ESCUELA DE FORMACIÓN
E INNOVACIÓN
REGIÓN DE MURCIA

Cuerpo Técnico, Opción Analista de Aplicaciones. Turno de Promoción Interna

MÓDULO DE SEGURIDAD INFORMÁTICA
(Supuesto práctico)

Autor: Sergio Antonio García Sánchez

Avda Infante Juan Manuel 14
30011 Murcia
Telf: 968362189
Fax: 968366456
direccion.eap@carm.es
http://efiapmurcia.carm.es/

ÍNDICE

1. SUPUESTO PRÁCTICO

1.1. Supuesto nº 1.

1.1.1. Un centro directivo (DGE) de una administración pública española, con competencias en materia de empleo, ha previsto la puesta en marcha de un Sistema de Información para ejercer sus potestades en materia de formación para el empleo (SIFE).

1.1.2. Más concretamente, SIFE permitirá gestionar de forma innovadora acciones formativas para diversos colectivos entre los que se priorizarán aquellos que se encuentren en riesgo de exclusión social y víctimas de violencia de género.

1.1.3. Además, SIFE estará conectado con los servicios de Administración Electrónica (SAE). El interesado tramitará en la sede electrónica la correspondiente solicitud de inicio del procedimiento administrativo de formación para el empleo (PAFE).

1.1.4. Seguidamente, SIFE realizará una clasificación de la solicitud y con ayuda de un algoritmo de inteligencia artificial (AIA) determinará si se admite o no en una lista de espera de formación para el empleo (LEFE), cuyo acto tendrá reflejo en una resolución de la DGE.

1.1.5. Una vez lanzadas las convocatorias de acciones formativas por el procedimiento interno que tramita la DGE, los interesados serán contactados a través de una red social de mensajería instantánea (RSMI) radicada en España con servidores ubicados en territorio español.

1.1.6. Se tiene previsto que SIFE disponga de funcionalidades de tecnología conversacional aplicada a la atención automatizada de los interesados mediante un “chatbot” (CHATI) que se ha desarrollado por la empresa MURTIC que además presta soporte de mantenimiento de software.

1.1.7. El back-end de CHATI está ubicado en los sistemas informáticos gestionados por el centro directivo competente en informática (DGI). Dichos sistemas informáticos se alojan en dos nubes distintas: una nube privada (NUPRI) y una nube pública (NUPUB).

1.1.8. NUPRI es una nube del tipo IaaS y está gestionada por un proveedor (NUBLIN) que tiene sus centros de procesamiento en España. En esta nube se ubican servidores de bases de datos (SBBDD) y de copia de seguridad (SBCK).

1.1.9. NUPUB es una nube del tipo PaaS y está gestionada por un proveedor (NUBLON) que presta servicios en todo el mundo y tiene geolocalizados sus servidores en cuatro zonas geográficas, entre las que está la del Espacio Económico Europeo (EEE) que tiene sus servidores en Irlanda. En esta nube se ubican los servidores de aplicaciones (SAPLI) y servidores web (SWEB).

1.1.10. En cuanto a la infraestructura de comunicaciones gestionada por DGI para dotar de estos servicios a toda la administración pública, se cuenta con un perímetro corporativo de seguridad (PCS) destinado a separar la red interna de usuarios de la red internet.

1.1.11. DGI gestiona un equipo de respuesta ante incidentes de seguridad informática (CSIRT), que coordina las actuaciones ante incidentes de los equipos de atención al usuario (CAU), de comunicaciones (COM) y de sistemas (SIS).

1) A la hora de identificar los datos personales que tratará SIFE, señale la opción más correcta teniendo en cuenta la finalidad prevista:

a) Datos identificativos de interesados: NIF, nombre, teléfono, correo electrónico, sexo, dirección postal, nivel de discapacidad.

b) Datos identificativos de interesados, nivel de estudios, nivel de ingresos familiares y si ha sido víctima de violencia de género.

c) Datos identificativos de interesados: NIF, nombre, teléfono, correo electrónico, dirección postal, nivel de ingresos familiares y si ha sido víctima de violencia de género.

d) Datos identificativos de interesados (incluidos los datos biométricos), si ha sido víctima de violencia de género, datos laborales, datos económicos y otros datos relativos a exclusión social.

