



Disaster Recovery

ORACLE

Partner

“ LE REGOLE DEL DISASTER RECOVERY.

Quanto costa un blocco
e come ripartire in tempo
zero dopo un incidente ”

ORACLE

Partner

Nell'era della trasformazione digitale, le minacce alla sicurezza e all'integrità dei dati costituiscono una costante spada di Damocle per le aziende, chiamate a tutelare con ogni mezzo possibile la loro principale risorsa informativa. Per prevenire gli effetti nefasti degli incidenti è necessario implementare un'adeguata strategia di disaster recovery. Ciò assume una particolare rilevanza nel caso dei servizi fondamentali e delle infrastrutture critiche, ma occorre prendere coscienza del fatto che nessuna azienda può

dirsi del tutto al sicuro da un grave attacco informatico o da una calamità naturale in grado di dare luogo ad una serie di downtime estremamente penalizzanti per la continuità del business.

Vediamo pertanto cosa si intende per disaster recovery e cosa occorre fare per implementare azioni e procedure finalizzate a garantire la cosiddetta high availability, una disponibilità elevata dei sistemi informativi fondamentali per l'erogazione dei servizi informatici.

UNA DEFINIZIONE DI DISASTER RECOVERY

Il disaster recovery (DR) è un approccio che consente di ripristinare la disponibilità dell'infrastruttura IT dopo un evento negativo, come una calamità naturale, un incendio, un grave attacco informatico o un guasto accidentale ai componenti critici dell'infrastruttura stessa. Per tali ragioni, il DR costituisce uno degli argomenti chiave della continuità di business aziendale.

Il disaster recovery comprende una grande varietà di metodi e soluzioni, accomunate da un unico obiettivo, che possono essere utilizzate anche combinandone gli effetti. Tra le implementazioni più recenti figura il Disaster Recovery as a Service (DRaaS), un modello a servizi che prevede di rendere disponibile in cloud l'infrastruttura IT, in modo da poterla utilizzare nel caso in cui i server on-premise dovessero subire importanti downtime.

Tra i principali vantaggi del disaster recovery vi sono aspetti organizzativi, che risiedono nella capacità di predisporre un piano di DR per far fronte alle criticità più gravi a cui un'azienda può andare incontro dal punto di vista operativo. Mitigare in maniera efficiente gli effetti di

un downtime può evitare un grave danno economico, oltre a consentire una rapida e regolare ripresa delle attività, o addirittura nemmeno accorgersi del disservizio subito. L'assenza di un valido piano di disaster recovery equivale a viaggiare in totale balia degli effetti, con il rischio più che mai concreto di vedere il proprio business naufragare sotto i colpi degli eventi malevoli.



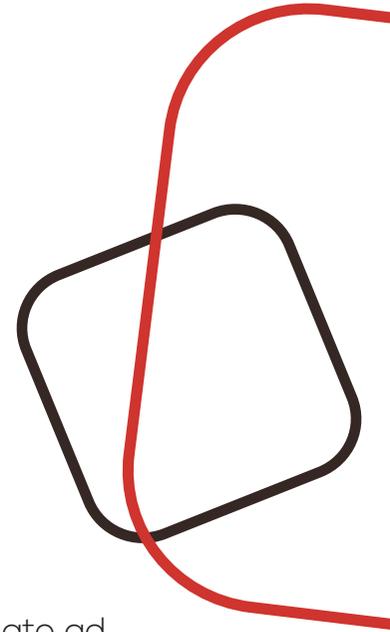
The Oracle logo is displayed in a bold, red, sans-serif font.The word "Partner" is written in a black, sans-serif font, positioned to the right of the Oracle logo and separated by a vertical line.

LE DIFFERENZE CON IL BACKUP E PERCHÉ È IMPORTANTE CONOSCERLE

Backup e disaster recovery costituiscono due aspetti complementari nella data strategy aziendale, ma differiscono in maniera sostanziale sia nei metodi che nelle tecnologie impiegate, oltre che negli obiettivi funzionali. Costituiscono due contenuti fondamentali nel piano di continuità aziendale (Business Continuity Plan).

