1 OBJETIVO

Proteger la integridad de la información de la empresa.

2 ALCANCE

Aplica para todas las sedes.

3 RESPONSABLE

Jefe de Sistemas y Mantenimiento.

4 Riesgos

Robo, pérdida o alteración de la información.

5 DESCRIPCION DEL PROCEDIMIENTO

N°	Descripción	Responsable	Registro
1	Necesidad de protección de la información	• Gerente • Ingeniero proveedor	• E-mail • Comité
2	Instalación de Antivirus, éste incluye protección contra todo tipo de malware. Se llama "Malware" a todo archivo con contenido de carácter malicioso para un equipo informático. El software utilizado ofrece protección contra los siguientes tipos de malware: • **Virus**: destruyen información y se reproducen automáticamente. • **Gusanos**: se copian y se envían masivamente desde un ordenador infectado a todos los miembros de la lista de direcciones. • **Troyanos**: abren puertas de acceso a un hacker que puede realizar remotamente cualquier tipo de actividad en el equipo afectado.	• Jefe de Sistemas y Mantenimiento	• Cotizaciones • Correos indicativos • Informes de la aplicación.

	• **Spyware**: extraen información personal almacenada en un ordenador. • **Phishing**: Es el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, de entidades bancarias), tratan de conseguir datos confidenciales del usuario. Suelen incluir un enlace que lleva a páginas web falsificadas. Así, el usuario, cree estar en un sitio de confianza e introduce la información que, en realidad, llega a manos del estafador. • **Amenazas combinadas**: Las últimas epidemias se han caracterizado por ataques combinados de varias amenazas a la vez o lo que se conoce como "blended threats". • **Dialers**: marcan números de teléfono de pago automáticamente y sin permiso del usuario. • **Jokes**: bromas que hacen perder el tiempo a los usuarios. • **Hacking tools** son todas aquellas herramientas que se puedan utilizar para robar información, accesos no permitidos, etc. • **Security risks** son aplicaciones que suponen una amenaza clara para la seguridad, y que sin embargo no pueden ser catalogados como virus. Por ejemplo, un programa dedicado a la creación de virus o troyanos.		
3	Existen además otros controles que son: • Firewall en todos los equipos de cómputo y en el router. • No contamos con VPN, sin embargo nuestra red privada tiene controles de acceso y solo puede ser usada en el equipo en el que está configurada. • Switch administrable (reemplaza el router), que permite administrar los anchos de banda, restringir accesos a internet, bloqueo de puertos, bloqueo por mac adress, detección de intrusos. • Puertos abiertos direccionados virtualmente, para aplicaciones que ingresan del exterior. • Directorios compartidos dentro de la red privada, con restricciones de acuerdo a la seguridad definida por cada proceso.	•	• Informes de la aplicación. • Reporte del equipo.

	• Inactivación de cuentas de correo y usuarios del software, al momento de terminar la relación laboral con un funcionario. • Registro de logs en el software de la empresa y en todos los aplicativos anexos.		
4	Adicionalmente se establecen acciones preventivas para la protección de la información, como las siguientes: • Campaña de uso de contraseñas seguras (alfanuméricas de 8 dígitos). • Bloqueo automático de equipos por inactividad, en la sede principal Pereira. Se requiere clave de acceso al equipo. • Protección de la base de datos con encriptamiento y contraseñas de uso confidencial. • Garantía de protección del código fuente por parte del proveedor del sistema.	•	• Registro de Inducción. • Registro de Capacitación. • Registro de claves de acceso a equipos. • Registro de claves de acceso al software.
5	Mantener actualizados los procedimientos y los sistemas de protección	• Jefe de Sistemas y Mantenimiento	• Correos

ELABORADO	**REVISADO**	**APROBADO**
Ana María Jiménez Trujillo Asistente de sistemas de gestión y recursos humanos	Paola Cardona Martínez	Lucas Cardona Martínez
Lucas Cardona Martínez Jefe de Sistemas y Mantenimiento	Coordinadora Administrativa	Jefe de Sistemas y Mantenimiento
09/02/2015	10/02/2015	10/02/2015