mediaservice.net
CORPORATE SECURITY & IMAGE

PROFILO SOCIETARIO

mediaservice.net
CORPORATE SECURITY & IMAGE

Via Santorelli, 15
10095 Grugliasco
Torino, ITALY
Tel. +39 011 3272100

www.mediaservice.net

1 Introduzione

1.1 Scopo del presente documento

Il presente documento presenta @ Mediaservice.net quale **Security Advisory Company**, unitamente alla competenze acquisite ed ai servizi erogati.

1.2 Presentazione dell'Azienda

Nata già nel 1997 come società di persone, costituita in società di capitale nel 2000, @ Mediaservice.net S.r.l. a partire da quella data è riorganizzata e consolidata dalla sua struttura aziendale originale da Daniele Poma (attuale Amministratore Unico).

Oggi, @ Mediaservice.net, è una **Security Advisory Company italiana**, a capitale interamente privato, che opera **sul mercato** della Sicurezza Informatica **da più di 15 anni**.

La missione di @ Mediaservice.net è **verificare, migliorare e mantenere il livello di sicurezza delle informazioni** dei Clienti e delle infrastrutture ICT ad essi collegate, operando in modo indipendente da Vendor, prodotti o tecnologie ed agendo in qualità di terza parte indipendente nel rispetto delle metodologie e *best practice* condivise a livello internazionale.

L'esperienza maturata e l'elevata professionalità delle risorse impiegate consentono a @ Mediaservice.net di posizionarsi tra le **aziende di riferimento a livello nazionale ed europeo** rispetto alle tematiche relative alla Sicurezza Proattiva (Corporate Protection, verifiche di sicurezza IT, Penetration Testing, Vulnerability Assessment, Risk Management), alla Sicurezza di Processo (ISO 27001, PCI DSS, security governance) e alla Formazione (esclusivisti per l'Italia di ISECOM OSSTMM).

I principali elementi caratterizzanti di @ Mediaservice.net sono l'elevato grado di **preparazione, esperienza, affidabilità e riservatezza** del personale, la partecipazione con ruoli attivi presso le principali associazioni ed organizzazioni di settore e gli elevati standard di qualità e di sicurezza che osserva nell'erogare i propri servizi ai Clienti, come più estesamente descritto nel seguito.

@ Mediaservice.net presidia il mercato Italiano attraverso la propria presenza su due sedi, entrambe dotata sia di personale tecnico, sia di staff manageriale:

- **Torino**, sede storica dell'azienda, la quale ospita la Direzione Generale
- **Roma**, filiale con competenza territoriale Centro-Sud Italia

1.3 Competenze e Certificazioni

Il personale impiegato da @ Mediaservice.net è composto da professionisti del settore con una **solida e comprovata esperienza**, in possesso di certificazioni professionali internazionalmente riconosciute quali:

Figura 1 - Competenze e certificazioni del personale di @ Mediaservice.net

1.4 Certificazione PCI DSS

@ Mediaservice.net è stata certificata dal PCI Security Council in qualità di QSA Company (Qualified Security Assessors) da Ottobre 2009 e ASV Company (Approved Scanning Vendor) da Luglio 2011.

Figura 2 - Certificazione PCI-DSS di @ Mediaservice.net

1.5 Ruoli attivi in associazioni di settore

Una delle caratteristiche salienti di @ Mediaservice.net è quella di utilizzare **metodologie e best practice** internazionali, **contribuendo allo sviluppo** delle stesse e ricoprendo ruoli attivi nella loro gestione e divulgazione.

