Procedimientos para prevenir el acceso no autorizado a la destrucción de documentos y registros (incluyendo programas de computación y archivos de datos).

Los datos almacenados en forma de bases de datos, archivos de correo plano, archivos de configuración, y archivos de contenido web solamente pueden ser accesados directamente mediante el conocimiento de las contraseñas y usuarios que poseen acceso a dichos archivos, así como la cuenta de súper usuario administrativo, cualquier acceso no autorizado implica el hecho de un ataque a los sistemas de seguridad de CIMAV, o una usurpación de contraseñas.

El procedimiento de prevención de destrucción de documentos es el siguiente:

- Mantener copia de respaldo de al información.
- Contraseña de súper usuario de muy alta complejidad.
- Contraseñas de usuario de los sistemas y aplicaciones de seguridad alta a intermedia.
- Contraseñas de los administradores de sistemas y aplicaciones de alto nivel de complejidad.
- Restricción del numero de usuarios administradores de sistemas al mínimo indispensable.
- Control de intrusos mediante muro de fuego (firewall) en cada sistema y restricción de conexiones autorizadas.