Modelo de informe de auditoría de seguridad de sistemas de información



**Prólogo**

La auditoría de la seguridad de los sistemas de información en Túnez está estipulada en la Ley Nº 5 de 2004 y organizada por los decretos de aplicación 2004-1249 y 2004-1250. En los decretos citados se identifican los organismos sujetos a la obligación de auditoría, los expertos auditores autorizados a realizar misiones de auditoría, el proceso de certificación de esos expertos auditores, así como las etapas clave de la misión de auditoría y los productos que se han de proporcionar al organismo auditado al final de la misión. Sin embargo, los controles de seguridad que se han de verificar no se han identificado a nivel de estos decretos.

|  |  |  |
| --- | --- | --- |
|  |  | Evolución del documento |
|  |  |  |
| Version | Fecha | Naturaleza de las modificaciones |
|  |  |  |
| 1.0 | 19/12/2014 | Versión inicial |
| 1.1 | 03/06/2015 | Recomendaciones añadidas |
| 1.2 | 03/05/2017 | Actualización de las áreas de auditoría |
| 1.3 | 14/10/2019 | MAJ tras la publicación de la orden del Ministro detecnologías de comunicación y económicasy el Ministro de Desarrollo, deinversión y cooperación internacional de la01 de octubre de 2019, estableciendo las especificaciones relativas al ejercicio de la actividad de auditoría en el ámbito de la seguridad informática. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

<Nombre de la empresa a auditart>



*<Insertar el logo de la empresa aquí>*

**Informe de auditoría de la seguridad de los sistemas de información**

**De *<Nombre de la empresa auditada>***



*<Insertar logo de la empresai>*

Experto/a auditor/a encargado del proyecto :……………………………………

Firma : …………………………….



*<Ponga el sello del auditor experto aquí>*

|  |  |  |
| --- | --- | --- |
| Versión del documento | Fecha | Emisión |
|  |  |  |
| ***<versión>*** | ***<fecha>*** | Documento confidencial |

**1** **Prólogo**



**1.1**

**Confidencialidad del documento**

Este documento es confidencial y su confidencialidad consiste en:

* La no divulgación de dicha información confidencial a terceros,
* La no reproducción de la llamada información confidencial, excepto con el acuerdo del organismo auditado,
* No beneficiar ni transmitir a terceros el contenido de esta información en términos de conocimientos técnicos,
* Considerar toda la información relativa a la producción y el sistema de información del organismo auditado declarada Confidencial.

**1.2 Histórico de modificaciones**



|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Versión |  |  | Fecha |  |  | Autor |  |  | Modificaciones |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

**1.3** **Difusión del documento**



Difusión (Nombre\_de\_oficina\_de\_auditoría)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Apellido | Nombre | Título | Teléfono | Email |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | Difusión (Nombre\_de\_oficina\_de\_auditoría) |  |  |  |  |
|  | Apellido | Nombre | Título | Teléfono | Email |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**2** **Marco teórico**

- Recordatorio del marco de la misión de auditoría (en aplicación de la Ley Nº 5 de 2004 y el Decreto 2004-1250)

* Indique si esta misión es una auditoría integral o una auditoría de seguimiento (misión de 3 años),
* Presentar el objetivo de esta misión de auditoría (estado de cumplimiento de una norma, recomendaciones, plan de acción),
* Indique, si procede, si esta asignación forma parte de la preparación para la certificación ISO 27001 u otro proceso de cumplimiento,
* Indique, si procede, la(s) norma(s) de la industria con la(s) que se realiza este encargo de auditoría,
* Indique las limitaciones y restricciones de la auditoría (muestreo, cambios desde la auditoría, etc.).

**3** **Términos y definiciones**

* Sírvase proporcionar las definiciones de los términos utilizados en el presente informe.

**4** **Referencias**

* Indique todos los documentos de referencia utilizados para la realización de este encargo de auditoría.

