando a los empleados de la organización y capacitándolos sobre las mejores prácticas para proteger la información de Combuscol SA y los datos de los clientes.

La adjudicación de credenciales como: usuarios (Login o UserID) y contraseñas (Clave o Password) a los diferentes funcionarios de Combuscol SA, así como su desactivación o eliminación de los sistemas se ejecutarán de acuerdo a los procedimientos establecidos y según sea solicitado por los jefes de área y/o coordinadores de operaciones.

Las cuentas de usuario son entera responsabilidad del funcionario al que se le asigne. La cuenta es para uso personal e intransferible.



Las cuentas de usuario (usuario y contraseña) son sensibles a mayúsculas y minúsculas (Case sensitive), es decir que estas deben ser tecleadas como se definan.

Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta es suspendido temporalmente y es reactivada sólo después de haber tomado las medidas necesarias a consideración del área de Tecnología de Combuscol SA.

TIPOS DE CUENTAS DE USUARIO

Todas las cuentas de acceso a los sistemas de información y aplicaciones son propiedad de Combuscol SA. Para efectos del presente lineamiento, se definen dos tipos de cuentas:

a) Cuenta de Usuario de Sistema de Información:

Son todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario de cada Sistema de Información en particular.

b) b. Cuenta de Administración de Sistema de Información:

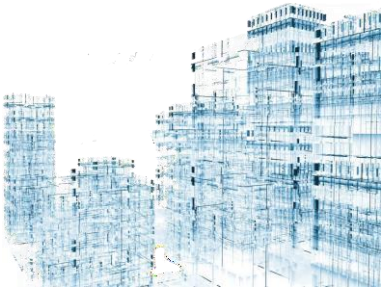
Corresponde a la cuenta de usuario que permite al administrador del Sistema, plataforma tecnológica o base de datos realizar tareas específicas de usuario a nivel administrativo, como, por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema. Usualmente estas cuentas están asignadas para su gestión por parte del área de Tecnología.

Se utiliza Bóveda del sitio https://lastpass.com/ para la gestión y almacenamiento seguro de contraseñas.

La información guardada en la bóveda es secreta, incluso para el proveedor LastPass.

Su contraseña maestra y las claves utilizadas para cifrar y descifrar los datos nunca se envían a los servidores de LastPass, y LastPass jamás puede acceder a ellas.

El proveedor cumple con la norma SOC 2 tipo II. El nivel de calidad de nuestros controles y procesos convierte LastPass en un auténtico referente en materia de seguridad y fiabilidad.



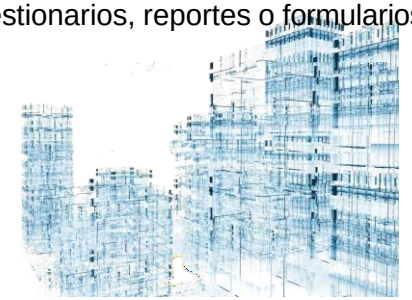
Ventajas de una bóveda de contraseñas

- ✓ Almacenamiento seguro: tome las medidas necesarias para que su información sensible esté guardada a buen recaudo.
- ✓ Contraseñas seguras: utilice contraseñas únicas y seguras sin tener que recordarlas.
- ✓ Ahorro de tiempo: conéctese a sus cuentas online mucho más deprisa.

El jefe de área de Tecnología de la Información deberá contar con una llave maestra personal que abre la Bóveda del sitio seguro: https://lastpass.com/ donde están alojadas las contraseñas sensibles para la administración de los sistemas de información, plataformas tecnológicas y bases de datos.

Estas cuentas de usuario deben mantener las siguientes políticas:

- ✓ Todas las contraseñas de los usuarios administradores deben ser cambiadas 1 vez cada semestre.
- ✓ Todas las contraseñas de usuario del sistema de información deben ser cambiadas 1 vez cada semestre.
- ✓ Los usuarios no podrán reutilizar ninguna de las últimas 2 contraseñas al momento de cambiar su contraseña.
- ✓ El sistema almacenará de forma segura (hasheada) el historial de contraseñas para validar esta regla en el MPOS.
- ✓ Se permiten un máximo de 3 intentos fallidos consecutivos de inicio de sesión, al superar este límite, la cuenta será bloqueada automáticamente en el MPOS.
- ✓ Todas las contraseñas deben ser tratadas con carácter confidencial.
- ✓ Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.
- ✓ Se evitará mencionar y en la medida de lo posible, teclear las contraseñas en frente de otros.
- ✓ Se evitará revelar contraseñas en cuestionarios, reportes o formularios.



- ✓ Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.