2) En relación a los principios de protección de datos del RGPD que son necesarios tener en cuenta a la hora de abordar el diseño del Sistema de Información SIFE, señale la opción más correcta:

a) La duración del almacenamiento de los datos personales dependerá de la capacidad máxima contratada en la infraestructura de sistemas que se disponga en cada momento la DGI.

b) La duración del almacenamiento de los datos personales estará sujeto al plazo de conservación que establezca la DGE.

c) La duración del almacenamiento de los datos personales es el conocido como principio de minimización de datos.

d) El plazo de conservación de los datos se establece según acuerdo de nivel de servicio que haya establecido la DGI para sus servicios horizontales de almacenamiento.

3) En base al enunciado del supuesto, y para cumplir con el principio de transparencia del RGPD, elija la respuesta que mejor lo permita conseguir al responsable de tratamiento de SIFE:

a) Deberá informar a través de la plataforma de SAE, sobre la existencia de decisiones automatizadas en referencia al uso de CHATI de atención automatizada.

b) Deberá informar a los interesados sobre la existencia de decisiones automatizadas, lógica aplicada y efectos jurídicos a través de la plataforma de SAE, en el formulario de solicitud de inicio de PAFE.

c) No cabe informar a los interesados de la existencia de decisiones automatizadas, dado que no existen tales decisiones.

d) Existen decisiones automatizadas, pero no cabe informar a los interesados de su existencia, bastará con requerir el consentimiento para el tratamiento de los datos antes de la introducción de los mismos.

4) En relación al derecho de limitación de los interesados previsto por el RGPD, señale la opción más correcta ante una hipotética solicitud de ejercicio de dicho derecho ante el responsable de tratamiento identificado en el enunciado del supuesto práctico:

a) DGI como responsable de tratamiento se asegurará de que los datos queden efectivamente limitados para cualquier tratamiento que no sea la propia conservación de los mismos, u otros como la defensa de reclamaciones con el consentimiento del afectado.

b) En el caso de que haya solicitado previamente el borrado de los datos, aun así, el responsable de tratamiento puede conservarlos si está obligado a ello, lo que es incompatible con la limitación de los mismos.

c) DGI como responsable de tratamiento se asegurará de que los datos queden efectivamente limitados para cualquier tratamiento sin excepción alguna, por lo que procederá a su eliminación.

d) En el caso de que haya solicitado previamente el borrado de los datos, aun así, el responsable de tratamiento puede conservarlos si está obligado a ello, lo que es compatible con la limitación de los mismos.

5) Indique qué opción describe más correctamente obligaciones generales del responsable de tratamiento en relación a la protección de datos desde el diseño y por defecto establecida en el RGPD en el caso que nos ocupa:

a) Aplicará durante el tratamiento de datos, las medidas organizativas y técnicas apropiadas, y con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales relativos a la finalidad de formación para el empleo.

b) Aplicará antes del tratamiento las medidas organizativas apropiadas y durante el tratamiento de datos, las medidas técnicas apropiadas, y con

miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales relativos a la finalidad de formación para el empleo.

c) Aplicará, desde la determinación de medios del tratamiento y durante el mismo, las medidas organizativas y técnicas apropiadas, y con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales relativos a la finalidad de formación para el empleo.

d) Aplicará, desde la determinación de medios del tratamiento y durante el mismo, las medidas organizativas y técnicas apropiadas en base al riesgo de seguridad, y con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales relativos a la finalidad de formación para el empleo.

6) Indique qué opción describe más correctamente obligaciones generales del RGPD para el encargado y/o subencargado/s de tratamiento en el caso que nos ocupa:

a) El encargado de tratamiento para el SIFE aplicará las medidas organizativas y técnicas apropiadas, para asistir al responsable de tratamiento en la respuesta a un interesado que solicite el ejercicio de derechos del RGPD sobre sus datos en el SIFE, y tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable.

b) El encargado de tratamiento para el SIFE aplicará medidas técnicas apropiadas, para asistir al responsable de tratamiento en la respuesta a un interesado que solicite el ejercicio de derechos del RGPD sobre sus datos en el SIFE, y tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable.

c) NUBLIN y NUBLON como subencargados de tratamiento para el SIFE, deberán ofrecer garantías a DGE como encargado de tratamiento, de que serán capaces de aplicar las medidas organizativas y técnicas apropiadas.

d) Con la debida autorización previa por escrito del responsable de tratamiento para el SIFE, el encargado de tratamiento podrá recurrir a la contratación de servicios de NUBLON siempre que se garantice que el tratamiento se efectuará en territorio español y no existen transferencias internacionales si éstas no se han previsto expresamente por el responsable.

