	SISTEMA DE GESTIÓN - MiPG	Código: MN-GET-04
	PROCESO	Versión: 2
	GESTIÓN TECNOLÓGICA	Pág. 1 de 4
	POLÍTICA PARTICULAR USO DE CUENTAS DE USUARIO	Fecha Aprobación: 28-05-2019

## 1. Cambios efectuados

Versión	Descripción del Cambio	Fecha Aprobación
0	Procedimiento emitido en Versión 0 para prueba.	30-07-2018
1	Actualización	29-01-2019
2	Actualización encabezado, mejora redacción Política general	28-05-2019

## 2. OBJETIVO

Dar a conocer las políticas generales para el uso de las cuentas (usuario - contraseña) de acceso a los Sistemas Web del ITBOY.

## 3. ALCANCE

Esta política particular de uso de cuentas de usuario, aplica para todos los funcionarios Y contratistas, cuyas actividades de administración del sistema, de gestión o cualquier otro acceso que esté permitido para las contraseñas de sistema de los recursos del ITBOY, como: servicios Web, cuentas de correo electrónico, protectores de pantalla, en los recursos de los usuarios, administración de dispositivos remotos.


## 4. RESPONSABILIDAD

Son responsable todos los funcionarios y contratistas, que tengan creado en el sistema una cuenta de usuario y contraseña.

## 5. POLÍTICA GENERAL

- El uso de la cuenta de usuario es responsabilidad de la persona a la que está asignada. La cuenta es para uso personal e intransferible.
- La cuenta de usuario se protegerá mediante una contraseña. La contraseña asociada a la cuenta de usuario, deberá seguir los Criterios para la Construcción de Contraseñas de

	ELABORÓ:	REVISÓ	APROBÓ:
<b>NOMBRE</b>	JUAN CARLOS PUENTES GORDO	JOSE ABELARDO BECERRA PUERTO	WILLIAM DANIEL SILVA SOLANO
<b>CARGO</b>	PROF. ESPECIALIZADO	ASESOR PLANEACIÓN Y SISTEMAS	GERENTE GENERAL
<b>FECHA</b>	22-05-2019	24-05-2019	28-05-2019

	SISTEMA DE GESTIÓN - MiPG	Código: MN-GET-04
	PROCESO	Versión: 2
	GESTIÓN TECNOLÓGICA	Pág. 2 de 4
	POLÍTICA PARTICULAR USO DE CUENTAS DE USUARIO	Fecha Aprobación: 28-05-2019


acuerdo al procedimiento PD-GET-03 “Admon Usuarios Y Red.”

- Las cuentas de usuario (usuario y contraseña) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como están.
- No compartir la cuenta de usuario con otras personas: compañeros de trabajo, amigos, familiares, etc.
- Si otra persona demanda hacer uso de la cuenta de usuario hacer referencia a estas políticas. De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, deberá solicitarlo por escrito y dirigido al Administrador del Sistema.
- Si se detecta o sospecha que las actividades de una cuenta de usuario puede comprometer la integridad y seguridad de la información, el acceso a dicha cuenta será suspendido temporalmente y será reactivada sólo después de haber tomado las medidas necesarias a consideración del Administrador del Sistema.

### Tipos de Cuentas de Usuario

- Todas las contraseñas para acceso al Sistema Web con carácter administrativo deberán ser cambiadas al menos cada 6 meses.
- Todas las contraseñas para acceso al Sistema Web de nivel usuario deberán ser cambiadas al menos cada 6 meses.
- Todas las contraseñas deberán ser tratadas con carácter confidencial.
- Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea, ni vía telefónica.
- Si es necesario el uso de mensajes de correo electrónico para la divulgación de contraseñas, estas deberán transmitirse de forma cifrada.
- Se evitará mencionar y en la medida de lo posible, teclear contraseñas en frente de

