Fastclick Auditors

CONTRACTE DE SERVEIS D'AUDITORIA DE SEGURETAT INFORMÀTICA

1. IDENTIFICACIÓ DE LES PARTS

1.1. Empresa Auditora:

Fastclick Auditors
Representada per:
Josep Pellisa
Ramon Aibar
Daniel Miron

1.2. Empresa Auditada:

Institut Tecnològic de l'Ebre – Departament d'Informàtica
Representada per:
Professor Jose Diego Cervellera

2. OBJECTE DEL CONTRACTE

El present contracte té per objecte la prestació de serveis d'auditoria de seguretat informàtica per part de Fastclick Auditors a l'Institut Tecnològic de l'Ebre – Departament d'Informàtica.

L'objectiu principal és la realització d'auditories de seguretat, tant dinàmiques (en execució) com estàtiques (de codi font), de l'aplicació informàtica desenvolupada en Python amb interfície gràfica (GUI) que es detalla a l'Annex Tècnic I, que forma part integrant d'aquest contracte.

2.1. Les actuacions a realitzar tenen com a finalitat:

Identificar i avaluar vulnerabilitats de seguretat en els sistemes i aplicacions objecte de l'auditoria.

Analitzar el codi font de l'aplicació per detectar possibles errors de programació, pràctiques insegures i debilitats lògiques.

Proposar un pla de mesures correctores i millores per a la mitigació o eliminació dels riscos detectats.

Garantitzar els principis de integritat, confidencialitat i disponibilitat dels actius tecnològics i de la informació de l'Institut.

Lliurar un informe exhaustiu que reculli les conclusions, el nivell de risc associat a cada vulnerabilitat i les recomanacions tècniques per a la seva resolució.

L’abast concret de les proves, les metodologies a emprar i les especificacions tècniques es detallen exhaustivament en l’Annex Tècnic I d’aquest contracte.

3. ABAST DE L’AUDITORIA

L’auditoria comprendrà l’anàlisi de l’aplicació informàtica desenvolupada en Python amb interfície gràfica (GUI), amb les següents activitats:

Realització d’auditories bàsiques de xarxa, incloent l’anàlisi de ports oberts, serveis actius i configuracions de seguretat.

Anàlisi de vulnerabilitats en servidors i sistemes configurats, amb especial atenció a serveis com SSH i FTP.

Control i revisió dels registres del sistema per detectar anomalies o incidents de seguretat.

Generació automàtica d’informes tècnics amb els resultats obtinguts, vulnerabilitats detectades i recomanacions d’actuació.

3.1. Exclusions:

Queden expressament exclosos de l’abast d’aquesta auditoria els dispositius personals, els sistemes físics de control d’accés i els serveis externs allotjats fora de la infraestructura de l’Institut.

4. FUNCIONS I PERMISOS

4.1. Permisos Atorgats

L'empresa auditora (FASTCLICK AUDITORS) tindrà accés als sistemes i aplicacions objecte de l'auditoria amb els següents permisos i condicions:

- Comptes d'usuari amb privilegis limitats per a la realització de les proves necessàries
- Accés de lectura als registres del sistema (logs) per a l'anàlisi de seguretat
- Permís per executar eines d'auditoria no intrusives i escanejadors de vulnerabilitats
- Accés a les aplicacions en entorn de proves amb dades no productives
- Permís per realitzar proves d'autenticació i autorització dins de l'abast contractat
- Accés a la documentació tècnica necessària per a la comprensió de l'arquitectura del sistema

4.2. Restriccions i Limitacions

Es estableixen les següents restriccions per garantir la integritat dels sistemes:

- Prohibició d'accés amb comptes d'administrador o privilegis elevats sense autorització

expressa

- Restricció de modificacions permanents en la configuració dels sistemes
- Prohibició d'extracció o còpia de dades confidencials sense autorització prèvia per escrit
- Limitació de les proves intrusives que puguin afectar la disponibilitat dels serveis
- Prohibició d'accés a sistemes no inclosos en l'abast de l'auditoria
- Restricció de la instal·lació de programari no autoritzat als sistemes del client

4.3. Procediment d'Autorització

- Totes les activitats que requereixin permisos especials hauran de ser autoritzades prèviament per escrit pel responsable de seguretat del client
- Les autoritzacions específiques s'emmagatzemaran en el registre d'activitats de l'auditoria
- Qualsevol desviació dels permisos atorgats haurà de ser comunicada immediatament

4.4. Supervisió i Control

- Totes les activitats realitzades durant l'auditoria quedaràn registrades en un log d'activitats
- El client tindrà dret a supervisar les activitats de l'auditor en tot moment
- Es facilitarà accés als registres d'activitat al client quan sigui requerit

5. CONFIDENCIALITAT

5.1. Obligació de Confidencialitat

Fastclick Auditors es compromet a mantenir la més estricta confidencialitat sobre tota la informació, dades, documents, resultats i qualsevol altre element al qual tingui accés durant l'execució de la present auditoria. Aquesta obligació s'estén a tots els membres de l'equip assignat al projecte, així com a qualsevol persona sota la seva supervisió, i es mantindrà vigent de manera indefinida, inclòs després de la finalització de la relació contractual.