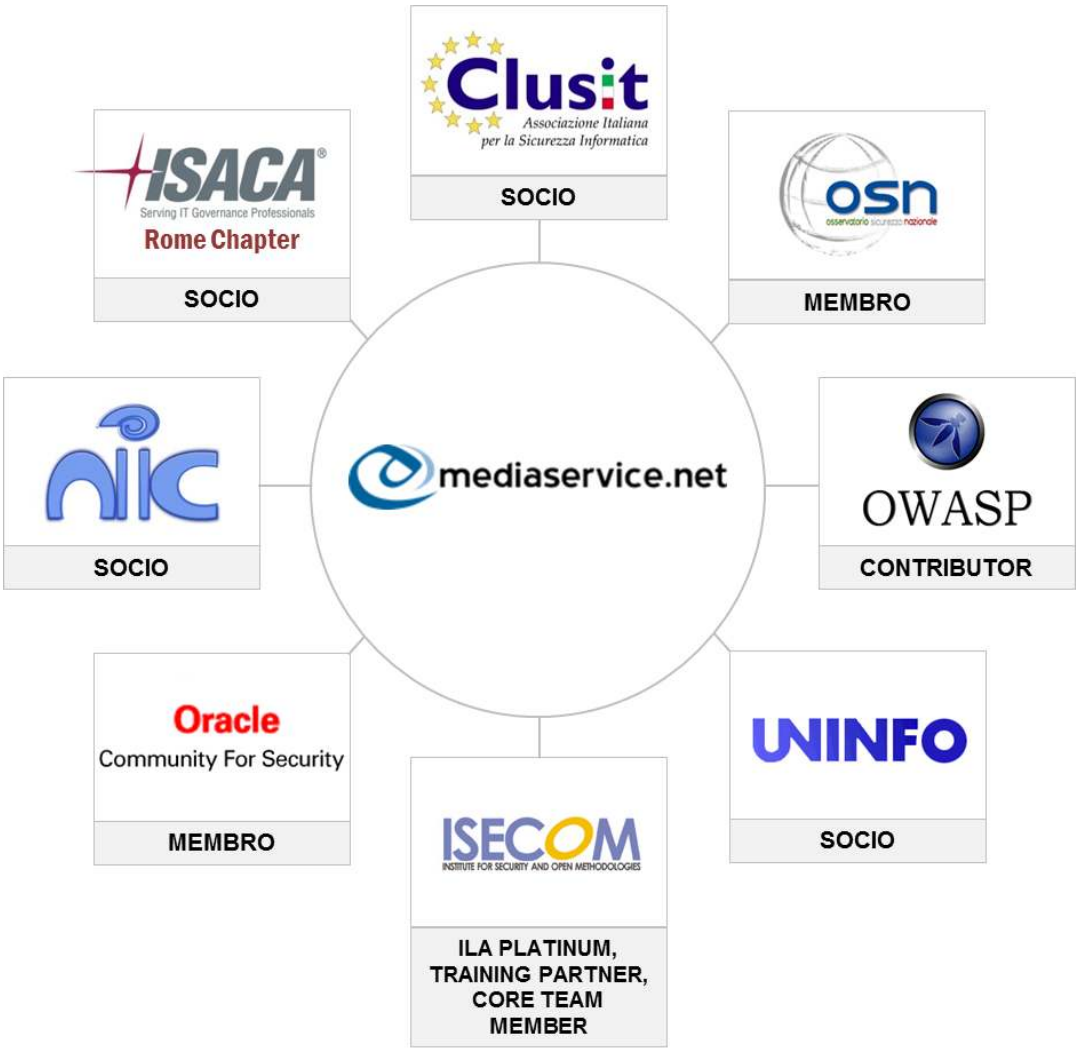

Figura 3 - Ruoli attivi di @ Mediaservice.net in associazioni di settore

1.6 Sistema di gestione integrato per qualità e sicurezza

@ Mediaservice.net, al fine di garantire ai suoi Clienti il livello di eccellenza raggiunto dai propri servizi di Security Advisoring, ha ritenuto di strategica importanza **certificare e mantenere allineati la propria struttura e la competenza del proprio personale** verso i più prestigiosi schemi presenti sul mercato internazionale (UNI EN ISO 9001:2008 e ISO/IEC 27001:2005).

Il coronamento di questa attenzione storica di @ Mediaservice.net verso la qualità e la sicurezza di processo è arrivato a Marzo 2012 con il **conseguimento della certificazione del Sistema Integrato per la Sicurezza delle Informazioni e per la Qualità** (SGI) da parte di DNV Italia, impostato sull'ambito di "Progettazione ed erogazione di servizi di Advisory e formazione in materia di sicurezza delle informazioni".

1.6.1 Responsabilità

@ Mediaservice.net è assicurata con i **LLOYD'S di Londra e con Gruppo Fondiaria SAI** al fine di garantire la massima copertura ai propri Clienti a fronte di improbabili ma comunque possibili eventi dannosi derivanti dall'esercizio delle proprie attività di Advisoring.

Tali coperture assicurative sono valide a livello mondiale e coprono i seguenti punti secondo specifici massimali:

- RCO (Responsabilità civile verso prestatori di lavoro);
- RCT (Responsabilità civile verso terzi);
- Indennità professionale;
- Infedeltà dei dipendenti;
- Danneggiamento di siti Internet;
- Responsabilità verso i propri prodotti (Product Liability);
- Responsabilità ambientale (Pollution Liability);
- Protezione del marchio (Brand Protection);
- Spese legale.

Mediante richiesta scritta, @ Mediaservice.net, potrà fornire copia delle suddette polizze complete di indicazione dei relativi massimali.

