



## Plan de contingencia

### PLC-RSK-06 (Incendio del Site):

1. Comunicarse con la aseguradora.
2. Realizar una evaluación de los daños físicos (pérdidas).
3. Realizar un reporte de los daños que sufrió la aplicación; donde se narra todo aquello que provoque un retraso, como pérdida de información, pérdida del servidor y equipos.
4. Realizar un plan de acción para solucionar el problema; en los que se busca reponer las pérdidas inmediatamente y recuperar el tiempo perdido por este incidente.
5. Comunicarse con el cliente para notificarle la situación ocurrida.

### PLC-RSK-12 (Falta de Seguridad):

1. Mantener la calma.
2. En caso de ser un trabajador, notificar a los superiores.
3. Realizar investigación pertinente de los archivos; saber que archivos fueron filtrados.
4. Buscar la brecha de seguridad que hace vulnerable al servidor.
5. Seguir rastro del hacker y notificar a las autoridades.
6. Hacer un parche del servidor para evitar que vuelva a ser vulnerable ante hackeos.
  - a. Se debe tomar en cuenta que habrá pérdida de información y se debe tratar de perder la menor información posible.

### PLC-RSK-14 (Incumplimiento del Contrato de Confidencialidad):

1. Buscar y encontrar al responsable del acto.
2. Contactar a las autoridades.
3. Realizar una demanda en contra del responsable.
4. Buscar una solución a los daños que realizó el responsable.