Il backup opera in maniera granulare, sui singoli file, di cui effettua copie con logica point-in-time (PIT) per fare una fotografia (snapshot) del sistema in un determinato momento. Tale immagine consente in qualsiasi momento di procedere con un ripristino totale o parziale. Per tali

ragioni un sistema di backup è spesso associato ad un sistema di recupero dei dati, che ha la funzione di ripristinare file e cartelle nel point-of-time desiderato. Il disaster recovery agisce in maniera decisamente più trasversale, con l'obiettivo di ripristinare l'intero sistema IT in caso di downtime, incidenti o altre minacce alle sorti della continuità di business aziendale. Per tale motivo i sistemi di DR tendono a replicare l'intera infrastruttura IT dell'azienda, in modo da consentire di recuperare anche da fenomeni fisici, come potrebbe avvenire nel caso di un incendio presso un data center.



LE CAUSE DI UN DOWNTIME

Prima di entrare nel merito dei fattori scatenanti alla base di una possibile interruzione di servizio, è opportuno notare come sia utile distinguere tra un downtime pianificato, come la manutenzione di un server o l'aggiornamento di

un software di sistema, e un downtime non pianificato, come quello che può generarsi a causa di un incidente o di una calamità imprevista.

Tra i principali fattori che possono dare luogo a un downtime più o meno prolungato ritroviamo i danni dovuti ai disastri naturali (terremoti, allagamenti, tempeste, ecc.), incendi, furti, vandalismi ed altre azioni in grado di provocare danni fisici all'infrastruttura IT. In altri casi, la causa del downtime può essere riconducibile a guasti e malfunzionamenti dei sistemi informatici, in particolare quelli che regolano il funzionamento dei data center, come le interfacce di rete, i sistemi di refrigerazione, ecc. Una ulteriore causa è dovuta ad esempio ai temibili attacchi ransomware, in grado di paralizzare l'intera infrastruttura IT. A prescindere dalle cause del downtime, il piano di disaster recovery prevede vari livelli di resilienza, in funzione della tipologia di business e del budget a disposizione per implementare un'architettura adeguata a garantire la continuità di business richiesta dagli obiettivi aziendali.



QUANTO PUÒ COSTARE UN DOWNTIME?

In estrema sintesi, un downtime rende inaccessibili i dati necessari per il funzionamento di varie applicazioni, compromettendo in maniera più o meno evidente la continuità di business. Per tali ragioni, gli effetti di un downtime vanno ben oltre il danno economico diretto ed indiretto relativo all'interruzione di servizio.

Oltre al calo di produttività e alla riduzione degli introiti ad essa collegati, l'azienda che rimane vittima di un downtime deve spesso fronteggiare l'insoddisfazione dei propri clienti, che potrebbero lamentarsi pubblicamente, far valere le proprie ragioni nel caso di inadempienze contrattuali, oltre a prendere in considerazione le soluzioni offerte da un concorrente.

Nei casi più gravi, è possibile andare incontro a gravi danni di natura reputazionale, che potrebbero condizionare in maniera non rimediabile la credibilità di un brand e la sua competitività sul mercato. Recuperare un crollo reputazionale è quasi sempre un'impresa ben più ardua rispetto al recupero di un danno economico derivante da un mancato introito a livello produttivo.

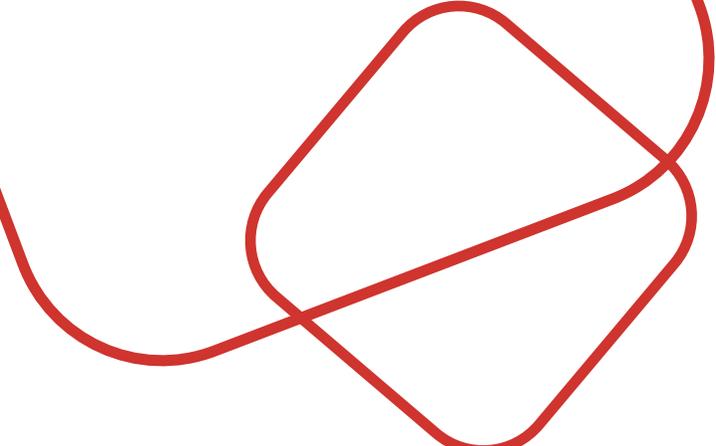
REGOLE E PASSI CHIAVE PER UNA CORRETTA STRATEGIA DI DISASTER RECOVERY

Le procedure fondamentali nell'ambito del disaster recovery comportano il design e l'implementazione di sistemi IT capaci di sopravvivere, in tutti i sensi, a un disastro in modo da riprendere in maniera regolare le operazioni con il minimo livello di intervento e la minor perdita di dati possibile.