7) En relación a la seguridad de los datos personales prevista por el RGPD, indique cuál de las siguientes afirmaciones da una respuesta más correcta para el caso que nos ocupa:

a) Ambos, responsable y encargado de tratamiento, deben aplicar medidas técnicas y organizativas apropiadas, de manera integral y uniforme sin importar qué tipo de dato personal se maneja en SIFE.

b) El encargado de tratamiento debe aplicar medidas técnicas apropiadas, de manera particular para actividades de tratamiento en SIFE de los datos sobre exclusión social y víctimas de violencia de género.

c) Ambos, responsable y encargado de tratamiento, deben aplicar en SIFE aquellas medidas organizativas y técnicas apropiadas que garanticen un nivel de seguridad adecuado a los riesgos para los derechos y libertades de los ciudadanos.

d) El responsable de tratamiento debe aplicar medidas técnicas apropiadas, de manera particular para actividades de tratamiento en SIFE de los datos sobre exclusión social y víctimas de violencia de género.

8) Si se produce una violación de seguridad de los datos personales en SIFE, ¿cuál sería la PRIMERA actuación que se debería llevar a cabo?

a) Describir medidas adecuadas que permitan minimizar las consecuencias de la violación y notificarlas sin dilación indebida a la Agencia Española de Protección de Datos, desde el mismo momento en que se conozca la violación.

b) Tomar medidas de contención que permitan minimizar las consecuencias de la violación de seguridad de los datos personales, desde el mismo momento en que se conozca la violación.

c) Notificar sin dilación indebida a los afectados sobre la violación desde el mismo momento en que se conozca la violación.

d) Analizar las consecuencias de la violación para decidir si se ha de notificar inmediatamente a la autoridad de control, a los afectados, o a ambos.

9) En relación al ámbito de aplicación del ENS, en el caso que nos ocupa, elija cuál de las siguientes opciones considera más adecuada:

a) SIFE en conjunto no es del ámbito de aplicación del ENS dado que está formado por elementos como CHATI o RSMI cuya finalidad no es la tramitación electrónica de expedientes.

b) SIFE no es del ámbito de aplicación del ENS dado que al fin y al cabo es una aplicación informática sectorial del ámbito del Empleo, no de carácter corporativo como puede ser la Sede Electrónica.

c) SIFE entra en el ámbito de aplicación del ENS dado que es un Sistema de Información que da soporte a PAFE.

d) SIFE tiene elementos que están en el ámbito del ENS, como son aquellos que comunican con SAE y, otros que no entran en el ENS, como RSMI o CHATI.

10) Siguiendo los principios básicos del ENS, escoja cuál de las siguientes alternativas es la decisión correcta más completa:

a) La elección de medidas de seguridad será siempre en función de los riesgos a los que está expuesto SIFE, y se desplegarán de manera puntual en el PCS dado que es el elemento que concentrará el mayor número de vías de ataque.

b) La elección de medidas de seguridad será siempre en función de los riesgos a los que está expuesto SIFE, y se desplegarán de manera puntual en los SWEB y SAPLI dado concentran el mayor número de vectores de ataque.

c) La elección de medidas tendrá en cuenta los elementos organizativos de la DGE y los elementos técnicos que la DGI gestiona para SIFE, y se desplegarán formando varias líneas de defensa.

d) La elección de medidas tendrá en cuenta todos los elementos de SIFE, incluyendo la concienciación de los responsables jerárquicos, sus elementos organizativos y los elementos técnicos que dan soporte.

