Respuestas del cuestionario audidat

**Nombre**: {{nombre}}

**Apellidos**: {{apellidos}}

**MARCO OPERACIONAL**

1. **Política de seguridad**
2. ¿Ha aprobado la entidad una Política de seguridad? : {{ q1A}}
3. ¿Ha designado los distintos roles incluidos en su Política de seguridad? : {{ q1B}}
4. **Normativa de seguridad**
5. ¿Ha aprobado la entidad una Normativa de seguridad? :{{ q2A}}
6. ¿Ha sido difundida la Normativa de seguridad? : {{ q2B}}
7. ¿Ha realizado un inventario de activos de información?: {{ q2C}}
8. ¿Ha realizado un inventario de las credenciales de los usuarios de los sistemas de información? : {{ q2D}}
9. **Procedimiento de seguridad**
10. ¿Ha facilitado a los usuarios de los sistemas de información una Política de uso de los propios sistemas de información?: {{ q3A}}
11. ¿Tienen documentado el contexto de la organización, incluyendo la segregación de tareas?: {{ q3B}}
12. ¿Dispone de un proceso de reporte de comportamientos anómalos?: {{ q3C}}
13. **Proceso de autorización**
14. ¿Ha aprobado la política de autorizaciones?: {{ q4A}}
15. ¿Tiene la entidad documentada todas las autorizaciones indicadas en la política de autorizaciones?: {{ q4B}}

**MARCO OPERACIONAL**

**PLANIFICACIÓN**

1. **Análisis de riesgos**
2. ¿Ha realizado un análisis de riesgos?: {{ q5A}}
3. **Arquitectura de seguridad**
4. ¿Ha elaborado un documento del Planteamiento integral de la identidad?: {{q6A}}
5. ¿Incluye el Sistema de gestón, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información?:{{q6B}}
6. **Arquitectura de seguridad**
7. ¿Cuenta con un protocolo de adquisición de nuevos componentes?: {{q7A}}
8. **Gestión de la capacidad**
9. ¿Ha elaborado un estudio previo como el indicado en el documento de Planificación (gestión de la capacidad)?: {{q8A}}
10. ¿Utiliza herramientas y recursos para la monitorización de la capacidad?: {{q8B}}
11. **Componentes certificados**
12. ¿Para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad utilizan el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación del Centro Criptológico Nacional?: {{q9A}}
13. ¿Para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad comprueban que tienen alguna certificación que cumpla con los requisitos funcionales de seguridad?:{{q9B}}

**Control de Acceso**

1. **Identificación**
2. ¿Cuenta con sistemas de identificación de usuarios?:{{q10A}}
3. ¿Pueden singularizar a la persona asociada a su rol y sus responsabilidades? :{{q10B}}
4. **Requisitos de acceso**
5. ¿Se limita el acceso a los recursos de tratamiento de información y a la información a los usuarios de los sistemas de información?:{{q11A}}
6. ¿Han desarrollado una política de uso de redes y servicios?:{{q11B}}
7. **Segregación de funciones y tareas**
8. ¿El sistema de control de acceso segrega funciones y tareas?:{{q12A}}
9. **Proceso de gestion de derechos de acceso**
10. ¿Cuenta con un proceso de gestión de derechos de acceso? :{{q13A}}
11. ¿Cuenta con un Política de acceso en remoto? :{{q13B}}
12. **Mecanismos de autentificación (usuarios externos)**
13. ¿En caso de existir usuarios externos, generan o pueden generar medios de identificación específicos? :{{q14A}}
14. ¿Quedan registrados los accesos con éxito y los fallidos? :{{q14B}}
15. **Mecanismos de autentificación (usuarios de la organización)**
16. ¿Otorgan a cada usuario una identidad?:{{q15A}}
17. ¿Utilizan un doble factor de autentificación en aquellos casos en los que se acceda desde zonas no controladas y/o con acceso remoto?:{{q15B}}
18. ¿Registran los accesos con éxito y los fallidos?:{{q15C}}
19. **Inventario de activos**
20. ¿Identifican los activos de la organización y definen las responsabilidades de protección adecuadas? :{{q16A}}
21. ¿Mantienen un inventario actualizado de todos los elementos del sistema? :{{q16B}}
22. **Configuración de la seguridad**
23. ¿Configuran todos los equipos antes de que empiecen a funcionar? :{{q17A}}
24. **Gestión de la configuración de la seguridad**
25. ¿Realiza revisiones de la configuración de los componentes del sistema?: {{q18A}}
26. ¿Verifican periódicamente la configuración hardware/software del sistema? :{{q18B}}
27. **Gestión de la configuración de la seguridad**
28. ¿Mantienen el equipamiento físico y lógico que constituye el sistema de acuerdo con las indicaciones del fabricante?:{{q19A}}
29. ¿Comprueban que las nuevas versiones del equipamiento funcionan correctamente?:{{q19B}}
30. **Gestión de cambios**
31. ¿Se analiza previamente si los cambios a la seguridad del sistema? :{{q20A}}
32. Una vez que se adopte el cambio, ¿se realizarán pruebas de aceptación?:{{q20B}}
33. **Protección frente a Código dañino**
34. ¿Instalan software de protección frente a código dañino en todos los equipos? :{{q21A}}
35. ¿Las funciones críticas se analizan al iniciar los sistemas? :{{q21B}}
36. **Gestión de incidentes**
37. ¿Dispone un proceso integral para hacer frente a los incidents que puedan tener impacto de seguridad en el sistema?: {{q22A}}
38. ¿Dispone de solucionesde ventanilla única para la notificación de incidentes al CCN?: {{q22A}}
39. **Registro de la actividad**
40. ¿Cuentan con registros de actividad en los servidores?:{{q23A}}
41. ¿Se revisan de forma periódica, los registros de actividad, buscando patrones anromales?:{{q23B}}
42. **Registro de gestion de incidentes**
43. ¿Cuentan con registro de incidentes?:{{q24A}}
44. **Protección de claves criptográficas**
45. ¿Las claves criptográficas se protegerán durante todo su ciclo de vida?:{{q25A}}
46. ¿Usan únicamente algoritmos autorizados?:{{q25B}}