2 de diciembre de 2017

Sena

Adsi

1181639

Mecanismos de control y seguridad

Andres david gonzalez betancourt

## 1. SEGMENTACIÓN DE PROCESOS, PERFILES Y ROLES:

En el mundo en el que vivimos cada día las conexiones son más agiles y lo que antes era una conexión de 30 segundos entre países hoy es de 2 segundos entre continentes y al acceder en la web a cualquier página no nos percatamos de la cantidad de saltos que hacen los paquetes para llegar a nosotros y los aplicativos web siempre son propensos a ataques ya que en ellos se almacena información importante.

La segmentación se realizará en 3 partes. La primera será los superadministradores o root que serán quienes tengan acceso en profundidad al sistema, bases de datos, código del aplicativo y demás esto para el tema de soporte técnico y configuraciones.

El segundo segmento serán los administradores locales que serán los usuarios Admin, estos usuarios tendrán permisos en el aplicativo para crear usuarios comunes, asignar permisos y demás todo esto sin afectar el funcionamiento del aplicativo.

Finalmente están los usuarios comunes y tendrán permisos básicos para realizar sus labores.

## 2. MECANISMO DE AUTENTICACIÓN A IMPLEMENTAR EN EL SISTEMA:

Nuestro sistema es un sistema web e indiferente de que su implementación sea local o en la nube la autentiacion será clásica con nombre de usuario y contraseña más un captcha. Estos datos de usuario y contraseña están almacenados en la tabla users de la base de datos a la cual solo tienen acceso los usuarios root.

## 3. CIFRADO DE DATOS: TIPO DE ALGORITMOS A IMPLEMENTAR.

El envío de información al servidor se realizará por el código post y no get en php para que no sea visible la información por parte del usuario o terceros, Adicional a esto se pondrá un captcha para evitar ataques de bots y las contraseñas no serán visibles siendo reemplazados los caracteres por asterisco. Cuando se reciba la contraseña se realizará validación MD5 por parte del servidor.

## 4. PROCEDIMIENTOS ADICIONALES DE SEGURIDAD A IMPLEMENTAR

Para fortalecer la seguridad del sistema de información las contraseñas tendrán una caducidad cada 3 meses. La primera letra deberá ser en mayúscula, no podrá ser menor a 8 caracteres y deberá contener un número.