

Sistemas de seguridad y proteccion.

231011 Kevin Antonio Andrade Lopez



Universidad tecnologica de aguascalientes

**¿Qué son los protocolos básicos de seguridad personal en la infraestructuras de redes?**  
Los protocolos de seguridad en infraestructuras de redes son como los guardianes digitales que protegen la información y garantizan que los datos viajen de manera segura. Sin ellos cualquier persona podría tener acceso a nuestros datos y muy posiblemente hacer uso de ellos de forma no autorizada y con intenciones de darles un mal uso.

1. **Uso de contraseñas seguras**:
   * Establecer contraseñas robustas es crucial. Recomiendo combinar letras mayúsculas y minúsculas, números y caracteres especiales.
   * Cambiar las contraseñas periódicamente ayuda a prevenir accesos no autorizados. Imagina que nuestras contraseñas son como las llaves de nuestra casa: si no las cambiamos, cualquiera podría tener acceso.
2. **Actualización de software y firmware**:
   * Mantener los sistemas operativos, aplicaciones y dispositivos actualizados es como cerrar las brechas en una cerca. Las actualizaciones corrigen vulnerabilidades conocidas.
   * No subestimes la importancia de parchear y actualizar. Es como mantener tu coche en buen estado para evitar problemas en la carretera.
3. **Autenticación de múltiples factores (MFA)**:
   * Aquí estamos hablando de “doble candado”. Además de la contraseña, se requiere una segunda forma de autenticación, como un código SMS o una aplicación de autenticación.
   * Piensa en ello como cuando necesitas tanto la tarjeta de crédito como tu huella digital para comprar algo costoso.
4. **Control de acceso basado en roles (RBAC)**:
   * Asignar permisos específicos según el rol del usuario es como dar diferentes niveles de acceso en una empresa. El gerente tiene acceso a más áreas que el becario.
   * Esto evita que alguien pueda meterse donde no le corresponde. Imagina a un extraño entrando en la sala de juntas sin permiso.
5. **Firewalls y segmentación de red**:
   * Los firewalls son como los guardianes de la puerta. Filtran el tráfico y bloquean amenazas.
   * La segmentación divide la red en zonas. Es como tener diferentes vecindarios en una ciudad. Si hay un incendio en uno, no afecta a los demás.
6. **Monitoreo y registro de eventos (logging)**:
   * Registrar eventos y actividades es como tener una cámara de seguridad en tu casa. Si algo raro sucede, puedes revisar las grabaciones.
   * Detectar anomalías temprano es clave. Imagina que alguien intenta abrir tu caja fuerte; querrías saberlo al instante.
7. **Cifrado de datos**:
   * El cifrado es como poner tus secretos en un sobre sellado antes de enviarlos por correo. Nadie más debería poder leer lo que hay dentro.
   * Algoritmos criptográficos hacen esto posible. Son como los códigos secretos que usaban los espías en las películas antiguas.
8. **Educación y concienciación**:
   * Capacitar a los usuarios es como enseñarles a manejar un coche. Deben saber las reglas y cómo evitar accidentes.
   * La seguridad no solo es cosa de expertos. Todos debemos estar informados.
9. **Respuesta a incidentes**:
   * Tener un plan para manejar situaciones de seguridad es como tener un extintor en casa. Esperamos no necesitarlo, pero si hay un incendio, sabemos qué hacer.
   * Imagina que alguien intenta hackear tu cuenta de correo. ¿Qué pasos seguirías?
10. **Auditorías y pruebas de penetración**:
    * Evaluar regularmente la seguridad de la red es como hacerle un chequeo médico anual. Detectamos problemas antes de que se conviertan en crisis.
    * Las pruebas de penetración son como simular ataques controlados. Es como si un ladrón intentara entrar a tu casa para ver si encuentra alguna debilidad.

**Reflexión personal:**

En estos días es crucial tener un control de los accesos a nuestra data, es necesario exponerle a todos lo vulnerables que pueden llegar a ser tanto nuestros datos como nuestra información. El manejo de un buen control de acceso es crucial, en caso de que fuese un centro de datos no nos gustaría que cualquier persona pudiera acceder, leer o manipular la información. Caso similar seria el acceso a un panel de control de administrador de cualquier sistema operativo, ya que tendría total control del sistema y darle un uso no adecuado.