I due parametri fondamentali per una corretta strategia di disaster recovery sono il Recovery Time Objective (RTO) e il Recovery Point Objective (RPO).

Nel caso del RTO è necessario identificare il tempo necessario per ottenere una determinata capacità operativa dopo il disastro. È ad esempio possibile determinare un obiettivo misurabile, come la disponibilità del 90% delle risorse IT entro i 20 minuti successivi all'incidente, così come qualsiasi altro livello di efficienza in funzione di un intervallo di tempo utile. La definizione di





tali parametri dipende soprattutto dai requisiti necessari per soddisfare i contenuti del business continuity plan aziendale. In altri termini, ogni azienda ha il proprio RTO efficace. I piani di disaster recovery che prevedono più fasi attuative possono avere un RTO specifico per ognuna di esse. Maggiore è la disponibilità (availability) del dato, tanto più semplice risulta ottenere un RTO più favorevole. Nel caso del RPO, come il termine stesso suggerisce, si considera un rollback, ossia il tempo necessario per ripristinare la piena funzionalità del sistema alla situazione precedente il disastro. Questo comporta che tutte le transazioni effettuate tra l'RPO e il disastro siano considerate come non recuperabili. Ad RPO inferiori corrisponde una resilienza più elevata.

Come nel caso del RTO, anche l'RPO viene determinato in funzione degli obiettivi del business continuity plan. Alcune aziende necessitano di una resilienza totale, che risulta senza dubbio molto più onerosa rispetto a chi può permettersi anche un recovery point objective di giorni, o addirittura di settimane. Anche in questo caso, non esiste

dunque una regola assoluta. I parametri vanno definiti caso per caso sulla base di ogni situazione aziendale. Nel presentare RTO e RPO abbiamo fatto riferimento ad una situazione estrema, di downtime totale. In realtà, ciò accade soltanto in alcune circostanze, molto drammatiche, in cui il disastro può bloccare totalmente l'intera produzione o l'erogazione dei servizi per lunghi periodi, creando disagi anche enormi, dalle conseguenze molto pesanti in termini economici.

Tuttavia, se i sistemi sono progettati per garantire un'adeguata disponibilità di risorse, si assiste a molti brevi downtime, riconducibili nell'ordine dei minuti o di poche ore. In questo caso, è possibile realizzare sistemi e procedure in grado di continuare la produzione senza eccessive penalizzazioni, fino a quando le funzionalità non vengono totalmente ripristinate.



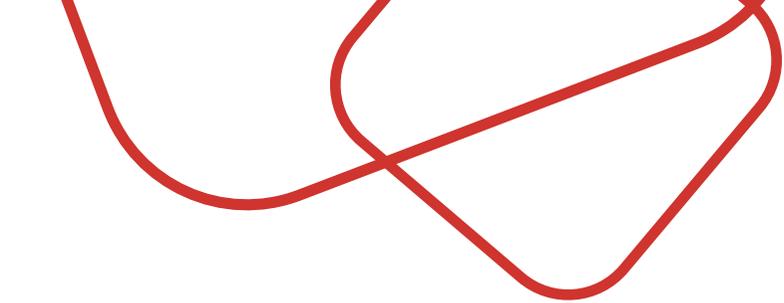
ORACLE

Partner

COS'È L'HIGH AVAILABILITY E PERCHÉ È LA CHIAVE DI VOLTA

In informatica, per availability si intende il livello con cui un'applicazione o un database viene reso disponibile, tant'è che questo livello si misura proprio sulla base della percezione degli utenti, che possono lamentare una difficoltà di accesso ai dati o un rallentamento delle prestazioni dei server e degli endpoint da essi utilizzati. Le ragioni per cui ciò accade le abbiamo in buona parte esaminate in precedenza, ma anche senza il verificarsi del famigerato disastro, potremmo semplicemente trovarci di fronte ad un'infrastruttura IT dimensionata in maniera insufficiente per reggere i carichi di lavoro previsti o

insufficiente a supportare i picchi di attività. In questo contesto, prende forma l'high availability (HA), per contrassegnare un'infrastruttura informatica capace di garantire un'elevata disponibilità delle risorse IT con livelli di performance adeguati a rispondere alle aspettative degli utenti. I sistemi HA sono quindi progettati per garantire servizi senza interruzioni, con uno standard 24/7, dotati una ridondanza capace di ovviare ai downtime accidentali e a quelli pianificati, come nel caso degli aggiornamenti ai componenti hardware e software che compongono l'infrastruttura IT.



