

San Juan de Pasto, 25 de Septiembre de 2024

Señores:
COACREMAT

Cordial Saludo,

Según la solicitud para realizar mejoras en la seguridad del sitio web enviamos la siguiente propuesta describiendo las recomendaciones que se propone implementar.

PROPUESTA TÉCNICO – FINANCIERA MEJORAS DE SEGURIDAD

- ❖ Captcha en formularios
- ❖ Autenticación y autorización seguras
 - Bloqueo de cuenta: Bloquear cuentas después de varios intentos fallidos de login
- ❖ Cifrado más fuerte de contraseñas
- ❖ Validación y filtrado de entradas
 - Verificar la validación de datos y el filtrado de entradas para evitar inyecciones SQL, XSS y otros tipos de ataques.
 - Verificar que el contenido que se está generando dinámicamente en las interfaces de vistas esté funcionando adecuadamente para evitar vulnerabilidades XSS.
- ❖ Protección contra CSRF (Cross-Site Request Forgery)
- ❖ Registro y monitoreo de eventos
 - Implementar un sistema de logging para registrar intentos fallidos de login, cambios en la configuración del sistema y otros eventos importantes.
 - Utilizar herramientas como `monolog` o la integración con logs para monitorear actividad sospechosa.
- ❖ Protección contra ataques de fuerza bruta
 - Limitar el número de intentos de inicio de sesión por usuario o dirección IP.
 - Implementar tiempos de espera progresivos en caso de múltiples intentos fallidos.
- ❖ Seguridad en sesiones
 - Usar identificadores de sesión aleatorios y regeneración de sesión después del login.
 - Configurar cookies de sesión con la opción `HttpOnly` y `Secure` para evitar que sean accesibles mediante scripts y sólo se envíen sobre HTTPS.
- ❖ Verificar protección contra inyecciones SQL
- ❖ Verificar que las dependencias se encuentre debidamente actualizadas para asegurar protección contra vulnerabilidades recientes

Total Inversión: \$ 2.900.000 (Forma de pago: 50% para iniciar y 50% a la entrega final)

Atentamente,

DIANA FLOREZ BRAVO
Ingeniera de Sistemas
Aplicaciones Web y Móvil