11) En relación a los requisitos mínimos del ENS, indique la alternativa correcta:

a) SIFE se diseñará e implementará con el mayor número de funcionalidades para el tratamiento de la información, de esta forma se aumentará la seguridad al tener estudiadas las medidas de seguridad requeridas.

b) PCS es un ejemplo del requisito de “Protección de las instalaciones”.

c) En base al requisito de “Autorización y control de los accesos”, el acceso a los servicios e informaciones de SIFE estará limitado a aquellos procesos autorizados para determinadas funciones permitidas.

d) Las normas de seguridad sobre uso seguro de SIFE forma parte del requisito de “Seguridad por defecto”.

12) En atención al requisito mínimo de “Profesionalidad” del ENS, indique la alternativa correcta:

a) Se refiere a que el personal de CSIRT debe estar instruido para atender la seguridad de los sistemas.

b) Se refiere a que el personal de CAU, CSIRT, COM y SIS debe estar instruido para atender la seguridad de los sistemas.

c) Se refiere a que el personal de SIS debe estar instruido para atender la seguridad de los sistemas.

d) Se refiere a que el personal de CSIRT y SIS debe estar instruido para atender la seguridad de los sistemas.

13) En el proceso de categorización del ENS de SIFE, DGE ha valorado como perjuicio grave a algún individuo en determinadas dimensiones de seguridad, indique cuál de las siguientes alternativas es correcta:

a) El nivel de confidencialidad es MEDIO bajo el supuesto de que un incidente supusiera la divulgación no autorizada de datos personales relativos a víctimas de violencia de género que maneja SIFE.

b) El nivel de trazabilidad es ALTO bajo el supuesto de que un incidente permitiese acceder a datos personales relativos a víctimas de violencia de género que maneja SIFE, sin que quede rastro de quién ha accedido.

c) El nivel de integridad es MEDIO bajo el supuesto de que un incidente no permitiese el acceso a SIFE durante varios días seguidos.

d) El nivel de autenticidad es MEDIO bajo el supuesto de que un incidente manipulara los datos de un expediente para sustituir el destinatario de una acción formativa.

14) SIFE se ha puesto en marcha y DGE se plantea realizar una auditoría interna de seguridad de SIFE de cara a una auditoría de certificación del ENS. Indique cuál de las siguientes alternativas es la afirmación correcta más completa:

a) La auditoría interna tiene como alcance todos los elementos informáticos que dan soporte a SIFE.

b) La auditoría interna tiene como alcance los elementos de SIFE sobre los que tiene competencia DGE como los que tiene DGI.

c) La auditoría interna tiene como alcance el Sistema de Gestión de la Seguridad de la Información (SGSI) existente.

d) La auditoría interna tiene como alcance los elementos de SIFE que no sean de carácter horizontal, quedando fuera las infraestructuras comunes de sistemas y comunicaciones.

15) Atendiendo a la naturaleza de las medidas de seguridad que se han previsto aplicar en SIFE, escoja la alternativa correcta que mejor las clasifique en la estructura descrita en el Anexo II del ENS:

a) Las medidas sobre identificación en el control de acceso a SIFE forman parte del marco operacional.

b) Las medidas sobre identificación en SIFE forman parte del marco operacional y de medidas de protección.

c) Las medidas relativas a mecanismos de autenticación para SIFE forman parte de medidas de protección.

d) Las medidas relativas a mecanismos de autenticación para SIFE forman parte del marco operacional.

16) En aplicación del Reglamento "eIDAS", tras la categorización ENS de SIFE, de las siguientes alternativas señale aquella que responda de manera más amplia al cumplimiento normativo sobre identificación electrónica:

a) Teniendo en cuenta que en SIFE la dimensión de seguridad determinante de Confidencialidad se ha adscrito a un nivel de seguridad MEDIO, el sistema de identificación electrónica poseerá un grado de confianza sustancial o superior.

b) Teniendo en cuenta que en SIFE la dimensión de seguridad determinante de Integridad se ha adscrito a un nivel de seguridad BAJO, el sistema de identificación electrónica poseerá un grado de confianza limitado, sustancial o superior.

c) Teniendo en cuenta que en SIFE la dimensión de seguridad determinante de Autenticidad se haya adscrito a un nivel de seguridad MEDIO, el sistema de identificación electrónica poseerá un grado de confianza sustancial.

d) Teniendo en cuenta que en SIFE la dimensión de seguridad determinante de Trazabilidad se ha adscrito a un nivel de seguridad BAJO, el sistema de identificación electrónica poseerá un grado de confianza limitado, sustancial o superior.

