Cuestionario de evaluación de Seguridad de la Información

1. Seguridad de la Información Organizacional

1. ¿Cuenta la organización con un miembro dedicado exclusivamente a funciones de seguridad de la información?

2. ¿Se requiere una verificación de antecedentes para todos los empleados que acceden o manejan datos de la organización?

3. ¿La organización cuenta con políticas escritas de seguridad de la información?
3.1. Si la respuesta es afirmativa, favor de adjuntar copias al responder este cuestionario.

4. ¿Existe una política formal de contraseñas que detalle los requisitos de estructura de las mismas?
4.1. ¿Cómo se verifica la fortaleza de las contraseñas?

5. ¿El personal recibe capacitación sobre concienciación en seguridad de la información?

6. ¿La organización cuenta con una copia de la Política de Acceso a Datos de la Empresa y está dispuesta a cumplir con estas directrices?

7. ¿Existe un proceso formal de gestión de cambios para modificaciones en TI?

8. ¿La organización ha implementado un marco de gobierno de TI como ITIL o ISO 27001?

9. ¿Su empresa procesa pagos con tarjetas de crédito en nombre de la empresa?
9.1. Si la respuesta es afirmativa, ¿cumple con la normativa PCI DSS?

2. Seguridad General

10. ¿Se encuentra instalado software antivirus en los servidores que procesan datos?

11. ¿Se encuentra instalado software antivirus en las estaciones de trabajo?

12. ¿Se aplican parches de seguridad y actualizaciones a las estaciones de trabajo de manera rutinaria?

13. ¿Se aplican parches de seguridad y actualizaciones a los servidores de manera rutinaria?

13.1. ¿Los parches son probados antes de ser implementados en el entorno de producción?

14. ¿Los empleados cuentan con un ID de inicio de sesión único para acceder a los datos?

15. ¿La organización tiene medidas de seguridad establecidas para la protección de datos?
15.1. Si la respuesta es afirmativa, describir en la sección de comentarios.

16. ¿El acceso a sistemas que contienen datos sensibles está restringido? (Ejemplo: números de tarjetas de crédito, números de documento, etc.)
16.1. Si la respuesta es afirmativa, ¿qué controles se han implementado?

17. ¿El acceso físico a los equipos de procesamiento de datos (servidores y equipos de red) está restringido?
17.1. Si la respuesta es afirmativa, describir los controles implementados.

18. ¿Existe un proceso seguro de eliminación de equipos de TI y medios de almacenamiento?
18.1. Si la respuesta es afirmativa, describir el proceso en la sección de comentarios.

3. Seguridad de la Red

19. ¿Los límites de la red están protegidos por firewalls?

20. ¿Se realizan escaneos de vulnerabilidades de red de forma regular?

21. ¿Su organización utiliza sistemas de detección de intrusos (IDS) o sistemas de prevención de intrusos (IPS)?
21.1. Si la respuesta es afirmativa, describir en la sección de comentarios.

22. ¿Se requiere que los empleados utilicen una VPN al acceder a los sistemas de la organización desde ubicaciones remotas?

23. ¿Se permite el acceso inalámbrico en la organización?
23.1. Si la respuesta es afirmativa, describir los mecanismos de protección implementados.

4. Seguridad de los Sistemas

24. ¿Los sistemas informáticos (servidores) cuentan con un esquema regular de copias de seguridad?
24.1. ¿Se ha verificado el proceso de respaldo y recuperación?
24.2. ¿Se almacenan copias de seguridad fuera del sitio?

24.3. ¿Las copias de seguridad están cifradas?

25. ¿La organización replica datos en ubicaciones fuera de su país de operación?

26. ¿La organización terceriza el almacenamiento de datos?
26.1. Si la respuesta es afirmativa, indicar a qué proveedor.

27. ¿Existe un control formal sobre los privilegios de administrador del sistema?

28. ¿Los servidores están configurados para registrar quién accedió a un sistema y qué cambios se realizaron?
28.1. Si la respuesta es negativa, ¿cómo se determina quién accedió y qué cambios se realizaron en caso de una brecha de seguridad?

5. Continuidad del Negocio / Recuperación ante Desastres

29. ¿La organización cuenta con planes de recuperación ante desastres para sus instalaciones de procesamiento de datos?
29.1. ¿Cuenta con un Plan de Continuidad del Negocio?

30. ¿Las salas de servidores están protegidas contra incendios e inundaciones?

31. ¿La organización cuenta con un sitio de recuperación "Hot Site"?

6. Respuesta ante Incidentes

32. En caso de una brecha de seguridad que involucre los datos de la empresa, ¿se notificará a la organización afectada?
32.1. Si la respuesta es afirmativa, ¿en cuánto tiempo se realizará la notificación?

33. ¿La organización cuenta con un plan formal de respuesta ante incidentes?

34. ¿La organización ha experimentado una brecha de seguridad en los últimos 3 a 5 años?
34.1. Si la respuesta es afirmativa, describir la información comprometida.
34.2. Si la respuesta es afirmativa, ¿cómo y en qué plazo se notificó a los clientes afectados?

7. Auditoría y Reporte al Cliente

35. ¿La organización recibe un informe SSAE-18 SOC o ISAE 3402?
35.1. Si la respuesta es afirmativa, especificar el tipo de informe SOC y adjuntar la última versión.