www.ads.it

L'offerta IT
Security & Infrastructures

ADS

IT Security
Offerta e Certificazioni

Offerta e Certificazioni

L'offerta IT Security & Infrastructures è così articolata:

> IT Security Consulting: attività consulenziali in cui ci si propone in qualità di trusted advisor su tutte le tematiche inerenti il processo di gestione della sicurezza informatica e della privacy;

> IT Security Design & Deploy: supporto nella progettazione ed implementazione sicura dei sistemi informativi con l'obiettivo di proteggere i dati e le comunicazioni, sia attraverso soluzioni open source che attraverso l'integrazione di prodotti commerciali;

> IT Infrastructures Design & Deploy: supporto nella progettazione ed implementazione di sistemi di monitoraggio della disponibilità e delle prestazioni dei sistemi informativi, di soluzioni per la razionalizzazione delle risorse elaborative e gestione della continuità operativa con una attenzione particolare alle tecnologie innovative.

Modalità di erogazione dei servizi

Le attività vengono proposte secondo una strategia di partnership con il cliente onde massimizzare l'impegno delle risorse e di conseguenza ridurre i costi. Gli interventi si prefiggono un obiettivo prefissato, rappresentato dalla consegna di un "deliverable", sia sotto forma di un documento di analisi condiviso con il cliente che di un sistema oggetto di collaudo positivo rispetto alle specifiche di progetto. Qualora il Cliente manifestasse l'esigenza di avere un supporto consulenziale "a servizio" sulle tematiche oggetto dell'offerta sarà possibile fornire un'assistenza personalizzata Nel caso di progetti complessi oppure con tempistiche ristrette è possibile attingere ad un network professionale qualificato.

Partnership tecnologiche di Settore

Partner	Livello	Prodotti
ZABBIX	Certified Partner	System Monitoring
FORTINET SILVER PARTNER	Silver Partner	Firewall, UTM
vmware professional PARTNER	Professional Partner	Software per la virtualizzazione
Cisco Systems Registered Partner	Registered Partner	Apparati di rete

Certificazioni Professionali

Ambito	Organizzazione	Acronimo	Certificazione
IT Security	GIAC	GCFW	Giac Certified Firewall Analyst
	GIAC	GCFA	Giac Certified Forensic Analyst
	ISACA	CISA	Certified Information System Auditor
	ISECOM	OPST	OSSTMM Professional Security Tester
	Fortinet	FCNSA	Fortinet Certified Network Security Administrator (2)
IT Infrastructures	VMware	VCP	Vmware Certified Professional (2)
	Cisco	CCNA	Cisco Certified Network Associate
	Zabbix	ZCS	Zabbix Certified Specialist (3)
	Zabbix	ZCLE	Zabbix Certified Large Environment (3)
	Oracle	OCP	Oracle Certified Professional

dati aggiornati a febbraio 2017

IT Security Consulting

Cybersecurity

Assessment delle misure organizzative e tecnologiche

L'obiettivo di queste attività è duplice: la valutazione oggettiva dell'adozione delle principali contromisure volte a ridurre i rischi incombenti sulla confidenzialità, integrità e disponibilità dei dati trattati dal sistema informativo aziendale e la definizione di un percorso ottimizzato e virtuoso in grado di assicurare all'organizzazione un livello di rischio accettabile.

Conformità normativa e Best Practices

> Normativa europea: General Data Protection Regulation (GDPR),
> Network Information Security (NIS)
> Standard ISO 27001, ISO 22301
> NIST Cybersecurity Framework
> Normativa di settore (Bancario, Codice Amministrazione, Digitale PA)
> 20 Critical Security Controls CIS & SANS
> OWASP Top20 e Mobile Top10

Risk Analysis & Management

> Metodologia VERA
> ENISA Threat Taxonomy
> Adeguamento ai controlli ISO 27001 e Critical Security Controls

Vulnerabilty Assessment & Penetration Testing

> Metodologie OSSTMM & OWASP
> CVSS - Common Vulnerability Scoring System evaluation
> Vulnerability Management
> Penetration Testing di tipo infrastrutturale ed applcativo

Progettazione Infrastrutture ed applicazioni sicure

> Applicazione dei requisiti Security by Design e Defense in Depth
> Integrazione dispositivi sicurezza (Firewall, HIDS, NIPS, NBA, Anti APT, SIEM)
> Supporto adozione principi Secure Coding di applicazione software

