Servicios Auditorias de Seguridad TIC

Seguretat TIC

Àrea d'Infraestructura Tecnològica i Operació Tecnològica de Sistemes

20/05/2019

Índice

1. Auditorías de seguridad TIC

2.1 Introducción

La Dirección Ejecutiva de Innovación, Tecnología y Negocio Internacional (DEITNI) de TMB tiene la responsabilidad de definir, implantar y controlar la seguridad lógica de todos los entornos TIC y la física en las dependencias de los CPD donde se encuentran los equipos TI.

Dentro de esta responsabilidad está incluida la realización periódica de auditorías de seguridad para la detección de posibles anomalías o riesgos de seguridad en los sistemas responsabilidad de DEITNI.

2.2 Objeto

El objeto del presente documento es definir las auditorías de seguridad TIC a realizar en sistemas de TMB a fin de conocer el novel de seguridad de los entornos auditados

2. Objeto de la solicitud

2.1 Auditorías de Seguridad TIC en sistemas de TMB

El objeto de esta contratación es la realización de tres auditorías de seguridad definidas de la siguiente manera:

2.1.1 Auditoría de un entorno SAP. El objeto de esta auditoría es detectar las vulnerabilidades que existan en el entorno SAP auditado. Se debe incluir en la auditoría por lo menos los siguientes aspectos:

- Sistema Operativo Linux
- Sistema SAP Basis
- SAP HANA
- Comunicaciones entre sistemas
- Comunicaciones cliente/servidor
- Identificación de las amenazas y la probabilidad de que ocurran
- Definición de medidas de mitigación a implementar
- Sistema de parcheado y cambios
- Gestión y acceso de usuarios
- Controles de acceso a la red
- Copias de seguridad y recuperación de datos
- Gestión de incidentes de seguridad

2.1.2 Auditoría de un entorno Microsoft Exchange. El objeto de esta auditoría es detectar las vulnerabilidades que existan en el entorno Microsoft Exchange.

Se debe incluir en la auditoría por lo menos los siguientes aspectos:

- Sistema Operativo Windows
- MS Exchange 2010
- Comunicaciones entre sistemas
- Comunicaciones cliente/servidor
- Identificación de las amenazas y la probabilidad de que ocurran
- Definición de medidas de mitigación a implementar
- Sistema de parcheado y cambios
- Gestión y acceso de usuarios
- Controles de acceso a la red
- Copias de seguridad y recuperación de datos
- Gestión de incidentes de seguridad

2.1.3 Auditoría en modo Red Team. En este caso se debe conseguir, en la medida de lo posible, acceso a nuestros sistemas, conseguir movimientos laterales, elevación de privilegios y acceso a los datos almacenados en ellos.

2.1.4 Entregables

Los entregables de estas auditorías deben contener como mínimo:

- Lista de sistemas analizados
- Lista de procedimientos analizados
- Lista de vulnerabilidades detectadas
- Propuesta de medidas correctoras con estimación de esfuerzo y coste de implantación
- Propuesta de plan de acción para la mitigación de las vulnerabilidades detectadas
- Propuesta de mejoras en los procedimientos analizados

3. Modelo de Prestación del Servicio

3.1. Puesta en marcha

Para la puesta en marcha del contrato se establecerá una fase inicial a fin de establecer las acciones a realizar para una correcta realización de las auditorías contratadas.

Durante esta puesta en marcha se recabará aquella información necesaria para el desarrollo del trabajo adjudicado.

Esta fase no se podrá extender más allá de 15 días desde la firma del contrato.

3.2. Equipo de Trabajo

El adjudicatario del servicio debe acreditar que dispone de profesionales con las siguientes acreditaciones:

- Offensive Security Certified Professional (OSCP)
- Offensive Security (OSWP)
- Offensive Security Certified Expert (OSCE)
- SANS CEH Certified Ethical Hacker
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)

- Certified Information Security Manager (CISM)
- ITIL V3 Foundation y/o Practitioner
- Certified Reverse Engineering Analyst

3.3. Medios

El adjudicatario deberá contar con todas las herramientas necesarias para desarrollar las actividades que se indican en este documento bajo los procedimientos marcados por TMB.

4. Seguretat i Confidencialitat

L'adjudicatari s'obliga a no difondre i guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del present contracte, i a subministrar-la només al personal autoritzat per TMB.

L'adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal al seu càrrec. Així mateix, s'obliga a aplicar les mesures necessàries per a garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal participant en el desenvolupament del contracte.

Un cop finalitzat el present contracte, l'adjudicatari es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per TMB, així com qualsevol altre producte obtingut com a resultat del present contracte.

El proveïdor ha de complir amb la política de Seguretat Tecnològica i el Cos Normatiu de Seguretat de TMB.

5. Compliment de la llei Orgànica de Protecció de Dades de Caràcter Personal

L'adjudicatari es compromet a acomplir quantes obligacions li son exigibles en matèria de protecció de dades personal tant pel Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques en el que respecte al tractament de dades personals i a la lliure circulació d'aquestes dades i per el que es deroga la Directiva 95/46/CE ("RGPD") com per la llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades de Caràcter Personal així com quantes normes legals o reglamentaries incideixin, desenvolupin o substitueixin a les anteriors en aquest àmbit.

6. Información adicional

Los licitadores podrán solicitar información sobre los pliegos y servicios objeto de la licitación:

- Información técnica: Juan José Del Río, Responsable de Unidad de Seguridad TIC, tel. 932 987 450. jjdelrio@tmb.cat
- Información general: Beatriz Castro, Responsable Unidad de Aprovisionamientos, tel. 932 987 108. bcastro@tmb.cat

Juan Jose Del Rio Estevez 2020.01.31 12:59:14 +01'00'

Seguretat TIC

INFRAESTRUCTURA TECNOLÒGICA I OPERACIÓ DE TECNOLOGIES I SISTEMES