Intesys

Sviluppo di Software Sicuro e GDPR Compliant

Le nostre procedure e le nostre metodologie

Versione 1.6 - Ottobre 2022

Intesys

Sommario

Introduzione

Il presente documento definisce i requisiti, le misure e i controlli di sicurezza che Intesys srl considera e applica nei processi sviluppo e manutenzione delle applicazioni software. La metodologia e le procedure seguite applicano le regole di sviluppo sicuro riportate nel Capitolo 14.2.1 dello standard ISO 27001 e fanno riferimento al regolamento 2016/679 del Parlamento europeo (GDPR, considerando n.78) in cui si dichiara esplicitamente che "... i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati ..."

Al fine di garantire che la sicurezza delle informazioni e la protezione dei dati personali siano parte integrante di tutte le fasi del ciclo di sviluppo del software, Intesys ha adottato una metodologia che identifica i requisiti di sicurezza prima dello sviluppo e manutenzione di ogni sistema applicativo.

Strettamente correlato con il presente documento è l'"Assessment per lo Sviluppo di Software Sicuro e GDPR Compliant" (nel seguito ASSS) che, sulla base della metodologia nel seguito descritta, descrive le misure di sicurezza che saranno implementate per proteggere dati e programmi per il singolo progetto di sviluppo software o major release concordato e contrattualizzato con il cliente.

Intesys ritiene che lo sviluppo di software sicuro debba essere considerato con la massima priorità fino dalle prime fasi dello sviluppo e questo comporta l'impiego di personale preparato e formato, oltre all'adozione di strumenti in grado d'individuare possibili falle durante i rilasci intermedi.

Il presente documento prende in considerazione come riferimenti:

- Requisiti del Regolamento n° 679/2016 in materia di protezione dei dati personali (nel seguito GDPR)
- Requisiti della norma ISO 27001 in materia di sicurezza delle informazioni;
- Requisiti dello standard OWASP (Open Web Application Security Project);

- Indicazioni contenute nel documento dell'Agenzia per l'Italia digitale LINEE GUIDA PER LA MODELLAZIONE DELLE MINACCE ED INDIVIDUAZIONE DELLE AZIONI DI MITIGAZIONE CONFORMI AI PRINCIPI DEL SECURE/PRIVACY BY DESIGN".

Il GDPR non formalizza precise specifiche per lo sviluppo di software compliant al regolamento. In generale però riteniamo che le applicazioni software che trattano dati personali debbano essere progettate sulla base di principi e indicazioni che lo sviluppatore si autoimpone, ispirandosi alle pubblicazioni in materia di Privacy. Il presente documento quindi definisce ulteriori requisiti, misure e controlli di sicurezza che Intesys srl considera e applica nei processi sviluppo e manutenzione delle applicazioni software che trattano dati personali.

Security by design – Privacy by design

Durante le fasi di analisi della sicurezza applicativa di una architettura di sistema (da definire o in fase di rivisitazione) è necessaria l'attuazione di pratiche di progettazione sicura attraverso l'individuazione di requisiti di sicurezza e contromisure, attraverso un approccio di Defense in Depth dell'applicazione. Nel seguito sono riportati i principali punti di attenzione estratti dalle linee guida OWASP.

Nel documento sono analizzate e descritte altresì necessità e attività relativamente alla manutenzione correttiva, adeguativa ed evolutiva del software sviluppato in produzione dopo le fasi di sviluppo, test e rilascio.

I concetti di protezione dei dati fin dalla progettazione (Privacy by Design) e di protezione per impostazione predefinita (Privacy by Default) rappresentano due capisaldi del GDPR. Il rispetto di questi due fondamentali principi garantisce la tutela costante e continuativa dei diritti degli interessati da parte del Titolare dei Trattamenti di dati personali. Qualsiasi progetto (sia strutturale sia concettuale) va realizzato considerando dalla progettazione (appunto by design) la riservatezza e la protezione dei dati personali, ove si prevede che questi siano implicati.

Approccio generale

Un software “è sicuro” IN RELAZIONE alle minacce che sono identificate per le funzioni previste, al livello di rischio calcolato per le singole minacce e alle misure di sicurezza poste in essere per mitigare i livelli di rischio associati alle minacce.

Intesys, per ogni nuovo progetto software e per ogni major release di software esistenti effettua una accurata analisi dei rischi attraverso una precisa metodologia che prevede l'identificazione delle minacce per la sicurezza che lo possono riguardare, il calcolo del livello di rischio per ogni minaccia, l'identificazione e la implementazione delle misure di sicurezza che mitigano i rischi calcolati.