Business Continuity & Disaster Recovery

> Business Impact Analysis
> Continuity Planning
> Redazione Piani di Continuità Operativa e Disaster Recovery

SOC (Security Operation Center) Setup & Operation

> Definizione requisiti progettazione SOC
> Definizione KPI, Maturity Model
> Integrazione indicatori ETSI ISI (Information Security Indicators)
> Gestione incidenti di sicurezza, attività di Digital Forensics

Campagne di Training ed Awareness

> Securing The Humans
> Campagne Anti Phishing
> Training tecnico
> Formazione del management

IT Security Consulting

Nuovo Regolamento Europeo sulla Data Protection - Legge 679/2016

Il 24 maggio 2016 è entrato in vigore a livello comunitario il Regolamento Europeo sulla Data Protection, che armonizza e sostituirà, con requisiti più attuali, le normative nazionali dei 28 paesi UE in materia di protezione dei dati. Tale provvedimento normativo offre maggiori tutele ai cittadini interessati dal trattamento informatico dei dati personali e prevede l'adozione di maggiori cautele da parte delle organizzazioni titolari delle suddettie attività, oltre all'obbligo di notifica degli episodi di data breach. Il tempo fissato per l'adeguamento alle disposizioni normative è di due anni, trascorsi i quali scatterà l'applicazione delle sanzioni che potranno avere degli impatti economici rilevanti, per cui è fondamentale che le organizzazioni pianifichino accuratamente e con tempestività il percorso da intraprendere verso la conformità.

Introduzione al tema

> Principali novità, cosa cambia rispetto alla legge sulla Privacy (D.Lgs 196/2003)
> Ambito di applicazione, nuovi ruoli e responsabilità, organizzazione a supporto
> Misure idonee di protezione, obbligo segnalazione episodi di data breach
> Provvedimenti sanzionatori

Percorso di conformità

> Mappatura dell'organizzazione e dei trattamenti
> Analisi dei rischi
> Privacy Impact Assessment
> Accountabilty, definizione di ruoli e responsabilità, la nuova figura del Data Protection Officer
> Verifica applicazione concetti Privacy by Design/Privacy by Default
> Supporto nell'implementazione delle misure organizzative e tecnologiche
> Attivazione del processo di notifica episodi di Data Breach

Sicurezza Organizzativa, Compliance & Data Protection

Attività di consulenza di alto livello per l'analisi e la gestione dei rischi onde migliorare la sicurezza, rispetto agli aspetti organizzativi, procedurali, tecnologici e fisici.
La rilevazione dello scenario avviene tramite interviste al personale, acquisizione di documentazione e di dati contenuti nei sistemi informativi; attraverso l'opportuna elaborazione delle informazioni raccolte si ottiene una valutazione attendibile del livello corrente di sicurezza.
La valutazione della sicurezza rispetto agli standard ISO 2700X, è basata su standard riconosciuti a livello globale; la conformità alle best practices di settore è una prerogativa molto richiesta per erogare servizi informatici ai propri clienti.
Nell'ambito specifico della Continuità Operativa l'offerta prevede gli interventi propedeutici alla redazione dei piani di BC/DR resi obbligatori dalle norme contenute, in ambito PA, nel Codice di Amministrazione Digitale (art 50 bis).
Viene inoltre offerto supporto sulle tematiche relative alla Privacy: Codice sulla protezione dei dati personali (D.Lgs.196/03), provvedimento del Garante sugli Amministratori di Sistema, aspetti legali e contrattuali in materia di Cloud Computing.

IT Security Consulting

Valutazione livello di sicurezza dell'infrastruttura IT

La proposta prevede di effettuare degli interventi tecnici attraverso l'esecuzione di un audit approfondito del livello di sicurezza dei componenti di base della infrastruttura IT (server, dispositivi di rete e di sicurezza) alla ricerca di possibili vulnerabilità. E' possibile approfondire l'analisi erogando servizi di penetration testing, attività che si pone l'obiettivo di prendere il controllo dell'apparecchiatura sotto esame in modo da accedere ai dati sensibili.
È reso disponibile un servizio di supporto sulle modalità di eliminazione delle vulnerabilità, oltre alle possibilità di erogare dei corsi di formazione rivolti al personale tecnico.
E' altresì possibile realizzare un audit delle politiche delle apparecchiature firewall/IDS onde verificare la coerenza tra le politiche di indirizzo progettate e le regole di filtraggio effettivamente applicate.