1.7 Elementi distintivi di @ Mediaservice.net

Alcuni fattori, patrimonio genetico di @ Mediaservice.net, caratterizzano l'azienda rispetto al mercato di riferimento ed ai competitors.

Tra questi:

- **@ Mediaservice.net è una Security Advisory Company**
  Il nostro obiettivo è supportare il Cliente nel comprendere ed indirizzare i problemi legati alla sicurezza informatica

- **Seniority decennale nell'approccio della sicurezza a 360°**
  Dalla Sicurezza Proattiva alla Security Governance

- **15 anni di presenza sul mercato della Sicurezza IT**
  La nostra esperienza, affidabilità e riservatezza quali garanzie del vostro investimento

- **Condotta Etica**
  Rispettiamo rigide linee di condotta ed un codice etico internazionale che ci impongono un comportamento al di sopra delle parti, rispettoso prima di tutto delle informazioni e dei valori dei nostri Clienti

- **100% del personale assunto e con basso turnover**
  A maggior tutela delle informazioni sensibili del Cliente

- **100% del personale certificato in metodologie internazionali**
  Garanzia di costante aggiornamento e di eticità.

- **Vendor Neutral, Product Independent**
  Indirizziamo le necessità dei Clienti verso la soluzione più adeguata

- **Nessuna tecnologia proprietaria, solo standard di mercato cui contribuiamo**
  I risultati delle nostre attività possono essere riprodotti anche dal Cliente stesso

- **Abbiamo formato il 100% dei professionisti ISECOM OSSTMM certificati in Italia**
  La formazione è uno dei metodi con i quali trasferiamo il nostro know how.

2 Standard di riferimento e Metodologie

Al fine di fornire un supporto consistente e interoperabile in tema di sicurezza delle informazioni, @ Mediaservice.net si basa sui **principali standard di mercato** per strutturare le attività di Advisoring svolte presso i Clienti. Secondo la tipologia di servizio, per l'attività operativa sono utilizzati diversi riferimenti nel seguito trattati in dettaglio.

2.1 ISO/IEC 27001

Questa norma di valenza internazionale costituisce sempre più il riferimento universalmente riconosciuto per attuare una corretta gestione della sicurezza delle informazioni. La norma, originata dall'inglese BS 7799-2, intende evidenziare con il concetto di "**Sistema di Gestione per la Sicurezza delle Informazioni**" (SGSI, in inglese ISMS) che non è sufficiente sviluppare un insieme di controlli e procedure per la sicurezza, ma occorre gestirli e mantenerli nel tempo attraverso l'impostazione e l'attuazione di processi e attività specifiche.
La sicurezza viene appunto vista come un insieme di processi ciclici ad ogni livello e la norma si concentra su aspetti di gestione della sicurezza, definendo un catalogo di contromisure di sicurezza ad un livello tale che possano essere applicate ad ambienti, sistemi e procedure diverse all'interno di qualsiasi tipologia di azienda.

I passi principali per gestire la sicurezza delle informazioni secondo questa norma possono essere efficacemente riassunti tramite il paradigma ciclico PDCA (Plan, Do, Check, Act) così inteso:

Figura 4 - Ciclo PDCA del SGSI

Il motore principale di questo paradigma è la **valutazione del rischio** (Risk Assessment) in base alla quale si stabilisce cosa è opportuno mettere in campo, da un **punto di vista tecnologico ma anche organizzativo**, per soddisfare i requisiti di sicurezza fissati precedentemente. Come per un sistema di gestione della qualità conforme alla UNI EN ISO 9001, è anche possibile arrivare a certificare un SGSI in modo da poterne dimostrare in modo esplicito la validità a clienti e fornitori.

2.2 OSSTMM

Le attività di verifica dei sistemi, delle reti e dei dispositivi sono condotte in conformità con l'**Open Source Security Testing Methodology Manual** (OSSTMM), lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza, sviluppato da ISECOM tramite il modello peer review.

ISECOM (Institute for Security and Open Methodologies) è un'**organizzazione internazionale di ricerca** senza scopo di lucro, fondata nel 2001 al fine di sviluppare e condividere metodologie aperte nel campo della sicurezza delle informazioni. ISECOM è inoltre un'**autorità di certificazione** sostenuta da partner istituzionali.

OSSTMM è una metodologia scientifica che definisce esattamente quali elementi devono essere verificati, che cosa occorre fare prima, durante e dopo i test di sicurezza e come misurare i risultati ottenuti. Consente pertanto di valutare sul campo in modo consistente e ripetibile la superficie di attacco relativa al contesto oggetto di analisi.