**5** **Presentación de la organización auditada**

* Presente brevemente la organización auditada (establecimiento, número de empleados, ámbito geográfico, misiones, servicios prestados, partes interesadas, clientes, etc.) según la plantilla presentada en el anexo 1,
* Presentar la ruta del proceso de la organización auditada (incluyendo el mapeo del flujo de datos),
* Para cada proceso, indique los requisitos de disponibilidad, integridad y confidencialidad de los datos procesados a ese nivel, de conformidad con el modelo presentado en el apéndice 2, a fin de identificar y controlar los procesos comerciales de la organización auditada, de modo que la evaluación de los riesgos se centre en los procesos comerciales más críticos según la actividad de la organización auditada.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **6** | **Alcance de la auditoría** |  |  |  |  |  |
| **6.1** | **Perímetro geográfico** |  |  |  |  |  |
| - Presentar la lista de estructuras a auditar: |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Estructura |  |  |  | Ubicación |  |  |
|  |  | 1 |  |  |  |  |  |  |  |  |  |
|  |  | 2 |  |  |  |  |  |  |  |  |  |
|  |  | 3 |  |  |  |  |  |  |  |  |  |
|  |  | … |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

* Justifique la elección del ámbito geográfico del contrato de auditoría y presente los criterios de muestreo, si procede.

**6.2** **Descripción de los sistemas de información**

* Describa los sistemas de información de las diferentes estructuras: Para cada estructura, presente todos los componentes del sistema de información con la justificación de las exclusiones, si las hubiera, según el modelo "Descripción del SI de Name\_Organisation\_Audité" (véase el anexo 3).,
* Toda exclusión de un componente del sistema de información (servidor, aplicación, base de datos, equipo de red, solución de seguridad o administración, ...) debe estar bien justificada.

**6.3 Diagrama sinóptico de la arquitectura de la red**

Esquematizar la red de Name\_Organization\_Audite mostrando las conexiones (LAN, WAN, etc), la segmentación, la ubicación de los componentes del IS, etc...

**7** **Metodología de la auditoría**

* Describa en detalle la metodología de auditoría adoptada,
* Identificar las áreas de seguridad de los sistemas de información cubiertas por la metodología de auditoría (estableciendo al mismo tiempo la correspondencia entre las áreas cubiertas y los marcos de auditoría utilizados).
* **Observaciones y recomendaciones :**
* La auditoría deberá tomar como marco de referencia básico el marco de referencia de la auditoría de seguridad de los sistemas de información establecido por la ANSI,
* La madurez de las medidas de seguridad y los controles establecidos debe establecerse en relación con las catorce (14) áreas de dicho sistema de referencia:

**A.5 Políticas de seguridad de la información**

**A.6 Organización de la seguridad de la información**

**A.7 Seguridad de los recursos humanos**

**A.8 Gestión de activos**

**A.9 Control de acceso**

**A.10 Criptografía**

**A.11 Seguridad física y ambiental**

**A.12 Seguridad operacional**

**A.13 Seguridad de las comunicaciones**

**A.14 Adquisición, desarrollo y mantenimiento de sistemas de información**

**A.15 Relaciones con los proveedores**

**A.16 Gestión de incidentes de seguridad de la información**

**A.17 Aspectos de la seguridad de la información en la gestión de la continuidad de las operaciones**

**A.18 Cumplimiento**

* Presentar las herramientas de auditoría utilizadas

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Herramientas |  |  | Versión utilizada |  |  | Licencia |  |  | Funcionalidades |  |  | Los componentes del SI de los objetos de la auditoría |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

- Presentar las listas de verificación utilizadas

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Título del documento |  |  |  | Versión |  |  | Fuente |  |  | Descripción |  |  | Componentes del SI objet de la auditoría |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

- Presente al equipo del proyecto que figura en la lista *Nombre\_Oficina\_auditora* :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Apellido Nombre | Cargo | Calificación | Certificadopor ANSI | Campos de intervención |
|  |  |  |  |  |
| …. | Jefe de proyecto | Ingeniero, |  | Ej : AOP, Auditoría servidores, Audit Bases Datos |
|  |  | Certificador ISO…,  |  |  Auditoría equipamiento de redes, |
|  |  |  |  | … |
|  | Jefe de equipo |  |  |  |
|  |  |  |  |  |
|  | Miembro |  |  |  |
|  | … |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* Presente al equipo de proyecto *Nombre\_empresa\_auditora* :

|  |  |  |
| --- | --- | --- |
| Apellido Nombre | Cargo | Función |
|  |  |  |
| … | Jefe de proyecto | Director … |
|  | … |  |
|  |  |  |
|  |  |  |

* Presentar el calendario de ejecución real de la misión de auditoría según el modelo "Calendario de ejecución real de la misión de auditoría de la seguridad de la SI de Nombre\_Organismo\_Auditor" (véase el Anexo 4).

