PROTOCOLO DE SEGURIDAD DE MANEJO DE LA INFORMACIÓN

CONCEJO DE SABANETA.

2024.

OBJETIVO

Los protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información.

Estos protocolos buscan evitar que usuarios no autorizados obtengan datos confidenciales o los modifiquen.

DESCRIPCIÓN DE LOS PROCESOS:

Los protocolos de seguridad informática son conjuntos de normas y reglas diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información en entornos digitales1. Estos protocolos buscan evitar que usuarios no autorizados obtengan datos confidenciales o los modifiquen. Aquí tienes algunos aspectos clave sobre ellos:

PRICIPALES PROCESOS APLICABLES:

1. **Autenticación de usuarios**: Este elemento es crucial e implica la gestión de identidades de los usuarios. Se verifica que la persona que solicita acceso a la información sea la correcta, evitando fraudes como la suplantación de identidad.

2. **Cifrado de datos**: Los sistemas utilizan el cifrado para encriptar la información que se transmite entre usuarios, evitando que sea interceptada en el camino.(TCP/IP)

3. **Organización de datos**: Se refiere a cómo se almacena la información del usuario para que pueda utilizarse cuando sea necesario.

PROCESOS IMPLEMENTADOS

1. **Capacitación del personal**: Se educa a tus empleados sobre buenas prácticas de seguridad informática. Esto incluye cómo manejar contraseñas, identificar correos electrónicos sospechosos y proteger datos sensibles.

2. **Copia de seguridad regular**: Se realiza copias de seguridad periódicas de los datos críticos de tu empresa. Almacénalas en ubicaciones seguras y verifica su integridad, este proceso esta para las dos área (jurídica y gestión documental)

3. **Controles de acceso rigurosos**: Se limita el acceso a la información solo a quienes lo necesiten. Usa contraseñas fuertes y el proceso de seguridad de las contraseñas se maneja a través del servidor (directorio Activo)

4. **Software antimalware**: Se instala y actualiza regularmente software de seguridad, como antivirus y antimalware, en todos los dispositivos, la seguridad esta definida desde el servidor principal

5. **Evitar correos electrónicos sospechosos:** Se capacita a tus empleados para que no abran enlaces o archivos adjuntos de correos electrónicos desconocidos o sospechosos.

Nota: Ante alguna sospecha o evidencia de malos procedimientos en el manejo de la información, se debe realizar la alerta al personal de tecnología (concejo) o tecnología del municipio (correo).

IT Concejo: Anderson Niño Mora Email: sabaneta.concejoit@gmail.com