La metodologia OSSTMM ha introdotto numerosi nuovi concetti nella disciplina della Sicurezza Proattiva, quali: OPSEC e controlli, Competitive Intelligence (CI), metriche per misurare la superficie di attacco (RAV), reportistica certificata (STAR). Una verifica di sicurezza conforme allo standard OSSTMM assicura:

- **Esaustività e profondità** dei test, con riduzione sostanziale dei falsi positivi e negativi.
- Conclusioni oggettivamente derivate dai risultati dei test stessi, tramite applicazione del **metodo scientifico**.
- **Rispetto di politiche, normative e leggi** vigenti applicabili al contesto oggetto di analisi.
- Risultati **consistenti e ripetibili**.
- Risultati **misurabili e quantificabili** secondo precise regole.
- La **reportistica certificata** costituisce la prova di un test basato sui fatti e rende gli analisti responsabili dell'audit.

La verifiche di sicurezza condotte con questa metodologia possono essere *opzionalmente* accreditate e certificate STAR OSSTMM 3.0 presso l'ente internazionale ISECOM. Tramite il calcolo del RAV e l'emissione di reportistica STAR certificata, OSSTMM consente al Cliente di ottenere le risposte alle seguenti domande fondamentali:

- *Quanto dobbiamo investire nella sicurezza?*
- *Su quali aspetti dobbiamo concentrarci in modo prioritario?*

- *Di quali soluzioni di sicurezza abbiamo bisogno?*
- *Quanto migliora il livello di sicurezza a seguito dell'adozione di specifiche contromisure?*
- *Come possiamo misurare i risultati dei piani correttivi?*
- *Come possiamo sapere se stiamo riducendo l'esposizione alle minacce?*
- *Quanto è resistente un determinato componente?*
- *Come possiamo ottenere conformità e sicurezza?*

L'obiettivo finale di una verifica conforme allo standard OSSTMM, pertanto, è fornire un processo concreto per essere funzionalmente sicuri.

2.3 OWASP

Le attività di analisi condotte sulle applicazioni web sono conformi alla **OWASP Testing Guide**, lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza applicative, sviluppato da OWASP tramite il modello peer review.

OWASP (Open Web Application Security Project) è una **comunità internazionale di ricerca** senza scopo di lucro, fondata nel 2001 al fine di aumentare la robustezza del software applicativo, promuovendo lo sviluppo ed il mantenimento di applicazioni web sicure.

La OWASP Testing Guide è un framework di verifica che descrive nel dettaglio come rilevare le problematiche di sicurezza associate al software applicativo. In particolare, essa fornisce gli strumenti metodologici per comprendere quando, come ed in che modo analizzare le applicazioni web. Una verifica di sicurezza conforme allo standard OWASP consente di rilevare le seguenti classi di problematiche[1]:

- **Injection** (in particolare SQL Injection)
- **Cross-Site Scripting** (XSS)
- **Broken Authentication and Session Management**
- **Insecure Direct Object References**
- **Cross-Site Request Forgery** (CSRF)
- **Security Misconfiguration**
- **Insecure Cryptographic Storage**
- **Failure to Restrict URL Access**
- **Insufficient Transport Layer Protection**
- **Unvalidated Redirects and Forwards**

[1] Cfr. Open Web Application Security Project Top 10 2010 (https://www.owasp.org/index.php/Top_10_2010)

2.4 Altri Riferimenti

Nell'ambito dei progetti sono inoltre considerate le seguenti norme e leggi:

- ISO/IEC 19011:2011 – *Guidelines for quality and/or environmental management;*
- ISO/IEC 20000-1:2011 – *Service management – Part 1: Specification;*
- ISO/IEC 27001:2013 – *Information Security Management System;*
- ISO/IEC 27002:2013 – *Code of practice for information security management;*
- ISO/IEC 27004:2009 – *Information security management – Measurement;*
- ISO/IEC 27005:2011 – *Information security risk management;*
- ISO 22301:2012 – *Societal security – Business continuity management system;*
- ISO 31000*:2009 – Risk management – Principles and guidelines;*
- ISO/EIC 38500*:2008 – Corporate governance of information technology;*
- COBIT v5.0 – *Control Objectives for Information and related Technologies;*
- OSSTMM v3 – *Open Source Security Testing Methodology Manual;*
- OWASP Testing Guide v3 – *Open Web Application Security Project Testing Guide;*
- CC v3.1 – *Common Criteria;*
- CEM v3.1 – *Common Methodology for Information Technology Security Evaluation;*
- ITIL v3 – *Information Technology Infrastructure Library;*
- PCI DSS v2.0 – *Payment Card Industry Data Security Standard;*
- Basilea2 – *International Convergence of Capital Measurement and Capital Standards;*
- SOX of 2002 – *Public Company Accounting Reform and Investor Protection Act;*
- D.Lgs. 231/2001 – *Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*;
- D.Lgs. 196/2003 – *Codice in materia di protezione dei dati personali;*
- D.Lgs. 262/2005 – *Tutela del risparmio e disciplina dei mercati finanziari;*
- D.Lgs. 81/2008 – *Tutela della salute e della sicurezza nei luoghi di lavoro*.