Valutazione livello di sicurezza delle applicazioni software

Le vulnerabilità da ricondurre ad uno sviluppo del software carente rispetto ai principi della sicurezza informatica sono stabilmente al di sopra del 50% del totale: termini noti agli specialisti dell'hacking quali Cross Site Scripting, SQL Injection,Cross Site Request Forgery e Man in The Browser, sono spesso citati dai media generalisti che riportano le notizie dei cosiddetti "data breach".
L''introduzione dei criteri di sicurezza durante le prime fasi del processo SDLC, principio noto come "Security by Design", uno dei punti chiave del nuovo GDPR, comporta al produttore software il risparmio di una notevole quantità di denaro.

Le best practices di settore suggeriscono ai clienti di verificare sempre la sicurezza dell'applicazione prima di esporla in ambiente di produzione. L'attività di verifica della sicurezza applicativa è molto più dettagliata rispetto alle verifiche di tipo infrastrutturale in quanto è necessaria un'interazione diretta con tutti gli aspetti dell'applicazione.

Incident Handling & Digital Forensics

A fronte della compromissione di un sito web, della sottrazione di informazioni dai sistemi informativi aziendali oppure un utilizzo doloso di un dispositivo PC client aziendale viene offerto un completo supporto nella creazione o revisione del processo di gestione degli incidenti informatici alla luce degli standard internazionali di settore (NIST, SANS, ISO ecc).
A fronte di un «incidente di sicurezza» si attiva il processo di indagine attraverso la verifica della reale portata del problema e la ricostruzione della dinamica dell'incidente basandosi su opportune tecniche investigative. L'intervento prevede l'esecuzione di una copia, senza modificare gli originali, di tutti i dati (disco, memoria, processi ecc.) presenti sui dispositivi di memorizzazione del sistema oggetto dell'incidente e la successiva analisi delle evidenze in laboratorio; in seguito si correlano i risultati e si produce un report dell'incidente basato su dati oggettivi ed incontrovertibili.

IT Security Design & Deploy

Questa sezione dell'offerta si propone di caratterizzare le architetture di rete Intranet (i sistemi interni che erogano servizi nei confronti degli utenti aziendali) ed i servizi esposti su Internet (siti web, ecommerce, posta elettronica, DNS) secondo il principio della «Defense in Depth», rendendo quindi più difficili le potenziali attività ostili da parte di un attaccante. Attraverso partnership commerciali o tramite l'utilizzo di soluzioni Open Source possono essere integrati nell'infrastruttura dei sistemi informativi prodotti specializzati nel contrasto alla diffusione del malware oppure di protezione nei confronti dei dati memorizzati e delle comunicazioni.

Prodotti di protezione perimetrale e servizi di sicurezza

I sistemi di protezione perimetrale (firewall, servizi UTM associati quali IDS/IPS, sistemi antivirus ed endpoint protection) possono spaziare su diverse soluzioni in funzione delle dimensioni e della topologia dell'architettura di riferimento; questi sistemi possono essere forniti sotto forma di appliance oppure quali applicazioni dedicate da utilizzare in una piattaforma virtualizzata e possono essere integrate all'interno di realtà di qualunque dimensione ed esigenze di performance.
Secondo il paradigma Cloud Computing tali sistemi possono essere resi disponibili in modalità servizio nella forma SecAAS (Security As A Service), liberando quindi l'utente finale dagli oneri di acquisto, manutenzione e gestione degli asset.

Sistemi di log management e security event correlation (SIEM)

I sistemi di log management e di correlazione degli eventi di sicurezza tenderanno sempre più a rappresentare il «cruscotto» della sicurezza aziendale. Le motivazioni che possono spingere all'investimento su tali soluzioni sono diverse:

> Compliance normativa, in Italia il decreto del Garante relativo al monitoraggio delle attività degli Amministratori di Sistema, negli USA le disposizioni HIPAA (trattamento dati sensibili sanitari ed assicurativi), oltre alle normative specifiche di settore quali PCI-DSS, disposizioni UE in materia bancaria, SOX oltre e standard ISO 27001;

> Necessità di concentrare in un unico punto tutti gli eventi di sicurezza inviati da tutti i componenti dell'architettura elaborativa al fine di monitorare in tempo reale il livello di rischio e rispondere in modo organizzato e tempestivo ad un eventuale attacco informatico;

> Utilizzando la stessa infrastruttura di controllo ed archiviazione centralizzata dei file di log è possibile avere un repository su cui effettuare delle analisi basate su tecniche di Business Analytics pertinenti aspetti diversi dalla sicurezza, ma rese possibili attraverso le informazioni contenute nei file di log, quali il processo di sviluppo del software oppure quello di gestione dei sistemi informativi.