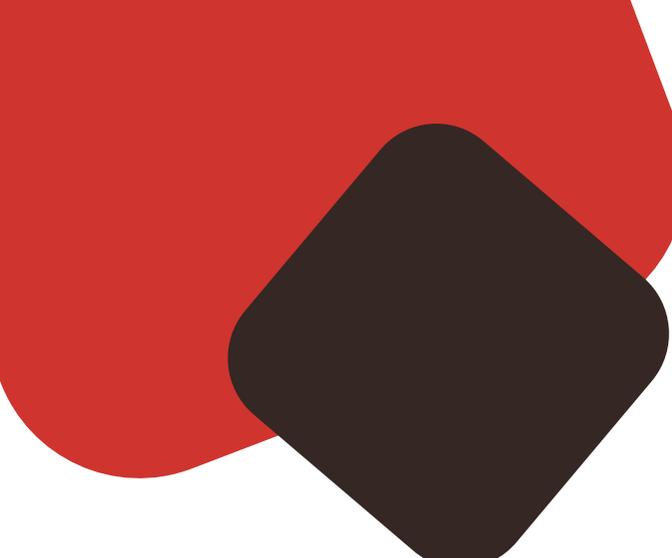
Un sistema ad elevata disponibilità è contraddistinto almeno da quattro caratteristiche fondamentali:

Affidabilità: con particolare riferimento ai sistemi hardware e software di una soluzione high availability. La componente software riguarda i database, i web server e le applicazioni eseguite su una determinata infrastruttura IT. Tali sistemi sono configurati in modo da ottenere una ridondanza di risorse, utile a fronteggiare un malfunzionamento localizzato senza condizionare il funzionamento a livello generale. Un esempio di sistema HA è ad esempio costituito da Oracle Real Application Cluster (Oracle RAC), specifico per garantire un database resiliente, capace di garantire la corretta operatività anche qualora uno dei server dovesse subire un inaspettato downtime.

Recuperabilità: un corretto approccio nei confronti della disponibilità delle risorse IT si interroga innanzitutto sulle possibili cause che possono determinare un downtime, in modo da pianificare tutte le contromisure necessarie nel contesto del piano di disaster recovery. Tale condizione consente di recuperare nel modo più rapido ed indolore possibile dai malfunzionamenti che possono condizionare la disponibilità delle applicazioni e dei database.

Rilevamento tempestivo degli errori: oltre al ripristino delle attività, il rilevamento tempestivo degli errori risulta fondamentale per rispettare le SLA (Service Level Agreement) che prevedono dei tier molto precisi in merito al livello di affidabilità di un servizio. Oltre alle pesanti ricadute a livello reputazionale, qualora non riuscissimo a ripristinare la corretta accessibilità dei dati entro il termine previsto, rischieremmo di incorrere in azioni legali da parte del cliente, la cui richiesta di danni potrebbe rivelarsi particolarmente significativa.

Continuità operativa: un'architettura HA deve necessariamente rendere il più trasparente possibile le operazioni per l'utente finale, che si tratti di compensare dei brevi periodi di downtime accidentali, così come effettuare gli aggiornamenti hardware e software necessari per garantire un adeguato livello di performance del sistema. Un'architettura ridondante può compensare facilmente a queste eventualità, in modo che gli utenti non se ne accorgano nemmeno.



ORACLE

Partner

L'high availability costituisce dunque il pilastro fondamentale per garantire un'adeguata disponibilità delle risorse IT e le sue logiche risultano perfettamente coerenti con le attività e i piani di disaster recovery. In particolare, un approccio HA risulta determinante nel contesto del data management e di tutti i sistemi che hanno l'obiettivo di garantire un'elevata disponibilità dei dati. Quando si scelgono dei servizi di database, oltre ai parametri relativi alla performance, è ad esempio indispensabile valutare con attenzione le SLA, in modo da scegliere i tier più funzionali alle proprie esigenze, anche in funzione dei costi che una disponibilità elevata spesso comporta.