Con l'obiettivo di definire e mettere in atto metodologie di sviluppo software e di gestione di progetti software che tengano conto anche della compliance con il GDPR abbiamo organizzato il nostro approccio definendo, specificatamente per il GDPR, due ambiti di intervento differenziati:

- metodologie e strumenti per garantire la sicurezza dei dati personali (privacy), speculare nell’approccio a quello relativo alla sicurezza del software
- metodologie e strumenti per garantire i diritti degli interessati

Minacce

L'individuazione e la modellazione delle minacce relative alla sicurezza informatica viene effettuata seguendo il modello STRIDE (https://en.wikipedia.org/wiki/STRIDE_(security).

Le minacce tenute in considerazione sono quindi le seguenti:

1. Spoofing (esteso più in generale ad "accesso non consentito")
2. Tampering (esteso anche a "dati resi indisponibili")
3. Repudiation
4. Information disclosure (privacy breach / data leak)
5. Denial of service
6. Elevation of privilege (esteso più in generale a "autorizzazione non coerente")

Spoofing (e accesso non consentito)

Si intende l’accesso ad un sistema informatico senza averne diritti (la persona/applicazione non è registrata come utente/servizio con diritti di accesso) o con credenziali non proprie (la persone/applicazione è registrata come utente/servizio ma accede con altra credenziale). Il termine «accesso» va inteso nel senso di «autenticazione» e distinto dal significato «visione,

modifica, cancellazione o creazione». Le misure attinenti questa minaccia sono quelle relative principalmente a autenticazione, autorizzazione e gestione degli accessi.

Tampering (e dati resi indisponibili)

Per (data) tampering intendiamo una deliberata manomissione di dati. Per esempio: cambi non autorizzati a dati persistenti contenuti in DB o operazioni che alterano i dati salvati da una transazione online. In questo contesto estendiamo il tampering con la mancanza di disponibilità di dati (i.e. perdita di dati) dovuta a cancellazione o a sovrascrittura (es. restore fallito) o a furto dei dati (in alcuni casi l'evento può anche essere causato da errore o incuria e non da intervento malevolo).

Repudiation

Questa minaccia è associata a casi in cui un utente/azienda/persona fisica nega di aver effettuato una azione/operazione senza che si possa provare/contestare il contrario. Il caso tipico è quello in cui un utente effettua una operazione illegale in un sistema senza che l'operazione sia tracciata o in un modo che permette di contestare l'autenticità del tracciamento. Un altro caso è quello in cui un utente effettua una operazione, legale (per esempio la firma di un contratto), e ne disconosce la responsabilità.

In generale un software/sistema, per fronteggiare questa minaccia, deve tracciare i dati relativi a operazioni "ripudiabili" e fornire prova forte della integrità del dato tracciato. Bisogna distinguere azioni per aumentare la garanzia di autenticità del dato realizzate dal software sviluppato piuttosto che messe in atto a livello sistemistico (esternamente al software), per esempio il trasferimento immediato dei log su un sistema diverso da quello "sorgente" che abbia utenze diversificate e/o dispositivi di memorizzazione read-only e/o sistemi di notarizzazione dei dati. In generale è attribuibile al software la responsabilità di generare dati di log delle operazioni che potrebbero fronteggiare minacce di ripudio delegando a livello di sistema di mettere in atto azioni per garantire l'integrità dei dati.

Information disclosure

Information disclosure riguarda il "mettere a disposizione" (in lettura e quindi anche per una diffusione non consentita) informazioni a persone che non dovrebbero averne il diritto/possibilità. Per esempio la possibilità di un utente di leggere un file per il quale non ne avrebbe diritto. Nel caso di gestione di dati personali si sta parlando di privacy breach / data leak / data breach, casistica precisamente normata dal GDPR.

Denial of service

Si intende una situazione in cui il normale funzionamento del servizio è bloccato o reso talmente lento da risultare praticamente inutilizzabile.

Elevation of privilege

Dopo la fase di autenticazione si intende, da parte di una persona o di un servizio, l'accesso a dati e servizi applicativi con privilegi diversi da quelli assegnati alle credenziali (utenza) che hanno effettuato l'autenticazione, in generale superiori Per esempio un utente senza privilegi specifici può guadagnarne in modo indebito fino a compromettere o distruggere tutti i dati di un sistema o il sistema stesso. Si può dare anche il caso di visibilità di dati di un altro profilo, quindi senza avere privilegi aggiuntivi ma tali da accedere e modificare dati teoricamente non disponibili.

Analisi e calcolo del livello di rischio

Il livello di rischio viene calcolato sulla base della composizione di Impatto e Probabilità.

Seguendo varie metodologie (OWASP in primis) assegniamo un valore (ALTO-MEDIO-BASSO) alla PROBABILITA' che una minaccia venga sfruttata (exploited) e un valore (ALTO-MEDIO-BASSO) al relativo IMPATTO.