3 L'Offerta

3.1 Portafoglio di offerta

Dipendentemente dal livello di approfondimento che si intende raggiungere, @ Mediaservice.net offre differenti tipologie di verifica. Lo schema seguente riassume tutti i **Servizi di Sicurezza** erogati:

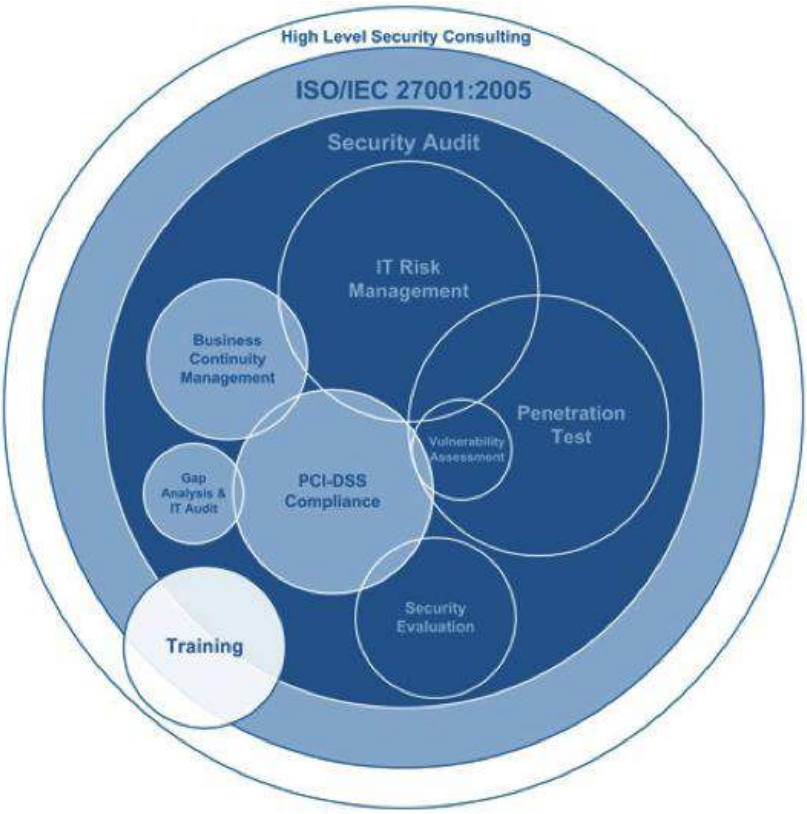

Figura 5 - Servizi di Sicurezza, Copyright © 2000-2011 @ Mediaservice.net

Tali servizi, meglio descritti nei paragrafi seguenti, possono essere raggruppati in tre macro categorie:

1. Sicurezza Proattiva
2. Sicurezza di Processo
3. Formazione

3.2 Servizi di sicurezza proattiva

3.2.1 Vulnerability Assessment

La verifica di sicurezza di tipo **Vulnerability Assessment** costituisce il primo livello dei servizi di Sicurezza Proattiva. Essa **prevede l'esecuzione di scansioni automatizzate e semi-automatizzate non invasive**, condotte avvalendosi di strumenti software open source e proprietari accuratamente selezionati, al fine di rilevare la presenza di vulnerabilità note all'interno dell'infrastruttura informatica oggetto di analisi. Tali scansioni sono successivamente integrate da verifiche manuali eseguite da personale altamente qualificato, volte ad eliminare i falsi positivi e negativi eventualmente introdotti dagli strumenti di analisi automatica.

Isolando tempestivamente le reali vulnerabilità presenti sul perimetro della rete pubblica o all'interno della rete privata, il servizio di Vulnerability Assessment consente al Cliente di mantenere una visione aggiornata del grado di robustezza dei propri sistemi informatici, ottimizzando gli sforzi di gestione della sicurezza.

