**Informe de evaluación de riesgos de seguridad**

|  |
| --- |
| **Parte 1: Seleccione hasta tres herramientas y métodos de fortalecimiento para implementar** |
| Se han identificado los siguientes riesgos en la organización:   * Los empleados comparten contraseñas. * La contraseña del administrador de la base de datos permanece con valores predeterminados. * Los cortafuegos carecen de reglas de filtrado de tráfico entrante y saliente. * No se utiliza autenticación multifactor (MFA).   Con base en lo anterior, se recomienda implementar las siguientes herramientas y métodos para fortalecer el uso de credenciales:   1. **Autenticación multifactor (MFA/2FA):**  Permite agregar una capa adicional de seguridad, garantizando que el acceso a las cuentas no dependa únicamente de una contraseña, sino también de un segundo factor de verificación (token, aplicación móvil, SMS, correo o llave física). 2. **Gestores de contraseñas empresariales:**  Implementar herramientas como **Bitwarden Enterprise, 1Password Business, LastPass Business o Dashlane Business** para la generación y gestión de contraseñas fuertes. Estas soluciones ofrecen contraseñas aleatorias y complejas, evitando que los colaboradores reutilicen claves débiles. Se recomienda instruir a los usuarios para que personalicen levemente las claves generadas, evitando la dependencia total de diccionarios automáticos. 3. **Políticas avanzadas de contraseñas en Active Directory / LDAP:**  Establecer reglas obligatorias para la creación de contraseñas seguras, con una longitud mínima de 16 caracteres, combinando mayúsculas, minúsculas, números y caracteres especiales. Esto fomenta la cultura de seguridad y reduce la probabilidad de credenciales vulnerables. |
|  |

|  |
| --- |
| **Parte 2: Explique sus recomendaciones** |
| Las recomendaciones propuestas buscan **reducir los riesgos humanos y técnicos asociados al mal uso de credenciales** y al mismo tiempo **fomentar la concienciación en ciberseguridad**.   * **Autenticación multifactor (MFA):**  Incluso si un colaborador compartiera su contraseña, esta no sería suficiente para acceder al sistema sin el segundo factor de autenticación. Su implementación debe acompañarse de políticas claras que prohíban el intercambio de credenciales entre empleados. * **Gestores de contraseñas empresariales:**  Facilitan a los usuarios la creación y almacenamiento de claves robustas, reduciendo la necesidad de memorizar contraseñas complejas. Con una adecuada capacitación, los colaboradores aprenderán a generar y modificar contraseñas seguras, lo que incrementa significativamente la resistencia ante ataques de fuerza bruta o filtraciones. * **Políticas avanzadas en Active Directory / LDAP:**  Refuerzan de manera obligatoria la seguridad en la creación de nuevas credenciales, minimizando el riesgo de contraseñas débiles o fáciles de adivinar. Su implementación, junto con la capacitación a los empleados, asegura que las buenas prácticas en seguridad se conviertan en parte integral de la cultura organizacional. |