La composizione delle due dimensioni PROBABILITA' e IMPATTO è regolata secondo la tabella seguente.

		PROBABILITA'		
		[B]ASSA (1)	[M]EDIA (2)	[A]LTA (3)
IMPATTO	[B]ASSO (1)	[B]ASSO (1)	[B]ASSO (1)	[M]EDIO (2)
	[M]EDIO (2)	[B]ASSO (1)	[M]EDIO (2)	[A]LTO (3)
	[A]LTO (3)	[M]EDIO (2)	[A]LTO (3)	[A]LTO (3)

Probabilità

La probabilità viene calcolata assegnando un valore (1-2-3 / B-M-A) relativamente a 4 «Threat Agent Factors»-TAF (OWASP Risk Rating Methodology, prima parte). Per la valutazione dei singoli TAF bisogna identificare, minaccia per minaccia, il Gruppo di Threat

Agents-GTA relativi, cioè caratterizzare i gruppi di persone che possono avere interesse, capacità o semplice possibilità di minacciare l'applicazione. Vanno tenuti in considerazione SIA "insiders" SIA "outsiders" e vanno tenuti in considerazione attacchi malevoli ma anche errori od omissioni involontari (questo in particolare per utenti "insider").

Di seguito sono elencati e descritti i 4 Threat Agent Factors presi in considerazione:

Livello di competenza tecnica posseduto dal Gruppo di Threat Agents (GTA) [LCT]: 3=alto (security penetration skill), 2=medio, 1=nessuno

Motivazione del GTA [MOT]: 3=alta ricompensa, 2= media ricompensa, 1=nessuna/bassa ricompensa

Opportunità disponibili/Risorse richieste al GTA [ORR]: 3=molte opportunità/risorse generiche, 2=alcune opportunità/risorse speciali, 1=nessuna opportunità/risorse costose e complesse

Dimensione del GTA [TAD]: 3=anonymus, 2=intranet/extranet (authenticated), 1=sviluppatori, sysadm

Il valore di PROBABILITA' è calcolato secondo la seguente tabella ("na" viene valutato =1)

PROBABILITA'	BASSO	MEDIO	ALTO
Somma valori	4-5	6-7-8-9	10-11-12

Impatto (sicurezza)

L'impatto relativamente all'ambito generale della sicurezza delle informazioni viene calcolato assegnando un valore (1-2-3 / B-M-A) relativamente a 4 «Key Impact Indicators» (vedi www.ictsecuritymagazine.com/articoli/key-impact-indicator-e-key-risk-indicator-per-la-cyber-risk-evaluation/):

Perdita di profitto [PRO]: 3=considerevole, 2=non trascurabile, 1=trascurabile.

Danno di reputazione [REP]: 3=considerevole, 2=non trascurabile, 1=trascurabile.

Multe/Spese legali [MSL]: 3=considerevole, 2=non trascurabile, 1=trascurabile.

Costo di ripristino [CRP]: 3=considerevole, 2=non trascurabile, 1=trascurabile.

(per [CRP] si considerano Mean Time To Repair, Equipment, People Unable to Work, Handling)

Il valore di IMPATTO (sicurezza) è calcolato secondo la seguente tabella ("na" viene valutato =1)

IMPATTO (sicurezza)	BASSO	MEDIO	ALTO
Somma valori	4-5	6-7-8-9	10-11-12

Impatto (GDPR)

L'impatto relativamente all'ambito specifico GDPR viene calcolato in due fasi:

Nella prima fase si valuta se il software gestirà dati relativi ad una tipologia di trattamento da sottoporre a valutazione d'impatto secondo le indicazioni del Garante per la protezione dei dati personali. Tali dati sono riconducibili alle seguenti fattispecie:

- Trattamenti valutativi o di scoring su larga scala che comportano la profilazione degli interessati e lo svolgimento di attività predittive.
- Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato.
- Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti.
- Trattamenti su larga scala di dati aventi carattere estremamente personale.
- Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti.
- Trattamenti sistematici, su larga scala e per periodi prolungati di dati biometrici e genetici.
- Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti cronici, richiedenti asilo).

Se una sola di queste fattispecie è implicata dal software oggetto del progetto l'impatto viene calcolato di livello "ALTO" e non viene effettuata la seconda fase.

