

Política de Control de acceso

Introducción

El principio básico es el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios.

Está permitido el acceso a todos los sectores físicos de la organización, excepto a aquellos para las cuales el privilegio debe ser concedido por una persona autorizada (punto "Gestión de privilegios").

- a) Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- b) Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- c) Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.
- d) Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- e) Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- f) Garantizar la seguridad de la información cuando se utiliza trabajo remoto.

Para cada perfil dispondrá unos requisitos de control de acceso tanto a la información como al entorno de trabajo.