17) En aplicación del Reglamento "eIDAS", tras la categorización ENS de SIFE, de las siguientes alternativas señale aquella que responda de manera más amplia al cumplimiento normativo sobre firma electrónica:

a) Teniendo en cuenta que en SIFE la dimensión de seguridad determinante de Confidencialidad se ha adscrito a un nivel de seguridad MEDIO, se requerirá el uso de un sistema de firma electrónica avanzada.

b) Teniendo en cuenta que en SIFE la dimensión de seguridad determinante de Autenticidad se ha adscrito a un nivel de seguridad ALTO, se requerirá uso de dispositivo de creación de firma electrónica que garantice que la generación de los datos de creación de firma corre a cargo de un prestador cualificado de servicios de confianza.

c) Teniendo en cuenta que en SIFE la dimensión de seguridad determinante de Trazabilidad se ha adscrito a un nivel de seguridad MEDIO, se requerirá el uso de un sistema de firma electrónica avanzada.

d) Teniendo en cuenta que en SIFE la dimensión de seguridad determinante de Disponibilidad se ha adscrito a un nivel de seguridad ALTO, se requerirá uso de dispositivo de creación de firma electrónica que garantice que la generación de los datos de creación de firma corre a cargo de un prestador cualificado de servicios de confianza.

18) Como resultado de la auditoría interna de SIFE se detecta una no conformidad "mayor" dado que no se ha efectuado un Análisis de Riesgos de SIFE antes de su puesta en marcha. Indique de entre las siguientes alternativas cuál sería, en base a los principios básicos del ENS, la mejor manera de haber realizado dicho análisis siguiendo MAGERIT:

a) Antes de poner en marcha SIFE, se acometería mediante un proyecto de análisis de riesgos dado que es un cambio sustancial y una vez SIFE está en el entorno de pre-producción es posible hacer pruebas de penetración y de vulnerabilidades.

b) Antes de poner en marcha SIFE, teniendo en cuenta el ciclo de vida de desarrollo de SIFE, se acometería incrementalmente desde el inicio y en paralelo a su desarrollo, mediante una adecuada coordinación entre los equipos de análisis y de desarrollo.

c) Antes de poner en marcha SIFE, mediante la valoración y posterior categorización de SIFE, dado que la categoría y los activos que constituyen SIFE determinan las medidas de seguridad que le aplican.

d) Se debería centrar únicamente en los elementos nuevos que se introducen con la puesta en marcha de SIFE, de esta forma se obtendrá el resultado del informe lo antes posible para corregir la no conformidad detectada.

19) Aplicado a SIFE el método de análisis de riesgos de MAGERIT, se van a estimar los riesgos teniendo en cuenta determinados elementos del inventario de activos del Sistema de Información. Indique cuál de las siguientes afirmaciones es correcta sobre identificación y clasificación de activos:

a) SBBDD y SBCK son activos esenciales dado que dan soporte al almacenamiento de los datos de SIFE, así como a su respaldo.

b) NUPRI y NUPUB no forman parte de los activos a considerar dado que son gestionados por proveedores externos.

c) SAPLI y SWEB son activos esenciales dado que permiten el acceso electrónico de los ciudadanos a SIFE.

d) De los trámites contenidos en PAFE se deducen los activos esenciales.

20) Aplicado a SIFE el método de análisis de riesgos de MAGERIT, se van a estimar los riesgos teniendo en cuenta las dependencias que se deducen del enunciado entre los activos del Sistema de Información. Indique cuál de las siguientes afirmaciones es correcta a la hora de determinar los impactos:

a) El impacto acumulado de CHATI dependerá del valor acumulado de todos los activos inferiores que le dan soporte como NUPUB y NUPRI.

b) El impacto repercutido de CHATI dependerá de la degradación que produciría la materialización de una amenaza sobre un activo inferior como NUPUB o NUPRI.

c) El impacto potencial acumulado de SAPLI dependerá del valor acumulado de NUPRI y las salvaguardas que se hayan desplegado.

d) El impacto residual repercutido de SWEB dependerá del valor propio de SWEB sin considerar salvaguardas.