	ELABORÓ:	REVISÓ	APROBÓ:
<b>NOMBRE</b>	JUAN CARLOS PUENTES GORDO	JOSE ABELARDO BECERRA PUERTO	WILLIAM DANIEL SILVA SOLANO
<b>CARGO</b>	PROF. ESPECIALIZADO	ASESOR PLANEACIÓN Y SISTEMAS	GERENTE GENERAL
<b>FECHA</b>	22-05-2019	24-05-2019	28-05-2019

	SISTEMA DE GESTIÓN - MiPG	Código: MN-GET-04
	PROCESO	Versión: 2
	GESTIÓN TECNOLÓGICA	Pág. 3 de 4
	POLÍTICA PARTICULAR USO DE CUENTAS DE USUARIO	Fecha Aprobación: 28-05-2019

otros.

- Se evitará el revelar contraseñas en cuestionarios, reportes o formas.
- 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 el activar o hacer uso de la utilidad de: ¿Recordar Contraseña? o ¿Recordar Password? de las aplicaciones.
- No se almacenarán las contraseñas en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y bajo resguardo.

No se almacenarán las contraseñas sin encriptación, en sistemas electrónicos personales (asistentes electrónicos personales, memorias USB, teléfonos celulares, agendas electrónicas).


Si alguna contraseña es detectada y catalogada como no segura, deberá darse aviso al(los) usuario(s) para efectuar un cambio inmediato en dicha contraseña.

Para efectos de las presentes políticas, se definen dos tipos de cuentas de usuario:

**1. Cuenta de Usuario de Sistema de Información:** todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información del ITBOY. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario del Sistema.

**2. Cuenta de Administración de Sistema de Información:** corresponde a la cuenta de usuario que permite al administrador del Sistema realizar tareas específicas de usuario a nivel directivo, como por ejemplo: agregar/modificar/eliminar cuentas de

	ELABORÓ:	REVISÓ	APROBÓ:
<b>NOMBRE</b>	JUAN CARLOS PUENTES GORDO	JOSE ABELARDO BECERRA PUERTO	WILLIAM DANIEL SILVA SOLANO
<b>CARGO</b>	PROF. ESPECIALIZADO	ASESOR PLANEACIÓN Y SISTEMAS	GERENTE GENERAL
<b>FECHA</b>	22-05-2019	24-05-2019	28-05-2019

	SISTEMA DE GESTIÓN - MiPG	Código: MN-GET-04
	PROCESO	Versión: 2
	GESTIÓN TECNOLÓGICA	Pág. 4 de 4
	POLÍTICA PARTICULAR USO DE CUENTAS DE USUARIO	Fecha Aprobación: 28-05-2019

usuario del sistema.

### **Criterios en la construcción de contraseñas seguras**

Una contraseña segura deberá cumplir con las siguientes características:

- La longitud debe ser al menos de 8 a 15 caracteres.
- Contener caracteres tanto en mayúsculas como en minúsculas.
- Puede tener dígitos y caracteres especiales como `_`, `-`, `/`, `*`, `$`, `¡`, `¿`, `=`, `+`, etc.
- No debe ser una palabra por sí sola, en ningún lenguaje, dialecto, jerga.
- No debe contener información personal, nombres de familia.
- Algunos ejemplos de contraseñas NO seguras por si solas: Nombres de familiares, mascotas, amigos, compañeros de trabajo, personajes.
- No utilizar cumpleaños, aniversarios, información personal, teléfonos, códigos postales, etc.
- No utilizar patrones como 1234?, aaabbb, zyxwvuts.

	<b>ELABORÓ:</b>	<b>REVISÓ</b>	<b>APROBÓ:</b>
<b>NOMBRE</b>	JUAN CARLOS PUENTES GORDO	JOSE ABELARDO BECERRA PUERTO	WILLIAM DANIEL SILVA SOLANO
<b>CARGO</b>	PROF. ESPECIALIZADO	ASESOR PLANEACIÓN Y SISTEMAS	GERENTE GENERAL
<b>FECHA</b>	22-05-2019	24-05-2019	28-05-2019