# POLITICA PARA LA SEGURIDAD DE LA INFORMACION Y CONTROL DE ACCESO DE LA CORPORACIÒN PARA EL DESARROLLO SOCIAL Y CULTURAL DEL VALLE DEL CAUCA "CORPOVALLE"

## 1. INTRODUCCION:

Mediante el presente documento, LA CORPORACIÓN PARA EL DESARROLLO SOCIAL Y CULTURAL DEL VALLE DEL CAUCA "CORPOVALLE", define las políticas y normas para garantizar un adecuado uso de la información, control de acceso a los sistemas de información y en general a las herramientas dispuestas por la entidad para el desarrollo de las funciones propias de cada colaborador, contratista o tercero que tenga acceso a ellas, además se articula con la *Política de Protección de Datos Personales* de la entidad, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la Ley 1581 de 2012, para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información personal, que son de obligatorio acatamiento por parte de los destinatarios de esta políticas.

## 2. OBJETIVOS

- Impedir el acceso no autorizado a los sistemas de información físicos y lógicos.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Generar cultura a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la Ley 1581 de 2012.

## 3. ALCANCE

Las políticas y normas definidas en este documento aplican para todos los funcionarios, contratistas y terceros que tengan acceso a los sistemas de información de la empresa LA CORPORACIÓN PARA EL DESARROLLO SOCIAL Y CULTURAL DEL VALLE DEL CAUCA "CORPOVALLE".

## 4. RESPONSABILIDADES

### 4.1 Responsable de Seguridad de la Información



**Calle 11 No. 3-58 Edificio Citibank Oficinas 604-608**
**Teléfono: +57 (2) 8818079**
**www.corpovalle.co**
**info@corpovalle.co**

- Sugerir procedimientos para la asignación de acceso a los sistemas, bases de datos y servicios de información multiusuario; la solicitud y aprobación de acceso a Internet o redes externas; el uso de computación móvil, trabajo remoto.
- Analizar y sugerir medidas a ser implementadas para hacer efectivo el control de acceso de los usuarios a servicios como Internet, red interna entre otros.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de acceso, creación de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, uso controlado de software del sistema y correo electrónico institucional y/o herramientas colaborativas.

### 4.2 Propietarios de Información

Evaluar los riesgos a los cuales se expone la información con el objeto de:

- Clasificar la información
- Determinar los controles de acceso, autenticación y utilización a ser implementados en cada caso.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Revisar periódicamente los procesos de acceso a la información.

### 4.3 Líderes de Procesos o Jefes de Área

- Autorizar el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, acatando las normas vigentes.
- Así mismo autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red, Internet, acceso al archivo físico, correo electrónico institucional y les herramientas colaborativas para labores explícitas del cumplimiento de sus funciones.

### 4.4 Representante Legal

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.



**Calle 11 No. 3-58 Edificio Citibank Oficinas 604-608**
**Teléfono: +57 (2) 8818079**
**www.corpovalle.co**
**info@corpovalle.co**

- Evaluar el costo y el impacto de la implementación de recursos de seguridad física para los archivos tangibles.
- Evaluar el costo y el impacto de la implementación de sistemas informáticos de seguridad.

## 5. POLITICAS GENERALES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

### 5.1 Políticas

- Deben establecerse medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y archivos físicos. Los controles de acceso deben ser conocidos por todos los empleados de LA CORPORACIÓN PARA EL DESARROLLO SOCIAL Y CULTURAL DEL VALLE DEL CAUCA "CORPOVALLE", y limitar el acceso hacia los activos de información de acuerdo con las responsabilidades del cargo.
- Se deben implementar procedimientos para la asignación de acceso a los sistemas de información, bases de datos y archivo físico.

### 5.2 Normas

#### 5.2.1 Control de Acceso

Los controles de acceso deberán contemplar:

- Requerimientos de seguridad de cada una de las aplicaciones.
- Definir los privilegios de acceso de los usuarios a las aplicaciones de acuerdo a su perfil de cargo en la entidad.
- Para el caso de los archivos físicos, solo podrán accesar los usuarios autorizados por el Representante Legal y con uso restringido a la competencia de las funciones de quien accede a los registros.

#### 5.2.2 Uso del Archivo Físico

- El Representante Legal establece procedimientos para permitir que los empleados de la empresa accedan al archivo físico que esta mantiene.
- Solo podrán acceder al archivo físico, los empleados previamente autorizados y no podrán generar copias o reproducciones de documentos sin autorización expresa del Representante Legal.
- Todo acceso al archivo y reproducción de documentos, solo se permitirá para casos asociados con el desarrollo de las funciones y del objeto social de la entidad.