21) Suponga que se detectan una serie de deficiencias de seguridad tras realizar un análisis de vulnerabilidades en el ámbito de SIFE. Indique cuál de las siguientes alternativas es correcta:

a) Las medidas de seguridad administrativas incidirán en aquellas vulnerabilidades que obedezcan a una deficiente configuración y administración de SAPLI y SWEB.

b) Las medidas de seguridad lógicas incidirán en aquellas vulnerabilidades que obedezcan a una deficiente configuración de las reglas de cortafuegos en PCS.

c) Las normativas legales de seguridad no incidirán en vulnerabilidades de SIFE.

d) Las medidas de seguridad físicas incidirán en aquellas vulnerabilidades que obedezcan a una deficiente configuración de las reglas de cortafuegos en PCS.

22) Suponga que SIFE está sufriendo un ataque de seguridad en algún elemento, identifique qué alternativa es la correcta:

a) El ataque es de tipo activo si se ha comprometido el PCS y se produce fuga de información confidencial de SIFE.

b) El ataque es de tipo pasivo si se ha comprometido el PCS y se produce denegación de servicio de SWEB.

c) El ataque es de tipo activo si se ha comprometido el SWEB y se produce denegación de servicio de SWEB.

d) El ataque es de tipo pasivo si se ha comprometido el SWEB y se produce modificación de algún dato en SBBDD.

23) Se ha previsto realizar un escaneo de vulnerabilidades sobre los servidores SAPLI y SWEB que dan soporte a SIFE, indique la mejor manera de realizar el escaneo:

a) Se han de identificar las subredes donde se localizan los servidores. Se programará el escaneo en horario de oficina para asegurarse de que los servicios web están en uso y con la carga habitual de trabajo.

b) Se han de identificar las subredes donde se localizan los servidores y las URLs de los servicios web cuando existen más de un virtual-host en los servidores. Se programará el escaneo en horario que no tenga repercusión sobre el funcionamiento de los servicios.

c) Se han de identificar las subredes donde se localizan los servidores y las URLs de los servicios web cuando existen más de un virtual-host en los servidores. Se programará el escaneo en horario de oficina para asegurarse de que los servicios web están en uso y con la carga habitual de trabajo.

d) Se han de identificar las subredes donde se localizan los servidores. Se programará el escaneo en horario que no tenga repercusión sobre el funcionamiento de los servicios.

24) En un análisis de vulnerabilidades se detectan varios servidores SAPLI potencialmente vulnerables a GhostCat (Apache Tomcat) que permite al atacante la lectura de ficheros de configuración o el código de la aplicación hospedada en el servidor. De las siguientes medidas, elija aquella que suponga una mayor defensa:

a) Se ha de mantener actualizada la versión de Apache Tomcat.

b) Se ha de evitar incluir credenciales de usuario en el código fuente de las aplicaciones y ficheros de configuración.

c) Se ha de mantener actualizado el servidor donde se encuentra Apache Tomcat.

d) Se ha poner una regla de cortafuegos en el PCS para evitar que los atacantes aprovechen esta vulnerabilidad.

25) En atención a la confidencialidad que requieren determinados datos personales de SIFE, indique qué estrategia de defensa es la más adecuada en este caso:

a) La defensa criptográfica basada en el criptoanálisis, orientado al cifrado de mensajes y diseño de criptosistemas asimétricos basados en PKI.

b) La defensa no criptográfica basada en sistemas de detección de intrusiones en el PCS.

c) La defensa criptográfica basada en la criptografía simétrica para el cifrado en bloque como es Triple-DES.

d) La defensa no criptográfica de acceso al sistema mediante sistemas biométricos.

26) Elija la alternativa que clasifique y ubique correctamente el tipo de defensa de seguridad en los elementos de SIFE, según se desprende del enunciado:

a) Como tipo de defensa de Sistema de Detección de Intrusos: el uso de antivirus en SBBDD.

b) Como tipo de defensa de sistema operativo: el uso de mecanismos de autenticación de doble factor en el servicio de SSO (Single Sign On).

c) Como tipo de defensa de sistema operativo: analizador de vulnerabilidades como Nessus.

d) Como tipo de Sistema de Detección de Intrusos: un sistema pasivo IDPS basado en hosts de tipo NIDS.

