Plan de Contingencia

1. **Identificación de riesgos:**

- Acceso no autorizado: Posible intento de acceso al sistema por personas no autorizadas.
- Ataques de fuerza bruta: Intentos repetidos de adivinar contraseñas para acceder al sistema.
- Robo o filtración de credenciales: Posibilidad de que las credenciales de inicio de sesión sean robadas o filtradas.
- Vulnerabilidades de seguridad: Identificación de posibles vulnerabilidades en el sistema que podrían ser explotadas.

2. **Medidas preventivas:**

- Políticas de contraseñas: Establecer requisitos para las contraseñas, como longitud mínima, uso de caracteres especiales y cambios periódicos.
- Autenticación multifactor (MFA): Implementar la autenticación en dos pasos o factores adicionales para aumentar la seguridad del login.
- Auditorías de seguridad: Realizar auditorías periódicas del sistema para identificar posibles vulnerabilidades.
- Actualizaciones y parches: Mantener el sistema y todos sus componentes actualizados con las últimas correcciones de seguridad.
- Capacidad de bloqueo de cuentas: Permitir el bloqueo temporal de cuentas después de varios intentos de inicio de sesión fallidos.
- Cifrado de contraseñas: Almacenar las contraseñas de los usuarios de forma segura utilizando algoritmos de cifrado robustos.

3. **Respuesta a incidentes:**

- Monitoreo de actividades sospechosas: Implementar sistemas de monitoreo para detectar actividades inusuales o intentos de acceso no autorizado.
- Procedimientos de bloqueo y desactivación: Establecer procedimientos claros para bloquear y desactivar cuentas comprometidas o sospechosas.
- Notificación de incidentes: Definir el proceso para notificar a los usuarios afectados en caso de una brecha de seguridad.
- Investigación y mitigación: Establecer un equipo de respuesta ante incidentes para investigar y mitigar cualquier brecha o ataque.

4. **Comunicación:**

- Comunicación interna: una cadena de comunicación clara entre el equipo de TI, el equipo de seguridad y la gerencia para responder rápidamente a incidentes de seguridad.

- Comunicación externa: Definir el proceso de comunicación con los usuarios afectados y las autoridades pertinentes en caso de un incidente de seguridad grave.

5. **Recuperación:**

- Restauración de datos: Tener un plan de respaldo y recuperación para restaurar datos y sistemas en caso de pérdida o daño.
- Evaluación post-incidente: Realizar una revisión exhaustiva después de cualquier incidente para aprender lecciones y mejorar la seguridad en el futuro.

6. **Capacitación y concienciación:**

- Capacitación del personal: Capacitar a los empleados en buenas prácticas de seguridad informática y la importancia de proteger las credenciales de inicio de sesión.
- Concientización de usuarios: Informar a los usuarios sobre las últimas amenazas de seguridad y cómo proteger sus cuentas.