3.2.2 Penetration Test

Il servizio di verifica di sicurezza di tipo **Penetration Test** prevede l'**esecuzione di test approfonditi in modalità Ethical Hacking**. Esso si basa su tecniche di attacco inferenziali finalizzate all'identificazione delle vulnerabilità non note o comunque non rilevabili tramite i soli strumenti di scansione ed analisi automatica. L'attività di verifica si avvale delle competenze e dell'esperienza di personale altamente qualificato, allo scopo di simulare nel modo più esaustivo possibile le operazioni comunemente eseguite da un agente di minaccia esterno o interno**,** facendo uso degli strumenti e delle tecniche proprie di uno scenario reale.

Il servizio di Penetration Test consente il rilevamento sul campo delle eventuali vulnerabilità tecnologiche presenti all'interno dell'infrastruttura informatica oggetto di analisi. Esso permette, inoltre, di verificare l'adeguatezza delle politiche di sicurezza adottate ed il livello di rispetto delle stesse da parte del personale.

3.2.3 Security Evaluation

Il servizio di Security Evaluation prevede la **verifica in ambiente di laboratorio del livello di sicurezza associato a particolari processi, applicazioni, piattaforme hardware e software dalle caratteristiche eterogenee**. Al fine di garantire la massima profondità ed esaustività dell'analisi di sicurezza, la valutazione è eseguita sistematicamente sia a livello progettuale che implementativo, avvalendosi delle competenze e dell'esperienza di personale altamente qualificato. Il servizio comprende attività quali: reverse engineering, analisi dei protocolli di comunicazione, verifica dei meccanismi di cifratura, revisione del codice sorgente e delle configurazioni adottate.

Il servizio di Security Evaluation consente il rilevamento sul campo delle eventuali vulnerabilità progettuali o implementative presenti sulle piattaforme hardware e software oggetto di analisi. Permette, inoltre, di verificare l'adeguatezza delle procedure di sviluppo e deployment adottate ed il livello di rispetto delle stesse da parte del personale.

3.2.4 IT Risk Management

Il Risk Management **è il processo che permette di essere consapevoli, prima, e di gestire, poi, i rischi a cui sono sottoposti gli asset aziendali**. In ambito IT, tale processo consente di definire le linee guida per la pianificazione degli investimenti e delle attività, al fine di ridurre i rischi ed aumentare il livello di sicurezza associato ad un'infrastruttura informatica. Componenti importanti di questo servizio sono il Risk Assessment e il Risk Treatment:

- **Risk Assessment**: identificazione del contesto di attività e valorizzazione dei parametri di contorno fondamentali (asset, vulnerabilità, minacce, impatti, contromisure), al fine di valutare il livello di rischio residuo.
- **Risk Treatment**: qualora il rischio rilevato superi il livello di rischio definito come accettabile, vengono progettate, valutate e messe in opera opportune attività correttive di rientro.

I risultati possono essere espressi sia su **scala qualitativa**, sia su **scala quantitativa** (in euro).

@ Mediaservice.net, oltre ad impiegare metodologie e modelli di analisi già in uso presso i Clienti, seppur privilegi l'approccio suggerito da ISO/IEC 27005:2011 e ISO 31000:2009, è solita utilizzare le più evolute metodologie di analisi del rischio, effettuandone specifiche personalizzazioni al fine di incontrare al meglio le necessità evidenziate dal Cliente.

3.2.5 Security Audit

Il servizio di Security Audit costituisce un'innovazione in materia di valutazione del rischio IT, **combinando in un'unica attività le discipline del Penetration Test e del Risk Assessment**.

Il risultato di questa sinergia è un'analisi estremamente approfondita, finalizzata a determinare con precisione (anche quantitativa) il livello di sicurezza dell'infrastruttura informatica del Cliente, tramite l'impiego di metodologie formali di assessment tecnologico ed organizzativo.

La forte interazione tra queste due differenti tipologie di verifica consente di:

- **ottimizzare l'esecuzione delle verifiche tecnologiche**, razionalizzando gli effort e pesando al meglio le vulnerabilità e le esposizione rilevate;
- **migliorare la precisione della valutazione del rischio** e della successiva mitigazione, includendo un livello di dettaglio tecnico.

3.2.6 High Level Security Consulting

L'High Level Security Consulting è il **servizio di consulenza di più ampio respiro, che comprende qualsiasi argomento inerente la sicurezza informatica** (intesa sia da un punto di vista procedurale sia tecnologico) e che soddisfa esigenze puntuali non altrimenti comprese nell'offerta di @ Mediaservice.net.