5.2. Abast de la Informació Confidencial

S'entén com a informació confidencial, amb caràcter enunciatiu però no limitatiu:

- Els resultats parcials i finals de l'auditoria.
- Les vulnerabilitats i debilitats detectades als sistemes.
- La documentació tècnica, arquitectònica i operativa facilitada pel client.
- Les dades de configuració, credencials d'accés i registres dels sistemes.
- Qualsevol altra informació revelada durant l'execució dels treballs.

5.3. Protecció de Dades de Caràcter Personal

Ambdues parts es comprometen a complir escrupolosament amb la normativa vigent en matèria de protecció de dades de caràcter personal, en particular el Reglament General de

Protecció de Dades (RGPD) i la Llei Orgànica de Protecció de Dades i Garantia de Drets Digitals (LOPDGDD).

5.4. Deures com a Encarrerat del Tractament

En la seva condició d'Encarrerat del Tractament, Fastclick Auditors garanteix que:

- Utilitzarà les dades personals a les que accedeixi únicament per a la finalitat contractada.
- Aplicarà les mesures de seguretat tècniques i organitzatives necessàries per assegurar la seva integritat i confidencialitat.
- No comunicarà aquestes dades a tercers, ni tan sols per a la seva conservació, sense l'autorització prèvia i per escrit del Client.
- Destruirà o retornarà totes les dades al Client un cop finalitzada la prestació del servei.

5.5. Deures del Client com a Responsable del Tractament

L'Institut Tecnològic de l'Ebre, com a Responsable del Tractament, garanteix que ha informat correctament als afectats sobre la possible comunicació de les seves dades al prestador del servei d'auditoria amb la finalitat de realitzar els treballs objecte d'aquest contracte.

5.6. Auditories i Compliment

Fastclick Auditors es compromet a permetre i cooperar en les auditories que el Client consideri necessàries per verificar el compliment d'aquestes obligacions de confidencialitat i protecció de dades.

6. LLIURAMENT DE L'INFORME

6.1. Contingut de l'Informe Final

Un cop finalitzada l'auditoria, es lliurarà un informe tècnic exhaustiu en format PDF que inclourà, amb caràcter obligatori, les següents seccions:

Resum Executiu: Destinat a la direcció, amb una visió global dels resultats, el nivell de seguretat general i les conclusions principals sense profunditat tècnica.

Metodologia Aplicada: Descripció detallada de les tècniques, eines i procediments utilitzats durant l'auditoria, amb justificació del seu abast i limitacions.

Llistat Detallat i Prioritari de Vulnerabilitats: Inventari exhaustiu de totes les vulnerabilitats detectades, classificades segons el seu nivell de risc (Crític, Alt, Mitjà, Baix) basant-se en criteris objectius com impacte potencial, explotabilitat i activius afectats. Cada vulnerabilitat anirà acompanyada d'una descripció tècnica, evidències de la seva existència (captures, sortides d'eines, etc.) i vectors d'atac associats.

Anàlisi d'Impacte i Risc: Avaluació global de l'impacte que les vulnerabilitats podrien tenir sobre la confidencialitat, integritat i disponibilitat dels sistemes i la informació de l'Institut.

Recomanacions Tècniques d'Actuació: Per a cada vulnerabilitat identificada, es proporcionaran una o més recomanacions tècniques específiques, accionables i detallades per a la seva correcció o mitigació efectiva.

Pla de Millora Continuada: Conjunt de bones pràctiques i recomanacions estratègiques per

millorar la postura de seguretat de l'organització a mitjà i llarg termini.

6.2. Termini de Lliurament

El lliurament de l'informe final es realitzarà en un termini màxim de set (7) dies naturals des de la data de finalització de totes les proves tècniques d'auditoria. Aquesta data de finalització serà comunicada per escrit pel Contractista al Client.

6.3. Format i Lliurament

L'informe es lliurarà en format PDF amb protecció contra modificacions.
Addicionalment, es facilitarà en format editable (com .docx o .odt) per a facilitar la revisió i incorporació de comentaris per part del Client.
El lliurament es realitzarà mitjançant un mitjà que permeti constanci de recepció (com correu electrònic amb acus de recepció o plataforma segura signada).

6.4. Versió Preliminar i Acceptació

Opcionalment, i d'acord amb el Client, es podrà lliurar una versió preliminar o draft de l'informe per a una revisió inicial abans de l'emissió de la versió final.

El Client disposarà de cinc (5) dies naturals des del lliurament de la versió final per a formular per escrit les seves observacions. Passat aquest termini, l'informe es considerarà acceptat tàcitament.

7. VIGÈNCIA I TERMINACIÓ

7.1. Vigència del Contracte

El present contracte entrarà en vigor en el moment de la seva signatura per ambdues parts i es mantindrà vigent fins al compliment integral de totes les obligacions aquí previstes, especialment fins al lliurament i acceptació expressa o tàcita de l'informe final per part del client.