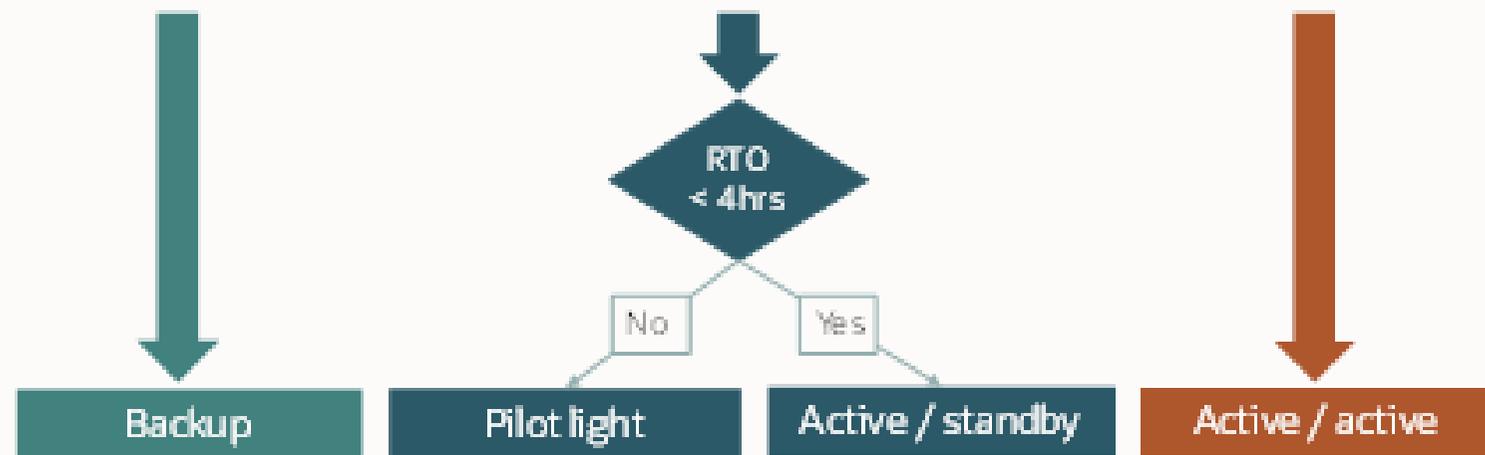
**DISASTER
RECOVERY**

IL CASO ORACLE: SOLUZIONI E STRATEGIE

Soprattutto quando si parla di affidabilità dei sistemi di dati, Oracle si conferma un punto di riferimento su ampia scala, e lo conferma il suo approccio HA nei confronti dei database, in quella che viene definita una Maximum Availability Architecture (MAA). Al di là dell'affidabilità intrinseca dei sistemi hardware / software, una MAA si distingue per una serie di best practice utili a minimizzare, e possibilmente ad annullare, i disservizi e i costi derivanti dai possibili downtime.

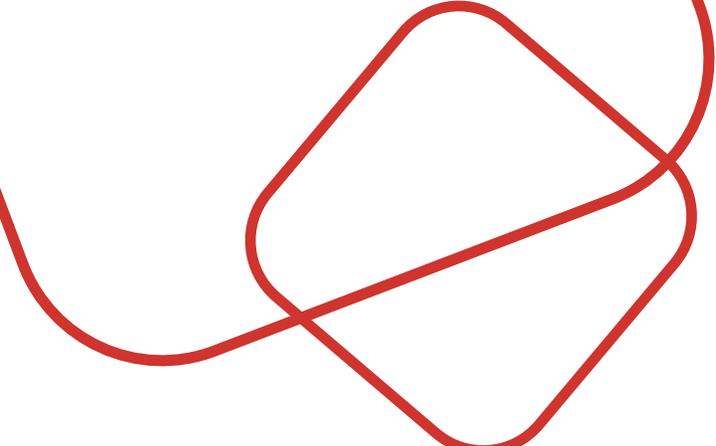
Una MAA prevede l'impiego, a seconda della situazione specifica, di soluzioni complementari in grado di assicurare il più elevato livello di disponibilità dei dati in funzione dei costi e del livello di performance richiesto.