Il servizio di High Level Security Consulting si avvale dell'esperienza del **personale altamente specializzato** di @ Mediaservice.net, il quale possiede competenze e capacità che gli consentono

di soddisfare qualsiasi necessità di sicurezza, in un'ampia gamma di scenari tecnologici. Seguono alcuni esempi delle tipologie di offerte più richieste:

- Revisione dei processi
- Progettazione sicura
- Stesura della documentazione
- Competitive Intelligence (CI)

3.3 Servizi di Sicurezza di processo

3.3.1 Gap Analisys & IT Audit

La **Gap Analysis** è un'attività volta a individuare la distanza (il Gap) tra una situazione reale e una norma, una legge o un qualsiasi insieme di requisiti, esaminandola in modo esaustivo. L'output di questa attività è una descrizione puntuale degli elementi mancanti per colmare tale distanza.

L'**IT Audit** è invece un processo formale per valutare la conformità rispetto a una norma, legge o policy aziendale individuata come requisito. Questa analisi viene effettuata a campione, seguendo l'impostazione definita dalla ISO 19011:2011 e i criteri di ISACA, producendo quindi una serie di evidenze a supporto delle conclusioni di conformità o di non conformità. Gli audit possono essere di prima parte (interni), di seconda (commissionati da un fornitore/cliente) o di terza parte (esterni).

I criteri utilizzabili per entrambi i servizi sono: ISO/IEC 27001:2013 o altre della famiglia 27000, D.Lgs. 196/03 e D.Lgs. 231/01, ISO/IEC 20000-1:2011 e ITIL 3, COBIT 5, PCI DSS 2.0, ISO/IEC 38500:2008, ISO 22301:2012) e altre.

3.3.2 ISO/IEC 27001:2013

La norma internazionale ISO/IEC 27001:2013 è finalizzata all'impostazione e applicazione di un Sistema per la Gestione della Sicurezza delle Informazioni (SGSI) allineandola con i requisiti di business aziendali. In estrema sintesi il SGSI è basato sul concetto di valutazione iniziale del rischio e di successiva implementazione delle contromisure necessarie a ridurlo ad un livello accettabile**.**

@ Mediaservice.net ha sviluppato un'offerta per supportare ogni tipologia di Cliente per l'**impostazione strutturata della gestione della sicurezza delle informazioni**, incentrata sulla crescita e sul successo del Cliente. L'offerta è completa, in grado di coprire e di centralizzare tutti i requisiti di sicurezza, legali o di business, e permette di affrontare in modo strutturato ogni problematica legata alla sicurezza delle informazioni. Questo approccio è personalizzabile secondo le necessità e la disponibilità di ogni realtà aziendale, è rivolto al miglioramento continuo e può essere **certificato in modo formale in conformità alla ISO/IEC 27001:2013**.

3.3.3 Business Continuity Management

Per Business Continuity Management (BCM) si intende la capacità dell'azienda di **continuare a svolgere la propria operatività e quindi il proprio business in seguito al manifestarsi di incidenti o di eventi catastrofici**. La gestione della continuità operativa e di servizio (o BCM) è un processo che:

- Identifica i potenziali incidenti in grado di minacciare la continuità del business aziendale;
- Fornisce una struttura in grado di organizzare una risposta a fronte del verificarsi di interruzioni dei processi di core business;
- Riduce i rischi correlati alla continuità aziendale e ne gestisce le conseguenze sul piano gestionale, amministrativo e legale

Rientrano in questo ambito la stesura e la revisione dei piani di gestione degli incidenti (Incident Management Plan - **IMP**), della continuità operativa (Business Continuity Plan - **BCP**) e di disaster recovery (Disaster Recovery Plan - **DRP**), in conformità a quanto previsto dagli standard di riferimento serie ISO/IEC 22301:2012 e ISO/IEC 24762:2008.

3.3.4 Conformità a PCI DSS

PCI DSS è l'acronimo di Payment Card Industry Data Security Standard. È, a tutti gli effetti, una norma internazionale di sicurezza creata da un consorzio formato dai principali operatori del settore **carte di pagamento** per ridurre i rischi di sicurezza per **esercenti e fornitori di servizi** che utilizzano carte di pagamento.

La norma si articola in una serie di requisiti di sicurezza afferenti agli ambienti in cui i dati delle carte sono memorizzati, elaborati o trasmessi, requisiti finalizzati a minimizzare le probabilità che si verifichino eventi dannosi e a contenerne le conseguenze. La sua impostazione è allineata con le best practice di settore.

L'approccio di @ Mediaservice.net parte dal supportare il Cliente nelle fasi di verifica delle vulnerabilità trimestrali e nell'esecuzione annuale dell'audit.

3.3.5 High Level Security Consulting

L'High Level Security Consulting è il **servizio di consulenza di più ampio respiro, che comprende qualsiasi argomento inerente la sicurezza informatica** (intesa sia da un punto di vista procedurale, sia tecnologico) e che soddisfa esigenze puntuali non altrimenti comprese nell'offerta di @ Mediaservice.net.