**8** **Resumen de los resultados de la auditoría**

* Recuerde los criterios y normas/puntos de referencia con los que se realizó la auditoría,
* Recordar la responsabilidad del auditor y los límites de la auditoría (muestreo, cambios desde la auditoría, etc.),
* Recordemos los tipos y la naturaleza de las pruebas realizadas para establecer estos resultados,
* Proporcionar una evaluación detallada de la aplicación del plan de acción resultante de la última misión de auditoría según la plantilla "Evaluación del último plan de acción" (véase el anexo 5
* Presente un resumen de las principales buenas prácticas identificadas y los fallos registrados durante la auditoría,
* Presentar un estado de madurez de la seguridad del sistema de información de la organización auditada según el modelo "Information System Security Maturity Status of Nombre\_Organizacion\_Auditora" (véase el anexo 6).

**9** **Presentación detallada de los resultados de la auditoría**

* Para cada área del marco de auditoría de seguridad de los sistemas de información, se trata de

o Presente la lista de los controles/medidas auditados considerados como criterios de auditoría.

o presentar las buenas prácticas identificadas.

o presentar la lista de vulnerabilidades,

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Dominio** |  | **Criterios** |  |  | **Resultados de la auditoría (conclusiones)** | Descripcióndechequesllevado a cabo...(pruebas, condiciones de prueba, |  |  |
|  |  |  |  |  | **de auditoría** |  |  |  | Descripcióndechequesllevado a cabo...(pruebas, condiciones de prueba, |  |  |
|  |  |  |  |  |  |  |  |  | Descripcióndechequesllevado a cabo...(pruebas, condiciones de prueba, |  |
|  |  |  |  |  |  |  |  |  | **etc)** |  |  |  |
|  |  |  |  |  | **A.5.1 Orientación sobre la gestión de la seguridad de la información** |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | **A.5.1.1** |  |  | **Buenas prácticas identificadas** |  |  |  |  |
|  | **A.5** |  |  |  |  |  |  |  |  |  |
|  |  |  |  | **Buena práctica 1** |  |  |  |  |
|  | **Políticas de** |  | **Políticas de seguridad de la información** |  |  |  |  |  |  |
|  |  |  |  | **Buena práctica 2** |  |  |  |  |
|  | **seguridad** |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  | **….** |  |  |  |  |
|  | **de la información** |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | **Vulnerabiliaddes registradas** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | **Vulnerabilidad 1 - Referencia de vulnerabilidad 1** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | **….** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | **Buenas prácticas identificadas** |  |  |  |  |
|  |  |  |  |  |  |  |  | **Buena práctica 1** |  |  |  |  |
|  |  |  |  |  |  |  |  | **Buena práctica 2** |  |  |  |  |
|  |  |  |  |  |  |  |  | **….** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | **Vulnerabilidades registradas** |  |  |  |  |
|  |  |  |  |  |  |  |  | **Vulmerabilidad 1 - Referencia de la vulnerabilidad 1** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | **….** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | **Criterio 3** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | **….** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | **Criiterio 1** |  |  |  |  |  |  |  |
|  | **A.6** |  |  |  |  |  |  |  |  |  |
|  |  | **…** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **…** |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | **Criterio 1** |  |  |  |  |  |  |  |
|  | **A.18** |  | **…** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |



**Para cada vulnerabilidad inaceptablemente registrada:**



Referencia de vulnerabilidad:

Descripción :

Pruebas de auditoría: Las pruebas de auditoría deben agruparse por áreas temáticas, clasificarse por criterios de auditoría y colocarse en un anexo "Pruebas de auditoría - Términos del área temática".

Componente(s) del SI afectado(s) :

Recomendación:



**Observaciones y recomendaciones :**

* Las esferas de la seguridad de los sistemas de información abarcadas por la auditoría pueden clasificarse en tres niveles:
	+ Aspectos organizativos de la seguridad de los sistemas de información
	+ Seguridad física de los sistemas de información
	+ Seguridad operacional de los sistemas de información
		- Auditoría de la arquitectura de la red
		- Auditoría de la infraestructura y la seguridad de la red
		- Auditoría de seguridad del servidor (capa de sistema y función de servidor)
		- Auditoría de seguridad de la aplicación
* Los criterios de auditoría deben verificarse en todos los componentes del alcance de la auditoría, cualquier exclusión del alcance de la auditoría debe justificarse

En caso de recurrir al muestreo, de acuerdo con el cliente, para la auditoría de ciertos componentes, el auditor debe:

o Presentar claramente los criterios para la selección de muestras concluyentes;

o describir explícitamente la muestra (la muestra debe ser representativa); o cubrir toda la muestra seleccionada por la auditoría.