> Le soluzioni proposte possono scalare in funzione delle dimensioni e della topologia dell'architettura informatica oppure dalle esigenze di conformità; anche questi sistemi possono essere fisici o virtualizzati e possono svolgere la loro funzione all'interno di realtà di qualunque dimensione ed esigenze di performance.

IT Infrastructures
Design & Deploy

Systems & Infrastructure Management

La complessità degli attuali sistemi informativi rende particolarmente difficoltose le attività di verifica delle funzionalità e della qualità dei servizi erogati. L'adozione di soluzioni di system management - application monitoring consente un approccio proattivo nella gestione di un intero sistema, monitorando i parametri vitali dell'intera infrastruttura ICT, prevenendo i disservizi e consentendo una organica politica di evoluzione dell'architettura hardware e software. Il costante controllo degli indicatori classici quali utilizzo CPU, occupazione risorse di memorizzazione, quantità dati trasferiti, numero sessioni, ecc., può essere abbinato al controllo di parametri ambientali (temperatura, umidità, fumo, rilevamento allagamenti ed apertura accessi) consentendo, tramite un immediato allertamento del personale, la prevenzione di disastri nell'ambito di tutta l'infrastruttura IT.
Allo stesso modo, il controllo dei tempi di risposta delle applicazioni critiche, permette una verifica costante della qualità di servizio erogato ai propri utenti, consentendo in caso di calo di performance, la possibilità di "incrociare" questi dati con quelli relativi all'utilizzo dell'infrastruttura riducendo sensibilmente le attività di analisi della problematica in essere.
La soluzione di monitoring basata sul prodotto Zabbix (totalmente open source per qualunque realtà dimensionale) consente di mantenere sotto controllo l'integrità e le prestazioni dei sistemi informativi e può essere applicata a qualunque realtà tecnologica che faccia uso della tecnologia IP.
La versatilità del prodotto, la vasta esperienza progettuale e la condizione di unico "Certified Partner" sul territorio italiano ci pongono in una posizione di riferimento per il mercato italiano negli ambiti della progettazione, realizzazione, supporto tecnico ed erogazione formazione.

Perchè scegliere Zabbix

La soluzione consente di superare alcune limitazioni presenti in altre alternative Open Source come ad esempio il considerevole numero di plugin, aggiornamenti più complessi ed onerosi, le funzionalità di autodiscovery dei sistemi da controllare non presenti in modo nativo oppure gli elevati costi di licensing e manutenzione. Zabbix non ha costi di licenza aggiuntivi anche se utilizzato a livello enterprise.

Caratteristiche tecniche:
> Sistema di monitoring Open Source;
> Architettura centralizzata o distribuita;
> Sistema scalabile sino ad oltre 100.000 dispositivi controllati;
> Monitoring in tempo reale della disponibilità e delle performance;
> Controllo dell'intera infrastruttura ICT con un solo strumento;
> Creazione di servizi IT gerarchici;
> Flessibilità d'uso: interazione tramite agent o protocollo SNMP;
> Controllo di sistemi operativi, applicazioni, apparati di rete;
> Interfaccia web, creazione di viste personalizzate;
> Servizio di alerting personalizzabile.

Virtualizzazione e Servizi Cloud

La virtualizzazione consente una flessibilità senza precedenti, oltre ad un intrinseco aumento dell'affidabilità. Tramite l'implementazione di sistemi virtuali è possibile effettuare il dispiegamento di nuove configurazioni server e recuperare, a seguito di guasti hardware, funzionalità in pochi minuti. Questa tecnologia consente, inoltre, l'ottimizzazione degli investimenti hardware, consentendo una gestione più efficiente del data center ed il contenimento dei costi relativi alle soluzioni di Continuità Operativa e Disaster Recovery. Nell'offerta è reso disponibile il supporto indipendente nella valutazione tecnica, normativa ed economica per la migrazione dei sistemi su piattaforme basate su paradigma Cloud Computing.