- ✓ Se evitará activar o hacer uso de la utilidad de recordar clave o recordar Password de las aplicaciones.

- ✓ Las contraseñas de Combuscol SA deben cumplir con al menos una de las siguientes cuatro categorías:

    - Letras mayúsculas (A-Z)
    - Letras minúsculas (a-z)
    - Números (0-9)
    - Caracteres especiales (! # $ % & ( ) * + , - . : ; = ? @ ^ _.)

- ✓ Los únicos caracteres especiales permitidos para la creación de contraseñas en Combuscol SA son: ! # $ % & ( ) * + , - . : ; = ? @ ^ _.

- ✓ Las contraseñas deben tener una longitud mínima de 10 caracteres y cumplir con los requisitos de complejidad

Uso apropiado de usuarios y contraseñas:

- ✓ No utilice información personal en las contraseñas.

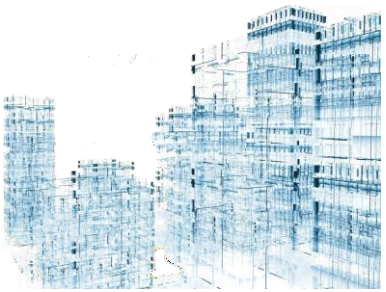
- ✓ Si decide crear una contraseña manualmente, utilice caracteres aleatorios, pero sin patrones típicos como “qwert” o “12345”.

- ✓ Nunca comparta contraseñas a través de correos o mensajes de texto

- ✓ Evite usar contraseñas similares en las que solo cambie una palabra o carácter.

- ✓ Usar las credenciales de acceso sobre los sistemas otorgados exclusivamente para fines laborales y cuando sea necesario en cumplimiento de las funciones asignadas.

- ✓ Cambiar periódicamente las contraseñas de los sistemas de información o servicios tecnológicos autorizados.



Uso indebido del servicio de usuarios y contraseñas:

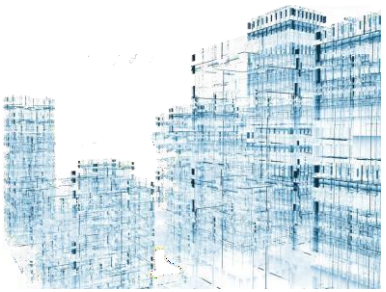
- ✓ Permitir el conocimiento de las claves a terceros.
- ✓ Almacenar las credenciales de acceso en libretas, agendas, post-it, hojas sueltas, etc.
- ✓ Almacenar las credenciales sin protección, en sistemas electrónicos personales (Tablet, memorias USB, teléfonos celulares, agendas electrónicas, etc.).
- ✓ Intentar acceder de forma no autorizada con otro usuario y clave diferente a la personal en cualquier sistema de información o plataforma tecnológica.
- ✓ Usar identificadores de terceras personas para acceder a información no autorizada o suplantar al usuario respectivo.
- ✓ Utilizar su usuario y contraseña para propósitos comerciales ajenos a la compañía.
- ✓ Intentar o modificar los sistemas y parámetros de seguridad de los sistemas de la red Combuscol SA.
- ✓ Utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej. no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).
- ✓ Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.
- ✓ Escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
- ✓ Utilizar contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
- ✓ Enviar la contraseña por correo electrónico o en un SMS.

Responsabilidades de los funcionarios con usuarios y contraseñas asignados

- ✓ Conocer, adoptar y acatar este lineamiento.
- ✓ Velar por la seguridad de la información a la que tenga acceso a través de las credenciales asignadas y a los sistemas de información autorizados para su acceso.
- ✓ Cerrar totalmente su sesión de trabajo para evitar el uso de su identidad, cuando se retire del equipo en que se encuentre laborando.
- ✓ Dar aviso al área de Tecnología, a través de los medios establecidos, de cualquier fallo de seguridad, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.

Seguimiento:

- ✓ Los administradores de los sistemas de información, bases de datos y plataformas tecnológicas pueden efectuar una revisión periódica de los accesos exitosos y no exitosos y al número de intentos efectuados a dichos sistemas para determinar posibles accesos indebidos o no autorizados.
- ✓ El área de Tecnología podrá revisar las bitácoras y registros de control de los usuarios que puedan afectar la operación de cualquier **sistema o plataforma.**



APROBACIÓN

Se firma en señal de aprobación el lineamiento de usuarios y contraseñas como parte de la Política de Seguridad de la Información de Combuscol SA.

Fernando Chaves Zarama
Gerente General

Jorge Jiménez
Director Financiero

Miguel Ángel Cano
Jefe de Tecnología

Cesar Ayala Pizano
Director Comercial y Operativo