Il servizio di High Level Security Consulting si avvale dell'esperienza del personale altamente specializzato di @ Mediaservice.net, il quale possiede competenze e capacità che gli consentono di soddisfare qualsiasi necessità di sicurezza, in un'ampia gamma di scenari tecnologici.

Tra le tipologie di offerte più richieste si incontrano la revisione dei processi, la progettazione sicura, la stesura della documentazione e la competitive intelligence (CI).

3.4 Formazione

3.4.1 Analisys & Testing

- Corsi Introduttivi e Corsi Propedeutici
  Preparano il candidato ad acquisire le competenze tecniche ed analitiche necessarie ad **eseguire verifiche e analisi di sicurezza**: è il know-how di base spesso richiesto quale primo passo del percorso di certificazione ISECOM.

- Corsi di Certificazione Internazionale ISECOM
  I percorsi formativi ISECOM, erogati in Italia in forma esclusiva da @ Mediaservice.net, in qualità di ISECOM Training Partner, prevedono un **esame di certificazione finale**, che dà diritto a un **titolo riconosciuto a livello internazionale**; queste certificazioni, così come la perfetta conoscenza della metodologia OSSTMM (Open Source Security Testing Methodology Manual) ed il rispetto totale delle regole di ingaggio**,** sono requisiti sempre più spesso richiesti come obbligatori in bandi di gara nazionali ed internazionali, ma anche titolo preferenziale nella selezione di personale addetto alla sicurezza informatica.

  Le certificazioni accreditate da ISECOM sono le seguenti:

  - **OSSTMM Professional Security Tester** (OPST) è la certificazione professionale ufficiale per l'esecuzione ed il reporting di test di sicurezza conformi alla metodologia OSSTMM di ISECOM ;
  - **OSSTMM Professional Security Analyst** (OPSA) è la certificazione professionale ufficiale per l'analisi della sicurezza, in conformità alla metodologia OSSTMM di ISECOM;
  - **OSSTMM Wireless Security Expert** (OWSE) è la certificazione professionale ufficiale per l'esecuzione di test di sicurezza Wireless conformi alla metodologia OSSTMM di ISECOM;
  - **OSSTMM Professional Security Expert** (OPSE) è la certificazione professionale ufficiale che attesta l'approfondita conoscenza della metodologia OSSTMM di ISECOM.

3.4.2 Compliance & Governance

Questi corsi hanno l'obiettivo di **formare** i partecipanti in modo specifico e verticale su due diverse tematiche**:** la **compliance a una norma o a uno standard di settore** e la **governance dell'Information Security**.

- Nel primo caso i discenti al termine del corso saranno in grado di coordinare in prima persona tutte le attività necessarie al raggiungimento e mantenimento della conformità alla norma prescelta;
- Nel secondo caso il corso è finalizzato a trasmettere la conoscenza essenziale a mantenere con successo l'allineamento della sicurezza IT con i requisiti del business.

3.4.3 IT Risk Management

Questo corso introduce il discente alle tematiche di **Risk Management e Business Impact Analysis i**n ambito IT, partendo dalle metodologie e dagli standard internazionali e focalizzandosi, in seguito, sull'applicazione pratica delle metodologie definite da ISO/IEC 27005 e ISO 31000 su case study reali, trasferendo nozioni facilmente applicabili anche ad altri soggetti e situazioni.

3.4.4 Corporate Education

Il pacchetto formativo è orientato a fornire ai partecipanti, in 1 o 2 giornate di formazione, una visione generale e adatta ad un pubblico non specializzato su tematiche specifiche, quali:

- programmazione sicura e OWASP;
- norme ISO/IEC 27001 o PCI DSS;
- introduzione alla computer forensics;
- overview sulla sicurezza delle informazioni;
- data privacy e policy interne.

Questa tipologia di corsi viene tipicamente erogata su richiesta con una forte personalizzazione dei contenuti in modo da poter meglio rispondere alle esigenze del Cliente e della realtà in cui opera. I corsi possono essere erogati ad un numero elevato di discenti, inquadrandosi come seminario o giornate di studio annesse a conferenze. Il pacchetto formativo si confeziona con successo anche all'interno di realtà aziendali che necessitano di diffondere alle proprie risorse regolamenti interni, requisiti cogenti, vincoli di legge o politiche aziendali.

In casi specifici e in base al contenuto destinato ad essere trasmesso, questi corsi possono essere organizzati ed erogati sotto forma di webcast o più in generale remotamente attraverso streaming multimediali.