Backup e Disaster Recovery

Per garantire il ritorno alla normale operatività occorre implementare e gestire sia un processo di backup locale, in modo da espletare le ordinarie funzioni di recupero dati erroneamente cancellati o modificati, sia un processo di disaster recovery che permetta la disponibilità e fruibilità dei dati anche in situazioni di malfunzionamento delle risorse IT. Le realizzazioni di sistemi di backup "disk-to-disk" permettono di raggiungere gli obiettivi preposti di primo livello mantenendo costi contenuti e prestazioni elevate. L'offerta consiste nella messa a disposizione di risorse elaborative presso il nostro Data Center attraverso i servizi Fast DB Recovery Oracle, basato sul trasferimento incrementale degli archive log e Fast VM Recovery, basato sul trasferimento delle snapshots VMware

Progetti significativi

Regione Emilia-Romagna

Servizio Sistema Informativo Informatico Regionale

Affidamento pluriennale del servizio di supporto alla sicurezza informatica

Sistema informativo complesso in ambiente eterogeneo composto da circa 600 server, 700 apparati di rete, centinaia di applicazioni, 5000 utenti interni con distribuzione dei servizi sull'intero territorio regionale. L'approccio è consistito nell'esecuzione di un primo assessment di carattere generale, nella definizione di una Security Policy, dei disciplinari in materia di Privacy, di sviluppo sicuro e test applicativo e di gestione degli incidenti.
In seguito si è provveduto all'esecuzione periodica di test di sicurezza ed all'integrazione di nuovi componenti nell'architettura di sicurezza ed alle verifiche a campione sugli utenti in merito alla consapevolezza delle procedure di sicurezza ed alla configurazioni dei loro strumenti di lavoro informatici.
E' stata introdotta nel processo Quality Assurance delle applicazioni software la verifica sistematica della sicurezza prima del loro rilascio in produzione ed è stata avviata un'attività volta alla razionalizzazione nella gestione delle informazioni di sicurezza sul sistema SIEM adottato dal Cliente con l'obiettivo di automatizzare il processo di Incident handling ed è stato proposto uno studio con valutazione tecnico economico sulle soluzioni anti APT.
Il progetto ha conseguito i seguenti benefici: un miglioramento generale del livello di sicurezza, la consapevolezza dei rischi, la formalizzazione di checklist per l'installazione di server ed apparati di rete, la riduzione dei costi del patching applicativo, la diffusione della cultura di sicurezza presso gli utenti finali, l'estensione delle politiche di sicurezza a fornitori e partner, oltr all'avvio del processo di monitoraggio continuo delle possibili minacce alla sicurezza.

Aggiornamento documento DPS ed analisi dei rischi - Conformità a Codice sulla protezione dei dati personali (D.Lgs.196/03)

Valutazione della criticità delle informazioni al fine di ottenere una loro classificazione con riferimento alle grandezze fondamentali delle sicurezza, identificazione dei dati da proteggere e loro classificazione in base alla loro criticità e tipologia. Individuazione dei potenziali incidenti, mediante analisi dei possibili agenti di minaccia che potrebbero insistere sui dati. Valutazione del livello di esposizione al rischio ed indicazione delle possibili contromisure, misurazione del rischio residuo e stesura del piano di mitigazione.

Redazione Studio di Fattibilità Tecnica – Conformità ad art. 50 del Codice di Amministrazione Digitale

Attività di consulenza (Business Impact Analysis ed analisi costi-benefici) su organizzazione, servizi informatici interni ed esterni, soluzioni tecnologiche, condivisione esigenze di continuità operativa.
Riferimento metodologico: "Linee guida per il DR delle Pubbliche Amministrazioni"– DigitPA. Redazione dello Studio di Fattibilità Tecnica da sottoporre da parte dell'Amministrazione al parere di AGID (ex DigitPA).

Regione Calabria

Nuovo Sistema Informativo Amministrativo Regionale

Fornitura soluzione di log management

Architettura elaborativa centralizzata nel CED regionale di Catanzaro, composta da circa 100 log sources comprendenti 50 server per la maggior parte virtualizzati oltre ad un corrispondente numero di applicazioni di tipo eterogeneo (MS Windows, Linux, Database Oracle, Application Server Tomcat ecc.)
Appliance LogLogic MX3020 con architettura completamente

ridondata, reporting mensile sugli accessi degli AdS (conformità al relativo provvedimento del Garante Privacy), memorizzazione locale file di log per un anno, supporto per attività di computer forensics; soluzione scalabile in vista di possibile espansione sistemi informativi.