7.2. Causes de Resolució

Qualsevol de les parts podrà resoldre el contracte, mitjançant notificació per escrit amb una antelació mínima de deu (10) dies naturals, en cas que es produeixi alguna de les següents circumstàncies:

Incompliment greu o reiterat de les obligacions essencials previstes en el contracte per part de

l’altra part.

Declaració de concurs, insolvència, dissolució o liquidació de qualsevol de les parts.

Causes de força major que impedeixin la continuació dels treballs durant un període superior a trenta (30) dies naturals.

7.3. Procediment de Resolució per Incompliment

Abans d’exercir el dret de resolució per incompliment, la part perjudicada haurà de notificar per escrit a l’altra part l’incompliment constatat, atorgant-li un termini de deu (10) dies naturals per a la seva subsanació. Si, transcorregut aquest termini, l’incompliment no hagués estat subsanat, es podrà procedir a la resolució del contracte.

7.4. Efectes de la Resolució

En cas de resolució del contracte, es procedirà a la liquidació dels treballs realitzats fins a la data de la resolució, que seran abonats en la proporció que correspongui. El contractista tindrà l’obligació de lliurar al client tots els documents, informes i resultats parcials obtinguts fins al moment de la resolució.

7.5. Obligacions Postcontractuals

Les clàusules relatives a confidencialitat, protecció de dades, propietat intel·lectual i responsabilitat mantindran la seva vigència després de la terminació o resolució del contracte, d’acord amb el que en elles es estableix.

8. PENALITZACIONS I INDEMNITZACIONS

8.1. Règim de Penalitzacions

S'estableixen les següents penalitzacions per a les infraccions contractuals:

Retard en el lliurament de l'informe: En cas de retard en el lliurament de l'informe final sense causa justificada, el Contractista abonarà una penalització equivalent al 2% del valor total del contracte (IVA exclòs) per cada setmana de retard, amb un màxim acumulat del 10% del valor del contracte.

Deficients en la qualitat del servei: Si es detecten deficiències substantives en la qualitat dels serveis prestats, imputables al Contractista, s'aplicarà una penalització equivalent al 3% del valor de la facturació mensual corresponent.

Incompliment del procediment de substitució de personal: L'incompliment dels terminis o procediments establerts per a la substitució de personal assignat al projecte comportarà una penalització equivalent a l'1% del valor total del contracte.

8.2. Responsabilitat per Danys i Perjudicis

El Contractista es farà responsable dels danys directes i efectivament produïts que es deriven de forma immediata i directa de l'execució de les proves d'auditoria, sempre que es demostri negligència greu o incompliment de les condicions acordades.

La responsabilitat màxima del Contractista queda limitada al valor total del contracte establert en la clàusula 3, excepte en casos de dolo o negligencia greu demostrada.

8.3. Procediment d'Aplicació de Penalitzacions

Abans de l'aplicació de qualsevol penalització, es requerirà al Contractista per escrit, atorgant-li un termini de 5 dies naturals per presentar les seves al·legacions.

Les penalitzacions es detrauran dels imports pendents de pagament al Contractista, o en cas que no n'hi hagi, es faran efectives amb càrrec a la garantia definitiva constituïda.

L'adjudicatari està obligat a respondre la garantia en la quantia que correspongui en un termini de 5 dies des de la seva execució.

8.4. Causes d'exempció de responsabilitat

Queden exemptes de responsabilitat les conseqüències derivades de:

- Cas de força major
- Errors o omissions en la informació facilitada pel Client
- Actuacions realitzades amb autorització expressa del Client
- Fallades dels sistemes del Client no imputables al Contractista

8.5. Complementarietat de les accions

L'aplicació de les penalitzacions previstes en aquesta clàusula no impedeix l'exercici d'altres accions que corresponguin legalment, inclosa la reclamació d'indemnització per danys i perjudicis quan les penalitzacions no cobrin la totalitat del dany sofert.

9. PROPIETAT INTEL·LECTUAL I LICENCES

9.1. Informes i Resultats:

Tots els drets de propietat intel·lectual sobre els informes, resultats i materials generats durant l'auditoria seran propietat de l'Institut Tecnològic de l'Ebre, atorgant-se a Fastclick Auditors una

llicència limitada per al seu ús intern i amb finalitats de millora dels seus serveis.

9.2. Eines i Programari:

L'empresa auditora garanteix que disposa de les llicències necessàries per a l'ús de les eines i programari utilitzats durant l'auditoria.

10. ACCEPTACIÓ I CONFORMITAT

Ambdues parts declaren haver llegit i comprendre totes i cadascuna de les clàusules d'aquest contracte, i manifesten la seva acceptació i conformitat amb el seu contingut, signant-lo en prova d'acord.

A Tortosa, a ____ de _____ de 2025.

Per l'Empresa Auditora (Fastclick Auditors):

Josep Pellisa
Signatura: _____

Ramon Aibar
Signatura: _____

Daniel Miron
Signatura: _____

Per l'Empresa Auditada (Institut Tecnològic de l'Ebre):

Jose Diego Cervellera
Signatura: _____