**Calle 11 No. 3-58 Edificio Citibank Oficinas 604-608**
**Teléfono: +57 (2) 8818079**
**www.corpovalle.co**
**info@corpovalle.co**

- Solo se podrán efectuar variaciones a la norma en caso de mandato judicial.

### 5.2.3 Administración de Accesos de Usuarios

El Representante Legal establece procedimientos para controlar la asignación de derechos de acceso a los sistemas, datos y archivo físico.

### 5.2.4 Creación de Usuarios

- El Representante Legal, deberá mantener los registros donde cada uno de los líderes responsables de los procesos o Jefes de área, haya autorizado a los empleados el acceso a los diferentes sistemas de información de la entidad.
- Los datos de acceso a los sistemas de información deberán estar compuestos por un nombre de usuario y contraseña que debe ser único por cada empleado.
- Cuando se retire o cambie de contrato cualquier empleado, se deberá aplicar la eliminación o cambios de privilegios en los sistemas de información a los que el usuario estaba autorizado.
- El funcionario responsable de seguridad de la información deberá realizar revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los empleados, manteniendo los registros de las revisiones y hallazgos.

### 5.2.5 Administración de Contraseñas de Usuario

- Las contraseñas de acceso deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, en lo posible utilizar caracteres especiales.
- Todos los empleados deberán cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia mínima de 6 meses.
- Los sistemas de información deberán bloquear permanentemente al usuario luego de 5 intentos fallidos de autenticación.

### 5.2.6 Uso de Contraseñas

Los usuarios deben cumplir las siguientes normas:

- Mantener los datos de acceso en secreto.

Contraseñas que no sean fáciles de descifrar o intuir y no tenerlas escritas.



**Calle 11 No. 3-58 Edificio Citibank Oficinas 604-608**
**Teléfono: +57 (2) 8818079**
**www.corpovalle.co**
**info@corpovalle.co**

- Que las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo: nombres, número de cédula, números de teléfono, fecha de nacimiento, etc.

- Notificar de acuerdo a lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

### 5.2.7 Control de Acceso a la Red

El funcionario responsable de seguridad de la información deberá asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la empresa mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Excepciones de acceso, serán aprobados por el Representante Legal, según la necesidad del cargo y verificación previa de que las paginas solicitadas no contengan código malicioso con el visto bueno del oficial de seguridad de la información.

### 5.2.8 Autenticación de Usuarios para Conexiones Externas

LA CORPORACIÓN PARA EL DESARROLLO SOCIAL Y CULTURAL DEL VALLE DEL CAUCA "CORPOVALLE", solo permitirá acceso remoto mediante herramientas informáticas aprobadas por el Representante Legal y su acceso solo podrá ser autorizado por el Administrador General.

### 5.2.9 Control de Conexión a Redes

La infraestructura de LA CORPORACIÓN PARA EL DESARROLLO SOCIAL Y CULTURAL DEL VALLE DEL CAUCA "CORPOVALLE", deberá estar definida por una red general con acceso privado para garantizar la confidencialidad de los datos que se transmitan.

### 5.2.10 Seguridad en los Servicios de Red

- Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la entidad.

- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la entidad.

### 5.2.11 Control de Identificación y Autenticación de Usuarios.

Todos los usuarios tendrán un identificador único de usuario solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.



**Calle 11 No. 3-58 Edificio Citibank Oficinas 604-608**
**Teléfono: +57 (2) 8818079**
**www.corpovalle.co**
**info@corpovalle.co**

### 5.2.12 Sistema de Administración de Contraseñas

El sistema de administración de contraseñas debe:

- Obligar el uso de Usuarios y contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de las mismas o cuando consideren que la misma ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Los usuarios deben cambiar las contraseñas provisionales o que han sido asignadas por el funcionario responsable de seguridad de la información.
- No permitir mostrar las contraseñas en texto claro cuando son ingresadas.
- Almacenar las contraseñas en forma cifrada.

### 5.2.13 Sesiones Inactivas

- Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que Terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.
- Si los sistemas de información detectan inactividad por un periodo igual o superior a diez minutos, deben automáticamente aplicar, "timeout" es decir, finalizar la sesión de usuario

Las anteriores políticas en su versión No. 1 entran en vigencia a partir del 15 de noviembre de 2018, fecha de aprobación del Director de Proyectos de LA CORPORACIÓN PARA EL DESARROLLO SOCIAL Y CULTURAL DEL VALLE DEL CAUCA "CORPOVALLE".



**Calle 11 No. 3-58 Edificio Citibank Oficinas 604-608**
**Teléfono: +57 (2) 8818079**
**www.corpovalle.co**
**info@corpovalle.co**