Aggiornamento documento DPS ed analisi dei rischi - Conformità a Codice sulla protezione dei dati personali (D.Lgs.196/03)
Valutazione della criticità delle informazioni al fine di ottenere una loro classificazione con riferimento alle grandezze fondamentali delle sicurezza, identificazione dei dati da proteggere e loro classificazione in base alla loro criticità e tipologia. Individuazione dei potenziali incidenti, mediante analisi dei possibili agenti di minaccia che potrebbero insistere sui dati. Valutazione del livello di esposizione al rischio ed indicazione delle possibili contromisure, misurazione del rischio residuo e stesura del piano di mitigazione.

Redazione Studio di Fattibilità Tecnica – Conformità ad art. 50 del Codice di Amministrazione Digitale
Attività di consulenza (Business Impact Analysis ed analisi costi-benefici) su organizzazione, servizi informatici interni ed esterni, soluzioni tecnologiche, condivisione esigenze di continuità operativa. Riferimento metodologico: "Linee guida per il DR delle Pubbliche Amministrazioni"– DigitPA. Redazione dello Studio di Fattibilità Tecnica da sottoporre da parte dell'Amministrazione al parere di AID (ex DigitPA). Successiva redazione del Piano di Continuità operativa da integrare con il Piano di Disaster Recovery.

AO Carlo Poma di Mantova

Revisione completa dell'infrastruttura di backup dell'Ente per quanto riguarda tutti i 10 database Oracle presenti, con l'implementazione di un sistema centralizzato RMAN integrato con il software di backup dell'Ente Symantec NetBackup, sul quale sono configurate le policy per la duplica a caldo dei database primari su un sito remoto.

Azienda Ospedaliera di Reggio Emilia

Redazione Studio di Fattibilità Tecnica - Conformità ad art. 50 del Codice di Amministrazione Digitale
Progetto di consulenza della durata di due mesi in materia di consulenza su sicurezza (parametro disponibilità delle applicazioni) e continuità operativa. L'ambito di applicazione ha coinvolto l'organizzazione, i processi e le tecnologie; l'analisi è stata condotta su 45 servizi informatici sanitari, amministrativi e di infrastruttura ed è stato fornito il supporto per presentazione finale dei risultati al Direttore Sanitario e l'invio della documentazione ad Agenzia per l'Italia Digitale.

Sistema di monitoraggio integrato
È stato implementato un sistema di monitoraggio esteso, in grado di analizzare sia lo stato che le performance dei server ma soprattutto lo stato e le performance degli applicativi sanitari critici. Tramite l'implementazione di svariati controlli e plugin proprietari si registrano i tempi di risposta applicativi, sia relativi a singole fasi specifiche che a simulazioni di interi "percorsi" – login, ricerca, somministrazione, logout, storicizzandoli su database e permettendone una rappresentazione grafica.
Alo stesso tempo, vengono impostate soglie di allarme in gradi di avvisare gli operatori CED in caso di rallentamenti e relativi disservizi.

San Donato Milanese

Rivisitazione dell'intero CED in ottica di Continuità di Servizio, implementazione di Oracle in configurazione RAC, backup fisici tramite utility RMAN integrata nel sistema di backup Time Navigator ed implementazione di un infrastruttura di virtualizzazione. Tutto il CED viene monitorato tramite un sistema NMS che controlla l'hardware ed il middleware presente (Oracle, Domino, Application Server).

Regione Marche

Implementazione di un infrastruttura Oracle RAC, della relativa configurazione dei backup fisici tramite RMAN integrati con IBM Tivoli, di un infrastruttura di application server (Apache httpd – Apache Tomcat) ridondati in bilanciamento di carico con apparati hardware F5.

Comune di Cagliari

Fornitura di un sistema di Log Management per la storicizzazione e consultazione dei log di accesso degli amministratori di sistema. Applicazione interamente sviluppata dal Gruppo Finmatica in grado di storicizzare tutti i log di accesso provenienti da tutti i sistemi operativi e database, permettendo funzionalità di consultazione (tramite browser web) ed archiviazione.

IT Security
Offerta e Certificazioni

GRUPPO FINMATICA

via della Liberazione 15 40128 Bologna
Tel 0516307411 Fax 0516307498
e-mail entilocali@ads.it www.ads.it