VERIFICACIÓN DE CIBERSEGURIDAD PARA NUEVOS PROVEEDORES

Nombre del Proveedor:
Nombre del Responsable de TI:
Responsable Técnico de TI: **Email:**

Por favor, responda las preguntas a continuación.

	PREGUNTA	RESPUESTA
1.	¿Su empresa tiene una Política de Uso Aceptable (AUP) de ciberseguridad que se aplica y comunica a todos los usuarios/empleados?	
2.	¿Su empresa aplica reglas de complejidad de contraseñas para todos los usuarios/empleados en los sistemas de la empresa?	
3.	¿Su empresa utiliza autenticación multifactor (MFA) para todos los usuarios/empleados?	
4.	¿Su empresa permite conexiones VPN a su entorno? Si es así, ¿se aplica la autenticación multifactor (MFA) para todas las conexiones VPN?	
5.	¿Su empresa tiene un programa formalizado de entrenamiento en ciberseguridad para todos los usuarios/empleados?	
6.	¿Su empresa permite que los usuarios/empleados usen emails personales para realizar negocios de la empresa? (por ejemplo, Gmail, Yahoo, etc.)	
7.	Por favor, describa cómo su empresa maneja la aplicación de parches y actualizaciones de seguridad para sus servidores y endpoints	
8.	¿Su empresa utiliza un antivirus gestionado en las computadoras de la empresa? Si es así, ¿cómo se actualiza? ¿Se realizan escaneos y remediaciones automáticas? Si es así, ¿con qué frecuencia?	
9.	¿Las tecnologías Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) y Domain-based Message Authentication Reporting and Conformance (DMARC) están implementadas en su servidor de correo electrónico? Si es así, ¿Que configuraciones definidas para cada una?	
10.	¿Puede su empresa registrar el dominio de correo electrónico de Wellbore Integrity Solutions: wellboreintegrity.com en el Sender Policy Framework (SPF)?	
11.	¿Su empresa tienes un sistema de protección de correos electrónicos que inspecciona todos los correos recibidos?	
12.	¿Su empresa tienes su propio dominio de correo electrónico?	
13.	¿Su empresa habilita firewalls en todas las computadoras?	
14.	¿Su empresa tienes un plan de gestión y escalamiento de incidentes de ciberseguridad que informa a los clientes sobre incidentes dentro de las 24-48 horas del evento?	