Informe de evaluación de riesgos de seguridad

|  |
| --- |
| **Parte 1: Selecciona hasta tres herramientas y métodos de reforzamiento a implementar** |
| Debido a la reciente filtracion de datos se descubrio vulnerabilidades en el sistema de seguridad, las cuales son: Los empleados de la organización comparten las contraseñas, La contraseña del administrador de la base de datos es la predeterminada, Los firewalls no tienen reglas establecidas para filtrar el tráfico que entra y sale de la red y No se utiliza la autenticación multifactor (MFA).  Implementar medidas de seguridad para reforzar y cubrir estas vulnerabilidades sera escencial para evitar un posible incidente de este tipo a futuro.  Firewall: configurar un firewall con reglas que impidan la exfiltracion de datos.  Politicas de contraseñas: remplazar la contraseña predeterminada Autentificacion Multifactor: Al manejar datos sencibles todos los involucrados con el acceso a este tipo de informacion implementar la MFA.  Herramienta SIEM: monitorear constantemente el trafico de datos de la red. |
|

|  |
| --- |
| **Parte 2: Explica tus recomendaciones** |
| Firewall. Algunos firewalls avanzados tienen capacidades de IDS/IPS que pueden identificar y bloquear ataques en tiempo real. Configurar el firewall para bloquear paquetes especificos segun las politicas de seguridad. permiten establecer políticas específicas para diferentes aplicaciones, usuarios o grupos dentro de la organización (en este caso para algunos usuarios).  Politicas de contraseñas. Ante todo remplazar la contraseña predeterminada y aplicar un correcto uso de politicas de contraseñas como longitud minima, ej una regla que haga que la contraseña tenga un minimo de 12 caracteres, la complejidad hara que una contraseña se estructure con ciertas reglas, ej que una contraseña contenga caracter especial, una mayuscula, un numero, realizar una validacion con regex seria una buena opcion para que cumpla con criterios de complejidad. Inlusión de capacidades IDS/IPS en un firewall permite detectar y prevenir intrusiones de manera efectiva, proporcionando una capa adicional de defensa contra amenazas conocidas y desconocidas, es posible a través de la monitorización en tiempo real.  Autentificacion multifactor (MFA) Reforzar la seguridad con MFA conseguira que no cualquier persona pueda acceder de manera sencilla a la red, ej si una persona lograse obtener la contraseña de un panel administrativo aun le faltaria tener acceso al segun factor de autentificacion el cual puede ser reconocimiento facial, huella digital, sms, correo electronico de confirmacion, etc. |