27) Un atacante ha remitido un correo de phising al personal de la DGE con el fin de suplantar la aplicación web de consulta interna de LEFE. ¿Cuál de los siguientes escenarios tendría un menor riesgo residual asociado a este tipo de amenazas?

a) El servidor que alberga la aplicación web de acceso a LEFE se configura con un certificado digital que ha sido emitido por la PKI que los administradores de SIS han desplegado rápidamente en la propia red corporativa.

b) Existe un programa anual de concienciación de usuarios en materia de seguridad, además se ha previsto campañas de simulación de phising.

c) El servidor que alberga la aplicación web de acceso a LEFE se configura con el protocolo SSL lo que dota a las conexiones de Confidencialidad, Autenticidad e Integridad.

d) Se configura el servicio centralizado de Anti-Spam en el PCS para que filtre el ataque de phising.

28) Para la prestación de soporte de mantenimiento del software CHATI, la empresa MURTIC necesita el acceso remoto a sistemas informáticos gestionados por DGI. Elija de las siguientes alternativas la que resulte en un menor riesgo residual resultante:

a) Emplear una VPN de acceso remoto para el que se hayan definido en el cortafuegos del PCS las reglas concretas de acceso a unidades de red por VPN, así como las direcciones y puertos para efectuar el mantenimiento de la empresa MURTIC.

b) Emplear un enlace tipo LAN to LAN para el acceso remoto desde las oficinas de MURTIC, de manera que la red local de ésta se integre con la red corporativa gestionada por DGI y se beneficie de la seguridad proporcionada por el PCS en relación a las reglas de cortafuegos y filtros anti-spam configurados.

c) Emplear una VPN de acceso remoto para el que se hayan definido en el cortafuegos del PCS las reglas concretas de acceso a los puertos y direcciones IP que específicamente sean estrictamente necesarias para efectuar el mantenimiento de la empresa MURTIC.

d) Emplear un enlace tipo LAN to LAN para el que se hayan definido en el cortafuegos del PCS las reglas concretas de acceso a los puertos y direcciones IP que específicamente sean estrictamente necesarias para efectuar el mantenimiento de la empresa MURTIC.

2. SOLUCIÓN AL SUPUESTO PRÁCTICO

2.1. Soluciones al supuesto nº 1.

1) A la hora de identificar los datos personales que tratará SIFE, señale la opción más correcta teniendo en cuenta la finalidad prevista: Respuesta correcta: b

2) En relación a los principios de protección de datos del RGPD que son necesarios tener en cuenta a la hora de abordar el diseño del Sistema de Información SIFE, señale la opción más correcta: Respuesta correcta: b

3) En base al enunciado del supuesto, y para cumplir con el principio de transparencia del RGPD, elija la respuesta que mejor lo permita conseguir al responsable de tratamiento de SIFE: Respuesta correcta: b

4) En relación al derecho de limitación de los interesados previsto por el RGPD, señale la opción más correcta ante una hipotética solicitud de ejercicio de dicho derecho ante el responsable de tratamiento identificado en el enunciado del supuesto práctico: Respuesta correcta: d

5) Indique qué opción describe más correctamente obligaciones generales del responsable de tratamiento en relación a la protección de datos desde el diseño y por defecto establecida en el RGPD en el caso que nos ocupa: Respuesta correcta: c

6) Indique qué opción describe más correctamente obligaciones generales del RGPD para el encargado y/o subencargado/s de tratamiento en el caso que nos ocupa: Respuesta correcta: a

7) En relación a la seguridad de los datos personales prevista por el RGPD, indique cuál de las siguientes afirmaciones da una respuesta más correcta para el caso que nos ocupa: Respuesta correcta: c

8) Si se produce una violación de seguridad de los datos personales en SIFE, ¿cuál sería la PRIMERA actuación que se debería llevar a cabo? Respuesta correcta: b

9) En relación al ámbito de aplicación del ENS, en el caso que nos ocupa, elija cuál de las siguientes opciones considera más adecuada: Respuesta correcta: c

10) Siguiendo los principios básicos del ENS, escoja cuál de las siguientes alternativas es la decisión correcta más completa: Respuesta correcta: d