* Los resultados de la auditoría pueden clasificarse por componente de SI; es decir, para cada componente de SI, el auditor puede agrupar todas las buenas prácticas y vulnerabilidades identificadas clasificándolas por área y criterio de auditoría.
* Las pruebas de auditoría pueden ser de :
	+ Física: es lo que vemos, observar = observación,
	+ Testimonios. Es una evidencia muy frágil que siempre debe ser comprobada y validada por otras pruebas,
	+ Documentación: procedimientos escritos, actas, notas,
	+ Analítica: conciliaciones, deducciones de los resultados de las pruebas técnicas

Las pruebas de auditoría relativas a los aspectos de la seguridad operacional deben incluir pruebas de carácter analítico (resultados de escaneos, resultados de pruebas de penetración, etc.).

Se recomienda encarecidamente que se dé importancia a la consolidación de los resultados de los diferentes instrumentos y medios de auditoría (pruebas manuales, listas de comprobación de las mejores prácticas, instrumentos de exploración automática de la vulnerabilidad, instrumentos de pruebas de penetración).

**10 Evaluación del riesgo**

* Describa el enfoque de evaluación de riesgos adoptado.
* Justifique la elección de los procesos comerciales para la realización de la evaluación de los riesgos.
* Presentar los resultados de la evaluación de riesgos

Este estudio debería permitir elaborar una lista de los escenarios de riesgo más preponderantes, clasificados por orden de criticidad, identificando :

1. Las consecuencias del impacto/explotación de las vulnerabilidades asociadas

 o La complejidad de la explotación de las vulnerabilidades asociadas

o La probabilidad de que se produzcan amenazas asociadas

o Una estimación de la gravedad del riesgo (la gravedad del riesgo es el resultado de los factores involucrados)

Escenario de riesgo:

Descripción:

Referencia(s) de vulnerabilidad:

Componente(s) del SI afectado(s) :

Impacto(s)/consecuencia(s) de la explotación de las vulnerabilidades asociadas:

Complejidad de la explotación de la(s) vulnerabilidad(es) :

Gravedad del riesgo :

Recomendación:

Complejidad de la aplicación de la recomendación :



**11 Plan de acción**

* Organizar por proyectos las acciones/recomendaciones asociadas a las diferentes vulnerabilidades identificadas.
* Indique que el plan de acción se elabora de acuerdo con el auditado.
* Indique que el plan de acción tiene en cuenta los objetivos, los proyectos en curso y las perspectivas de la entidad fiscalizada.
* Indique que el plan de acción tiene en cuenta los resultados de la evaluación del riesgo ya establecida.
* Indique que las estimaciones propuestas por el auditor se dan sobre la base de un dimensionamiento adecuado de las necesidades de la entidad fiscalizada, sus capacidades humanas y financieras y la oferta en el mercado XXX
* Organizar por proyectos las acciones/recomendaciones asociadas a las diferentes vulnerabilidades identificadas.
* Elaborar el plan de acción según la plantilla "Plan de acción propuesto" (véase el apéndice 7).

odèle de Rapport d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2019



|  |  |
| --- | --- |
|  | **Anexo 1** |
|  |  |  |
| Nombre del organismo |  |  |
| Acrónimo |  |  |
| Estatuto |  | Public, Privé |
| Sector de actividad |  | Administration, Finances/Assurances, |
|  |  | Energie/Industrie, Services, Social/Santé, etc. … |
| Categoría |  | Ministère, Administration, Entreprise, Banque, |
|  |  | Assurance, … |
| Sitio Web |  |  |
| Dirección email |  |  |

**Anexo 2**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Designación del proceso |  |  | requisitos de los datos procesados en (1) |  |  |
|  |  |  |  |
|  |  |  | Confidencialidad |  |  | Integridad |  |  | Disponibilidad |  |  |
|  |  |  |  |  |  |  |  |  |  |
| Proceso 1 |  |  |  |  |  |  |  |  |  |  |
| Proceso 2 |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |
| Proceso n |  |  |  |  |  |  |  |  |  |  |

(1) Clasificado en 4 niveles: débil (1), medio (2), fuerte (3) y muy fuerte (4).