A disaster recovery solution for every application



RPO (data loss)	24 hours +	Seconds	Seconds	Zero
RTO (down time)	Hours - Days	Hours	Minutes	Zero
OpEx	Very low	Low	Medium	Higher
Complexity	Very Low	Medium	Low	Medium





ORACLE

Partner

Grazie alla varietà di soluzioni hardware e software presenti nella propria offerta, Oracle è in grado di garantire una soluzione su misura per qualsiasi contesto di affidabilità richiesto, in funzione della criticità da affrontare.

Il grafico illustrato in precedenza dimostra come sia possibile avvalersi di soluzioni di backup evoluto, capaci di superare senza affanni qualsiasi situazione non critica nell'arco di un RPO nell'ordine delle 24 ore. Procedendo verso destra si va nella direzione di un crescente livello di criticità, dove l'indice rilevante diventa il RTO, che tende a zero nel caso delle applicazioni che non possono permettersi alcuna soluzione di discontinuità, come nel caso delle infrastrutture critiche, dei servizi finanziari e delle applicazioni e-commerce, dove ogni secondo perso equivale ad un danno decisamente ingente.

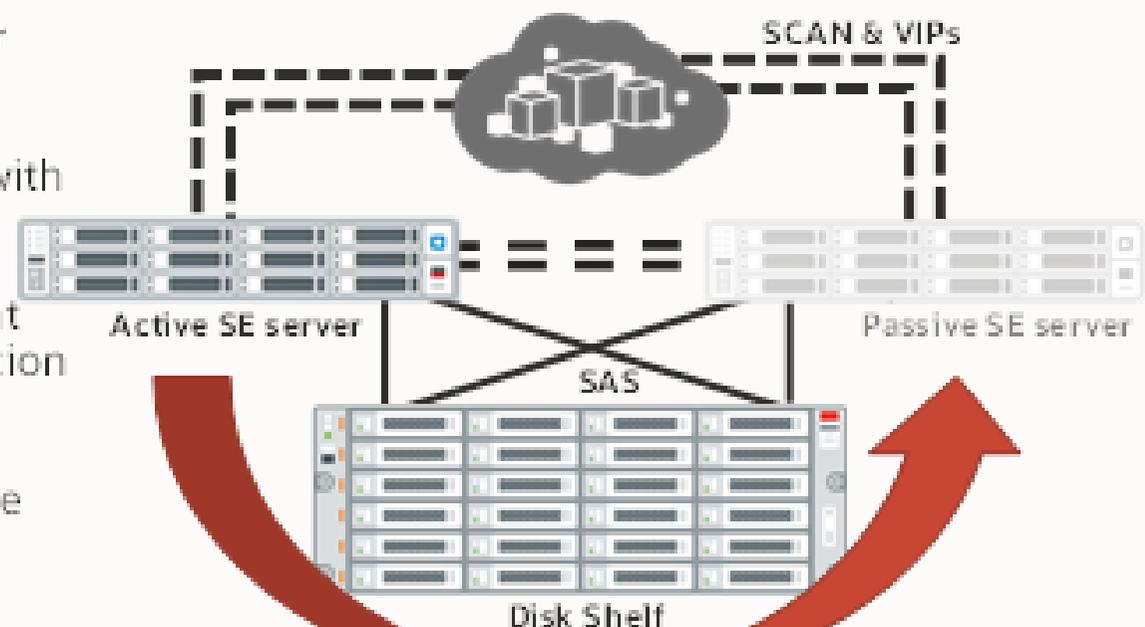
Standard Edition High-Availability(SEHA)

Every SE database is **automatically configured** for cold failover

Support for both planned and unplanned failover with **Near-Zero** downtime

Uses **SCAN and VIPs** to ensure unique access point for the database in case of failover without application or mid-tier reconfiguration

ODA automatically maintains **consistency** of Oracle Homes across nodes



ORACLE

Partner

LE RISPOSTE DI ORACLE E ICOS

Cosa si intende per disaster recovery? Cosa occorre fare per implementare azioni e procedure finalizzate a garantire la cosiddetta high availability, una disponibilità elevata dei sistemi informativi fondamentali per l'erogazione dei servizi informatici? In questa piccola guida abbiamo provato ma riassumere risposte, idee, proposte di piattaforme, per tutti gli approfondimenti potete contattare un partner Oracle di riferimenti come ICOS, www.icos.it