11) En relación a los requisitos mínimos del ENS, indique la alternativa correcta: Respuesta correcta: c

12) En atención al requisito mínimo de “Profesionalidad” del ENS, indique la alternativa correcta: Respuesta correcta: b

13) En el proceso de categorización del ENS de SIFE, DGE ha valorado como perjuicio grave a algún individuo en determinadas dimensiones de seguridad, indique cuál de las siguientes alternativas es correcta: Respuesta correcta: b

14) SIFE se ha puesto en marcha y DGE se plantea realizar una auditoría interna de seguridad de SIFE de cara a una auditoría de certificación del ENS. Indique cuál de las siguientes alternativas es la afirmación correcta más completa: Respuesta correcta: b

15) Atendiendo a la naturaleza de las medidas de seguridad que se han previsto aplicar en SIFE, escoja la alternativa correcta que mejor las clasifique en la estructura descrita en el Anexo II del ENS: Respuesta correcta: b

16) En aplicación del Reglamento “eIDAS”, tras la categorización ENS de SIFE, de las siguientes alternativas señale aquella que responda de manera más amplia al cumplimiento normativo sobre identificación electrónica: Respuesta correcta: c

17) En aplicación del Reglamento “eIDAS”, tras la categorización ENS de SIFE, de las siguientes alternativas señale aquella que responda de manera más amplia al cumplimiento normativo sobre firma electrónica: Respuesta correcta: b

18) Como resultado de la auditoría interna de SIFE se detecta una no conformidad “mayor” dado que no se ha efectuado un Análisis de Riesgos de SIFE antes de su puesta en marcha. Indique de entre las siguientes alternativas cuál sería, en base a los principios básicos del ENS, la mejor manera de haber realizado dicho análisis siguiendo MAGERIT: Respuesta correcta: b

19) Aplicado a SIFE el método de análisis de riesgos de MAGERIT, se van a estimar los riesgos teniendo en cuenta determinados elementos del inventario de activos del Sistema de Información. Indique cuál de las siguientes afirmaciones es correcta sobre identificación y clasificación de activos: Respuesta correcta: d

20) Aplicado a SIFE el método de análisis de riesgos de MAGERIT, se van a estimar los riesgos teniendo en cuenta las dependencias que se deducen del enunciado entre los activos del Sistema de Información. Indique cuál de las siguientes afirmaciones es correcta a la hora de determinar los impactos: Respuesta correcta: b

21) Suponga que se detectan una serie de deficiencias de seguridad tras realizar un análisis de vulnerabilidades en el ámbito de SIFE. Indique cuál de las siguientes alternativas es correcta: Respuesta correcta: b

22) Suponga que SIFE está sufriendo un ataque de seguridad en algún elemento, identifique qué alternativa es la correcta: Respuesta correcta: c

23) Se ha previsto realizar un escaneo de vulnerabilidades sobre los servidores SAPLI y SWEB que dan soporte a SIFE, indique la mejor manera de realizar el escaneo: Respuesta correcta: b

24) En un análisis de vulnerabilidades se detectan varios servidores SAPLI potencialmente vulnerables a GhostCat (Apache Tomcat) que permite al atacante la lectura de ficheros de configuración o el código de la aplicación hospedada en el servidor. De las siguientes medidas, elija aquella que suponga una mayor defensa: Respuesta correcta: b

25) En atención a la confidencialidad que requieren determinados datos personales de SIFE, indique qué estrategia de defensa es la más adecuada en este caso: Respuesta correcta: c

26) Elija la alternativa que clasifique y ubique correctamente el tipo de defensa de seguridad en los elementos de SIFE, según se desprende del enunciado: Respuesta correcta: b

27) Un atacante ha remitido un correo de phising al personal de la DGE con el fin de suplantar la aplicación web de consulta interna de LEFE. ¿Cuál de los siguientes escenarios tendría un menor riesgo residual asociado a este tipo de amenazas? Respuesta correcta: b

28) Para la prestación de soporte de mantenimiento del software CHATI, la empresa MURTIC necesita el acceso remoto a sistemas informáticos gestionados por DGI. Elija de las siguientes alternativas la que resulte en un menor riesgo residual resultante: Respuesta correcta: c