**Anexo 3 : Descripción del SI de *Nombre\_Organizacion\_auditada* Para cada lugar dentro del ámbito geográfico de la asignación de la auditoría:**

**Aplicaciones**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Apellido **(1)** | Módulos | Descripción |  |  | Nombres o @IP de | Nombre | **Incluse au périmètre** |  |
| Entorno de desarrollo | Desarrollado por/Año | servidores de alojamiento | d’utilisateurs | **d’audit (6)** |  |
|  |  |  |  |

**Servidores (por plataforma)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Apellido |  | @IP | Tipo **(2)** |  | Sistema de explotación | Rôle/métier **(3)** | **Inclus au périmètre d’audit (6)** |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **Infraestructura de red y seguridad** |  |  |  |  |  |  |  |  |  |
| Naturaleza **(4)** | Marca |  | Nombre |  |  | Administré par : |  | Observations **(5)** | **Inclus au périmètre d’audit (6)** |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **Postes de travail** |  |  |  |  |  |  |  |  |  |  |  |
| Système d’exploitation | Nombre |  |  | **Inclus au périmètre d’audit (6)** |  |  |  |  |

…

1. Por favor, respete la misma nomenclatura utilizada en el informe de auditoría.
2. Tipo de servidor: MV (Máquina Virtual) o MP (Máquina Física).
3. Rol/negocio: Base de datos (MS SQL Server, Oracle, ...), mensajería, aplicación de negocios, Controlador de Dominio, Proxy, Antivirus, etc...

**Por favor, indique el nombre de la(s) solución(es) comercial(es) a nivel de cada una de ellas.**

1. : Naturaleza : Switch, Routeur, Firew**serveur**all, IDS/IPS, etc
2. Observaciones : información adicional sobre el equipo, por ejemplo, el nivel del switch
3. : Sí/No. Si no, presente las razones de la exclusión. En caso de que el elemento no sea auditado por razones de muestreo, indique el elemento con el que se ha tomado la muestra, especificando los criterios **adoptados.**

**Anexo 4 : El calendario de ejecución real de la misión de auditoría de seguridad de la IS de *Nombre\_Organismo\_Auditado***



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Componente |  |  |  |  | Duración enHombres/día |  |  |
|  |  |  |  | por cada intervención |  |
|  |  | Equipo de intervención |  |  |  |
|  |  |  |  |  |  |  |
| Fase | Propósito de la subfase | Fecha de |  En el sitio | Total |  |
|  |  |
|  |  |  | realización |  |  |  |  |
|  | 1: …………………... | Nombre:…………………… |  |  |  |  |  |
| Fase 1 | 2: …………………… | Nombre:…………………… |  |  |  |  |  |
| …. | Nombre:…………………… |  |  |  |  |  |
|  |  |  |  |  |  |
|  | n: …………………… | Nombre:…………………… |  |  |  |  |  |
|  | 1: ……………………... | Nombre:…………………… |  |  |  |  |  |
| Fase 2 | 2: ……………………… | Nombre:…………………… |  |  |  |  |  |
| …. | Nombre:…………………… |  |  |  |  |  |
|  |  |  |  |  |  |
|  | n: …………………… | Nombre:…………………… |  |  |  |  |  |
|  | 1: ……………………... | Nombre:…………………… |  |  |  |  |  |
| Fase n | 2: ……………………… | Nombre:…………………… |  |  |  |  |  |
| … | Nombre:…………………… |  |  |  |  |  |
|  |  |  |  |  |  |
|  | n: …………………… | Nombre:…………………… |  |  |  |  |  |



Duración total del proyecto en Hombres/días

**Anexo 5 : Evaluación de la aplicación del último plan de acción**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Proyecto** | **Acción** | **Críticas** | **oficial de políticas** | **Carga** | **Tasa de** | **Evaluación** |
|  |  |  |  | **(H/D)** | **realización** | **(1)** |
|  |  |  |  |  |  |  |
| Proyecto 1 : … | Acción 1.1 : |  |  |  |  |  |
|  | ……… |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | Acción 1.2 : |  |  |  |  |  |
|  | ……… |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | Acción 1.3 : |  |  |  |  |  |
|  | ……… |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | ... |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Proyecto 2 : … | Acción 2.1 : |  |  |  |  |  |
|  | ……… |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | Acción 2.2 : |  |  |  |  |  |
|  | ……… |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | Acción 2.3 : |  |  |  |  |  |
|  | ……… |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | ... |  |  |  |  |  |
|  |  |  |  |  |  |  |
| …. |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. Evaluación de las medidas adoptadas desde la última auditoría y de las deficiencias registradas en la aplicación de sus recomendaciones, con un informe sobre las razones aducidas por los responsables del sistema de información y sobre las deficiencias observadas, explicando dichas deficiencias.

**Anexo 6 : Estado de madurez de la seguridad del SI de *Nombre\_Organismo\_Auditado***

|  |  |  |  |
| --- | --- | --- | --- |
| **Dominio** | **Criterio** | **Valor** | **Comentarios** |
|  | **de evaluación** | **atribuído** |  |
|  |  |  |  |
| **A.5 Políticas de seguridad de** |  |  |  |
| **la información** |  |  |  |
|  |  |  |  |
| **A.6 Organización de la seguridad de** |  |  |  |
| **la información** |  |  |  |
|  |  |  |  |
| **A.7 Seguridad de los recursos** |  |  |  |
| **humanos** |  |  |  |
|  |  |  |  |
| **A.8 Gestión de activos** |  |  |  |
|  |  |  |  |
| **A.9 Controles de accesos** |  |  |  |
|  |  |  |  |
| **A.10 Criptografía** |  |  |  |
|  |  |  |  |
| **A.11 Seguridad físisca y** |  |  |  |
| **medioambiental** |  |  |  |
|  |  |  |  |
| **A.12 Seguridad operacional** |  |  |  |
|  |  |  |  |
| **A.13 Seguridad de las comunicaciones** |  |  |  |
|  |  |  |  |
| **A.14 Adqusición, desarrollo** |  |  |  |
| **y mantenimiento de los sistemas** |  |  |  |
| **de información** |  |  |  |
|  |  |  |  |
| **A.15 Relaciones de los** |  |  |  |
| **proveedores** |  |  |  |
|  |  |  |  |
| **A.16 Gestión de** |  |  |  |
| **seguridad de la información** |  |  |  |
|  |  |  |  |
| **A.17 Los aspectos de seguridad de** |  |  |  |
| **información en la gestión de la** |  |  |  |
| **continuidad de la empresa** |  |  |  |
|  |  |  |  |
| **A.18 Conformidad** |  |  |  |
|  |  |  |  |

Los valores que se asignarán a cada regla de seguridad invocada estarán entre 0 y 5 :

N/A - No aplicable

0 - Práctica inexistente

1 - Práctica informal: Acciones aisladas

2 - Práctica repetible y seguimiento: Acciones reproducibles

3 - Procesos definidos: Normalización de las prácticas

4 - Procesos controlados: medidas cuantitativas

5 - Procesos continuamente optimizados

**Anexo 7 : Plan de acción propuesto**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Proyecto** | **Acción** | **Prioridad** | **Responsable** | **Carga (H/D)** | **Planificación** |
|  |  |  | **de la acción** |  |  |
|  |  |  |  |  |  |
| Proyecto 1 : | Acción 1.1 : |  |  |  |  |
| …… | …………………….. |  |  |  |  |
|  |  |  |  |  |  |
|  | Acción 1.2 : |  |  |  |  |
|  | …………………….. |  |  |  |  |
|  |  |  |  |  |  |
|  | Acción 1.3 : |  |  |  |  |
|  | …………………….. |  |  |  |  |
|  |  |  |  |  |  |
|  | ... |  |  |  |  |
|  |  |  |  |  |  |
| Proyecto 2 : | Acción 2.1 : |  |  |  |  |
| …… | …………………….. |  |  |  |  |
|  |  |  |  |  |  |
|  | Acción 2.2 : |  |  |  |  |
|  | …………………….. |  |  |  |  |
|  |  |  |  |  |  |
|  | Acción 2.3 : |  |  |  |  |
|  | …………………….. |  |  |  |  |
|  |  |  |  |  |  |
| Proyecto n : | Acción 2.1 : |  |  |  |  |
| …… | …………………….. |  |  |  |  |
|  |  |  |  |  |  |
|  | Acción 2.2 : |  |  |  |  |
|  | …………………….. |  |  |  |  |
|  |  |  |  |  |  |
|  | Acción 2.3 : |  |  |  |  |
|  | …………………….. |  |  |  |  |
|  |  |  |  |  |  |