In alternativa viene assegnato un valore (1-2-3 / B-M-A) relativamente a

Quantità di dati personali oggetto di trattamento [QTD]: 3 = considerevole, 2 = non trascurabile, 1 = trascurabile;

Tipologia di dati personali oggetto di trattamento [TIP]: 3 = particolari (es. orientamento sessuale o politico, condizioni di salute, dati giuridici, genetici, biometrici, ecc.), 2 = soggetti a rischi specifici (es. coordinate bancarie, carte di credito), 1 = comuni (es. anagrafica);

Quantità di interessati i cui dati personali sono oggetto di trattamento [QTI]: 3 = considerevole, 2 = non trascurabile, 1 = trascurabile;

Il valore di IMPATTO (GDPR) è calcolato secondo la seguente tabella

IMPATTO (GDPR)	BASSO	MEDIO	ALTO
Somma valori	3-4	5-6-7	8-9

Il valore di IMPATTO finale è dato dalla composizione delle tue tipologie di impatto secondo la tabella seguente

		IMPATTO (sicurezza)		
		[B]ASSO	[M]EDIO	[A]LTO
IMPATTO (GDPR)	[B]ASSO	[B]ASSO	[B]ASSO	[M]EDIO
	[M]EDIO	[B]ASSO	[M]EDIO	[A]LTO
	[A]LTO	[M]EDIO	[A]LTO	[A]LTO

Assessment

Per ogni singola minaccia, relativamente alle caratteristiche funzionali e ai dati gestiti relativamente al progetto, viene calcolato il valore di probabilità e di impatto e quindi il livello di rischio. I risultati vengono riportati in uno specifico documento di Assessment per lo Sviluppo di Software, sicuro e GDPR compliant, (ASSS) e forniscono un quadro completo e preciso delle misure di sicurezza che saranno implementate per mitigare gli specifici rischi del progetto software o della major release in fase di sviluppo.

Misure di sicurezza

Intesys ha raccolto un vasto insieme di misure di sicurezza suddivise nelle sei categorie di minacce modellate da STRIDE identificando a priori quelle proporzionate (adatte a mitigare)

ad un livello di rischio BASSO e quelle proporzionate (adatte a mitigare) agli altri due livelli di rischio (MEDIO e ALTO).

Le misure di sicurezza proporzionate al livello di sicurezza BASSO vengono considerate obbligatorie di default (BASE) e vengono quindi applicate SEMPRE a prescindere dal livello di rischiosità.

L'elenco puntuale delle misure specifiche applicate al singolo progetto è contenuto nel documento ASSS e fa riferimento alle misure relative a livelli di rischio di livello MEDIO e ALTO.

Il documento ASSS è redatto d'accordo con il cliente nel caso venga concordata l'effettuazione dell'analisi del rischio e la definizione delle misure di sicurezza da implementare sulla base dei relativi risultati.

Rischio calcolato e misure da applicare

MINACCE E MISURE - SCHEMA DI APPLICAZIONE

Lo schema dele misure di sicurezza da applicare in relazione al calcolo del rischio effettuato (aggiuntive rispetto a quelle "BASE") sono riportate per chiarezza nella seguente tabella.

MINACCE STRIDE	Rischio (P*I)	MISURE:
M1 - Spoofing (e accesso non consentito)	BASSO	BASE
	MEDIO	Spoofing livello MEDIO
	ALTO	Spoofing livello ALTO
M2 - Tampering (e dati resi indisponibili)	BASSO	BASE
	MEDIO	Tampering livello MEDIO
	ALTO	Tampering livello ALTO
M3 - Repudiation	BASSO	BASE
	MEDIO	Repudiation livello MEDIO
	ALTO	Repudiation livello ALTO
M4- Information disclosure	BASSO	BASE
	MEDIO	Information disclosure livello MEDIO
	ALTO	Information disclosure livello ALTO
M5 - Denial of service	BASSO	BASE
	MEDIO	Denial of service livello MEDIO
	ALTO	Denial of service livello ALTO
M6- Elevation of privilege (autorizzazione non coerente)	BASSO	BASE
	MEDIO	Elevation of privilege livello MEDIO
	ALTO	Elevation of privilege livello ALTO

Il documento ASSS descrive puntualmente, per il singolo progetto del cliente, quali misure verranno applicate sulla base del calcolo del rischio effettuato relativamente ad ogni minaccia.

Piano dei test

In Intesys è stato definito un processo di Software Quality Assurance (SQA) con l'obiettivo di assicurare che il processo di sviluppo software sia monitorato e sia compliant con lo standard ISO27001 e il GDPR.

Analisi del codice statico

Per quanto riguarda i requisiti di sicurezza del software abbiamo standardizzato un sistema preciso e strutturato relativo all'analisi del codice statico (ACS) che ci permette di testare in maniera automatica qualità e rispetto di requisiti di sicurezza lungo tutto il processo di sviluppo.

Test del proprio codice (approccio “Clean as you code”)

L’approccio adottato, definito “Clean as you code” prevede che lo sviluppatore abbia la responsabilità personale del codice prodotto, evitando così che siano altri a dover intervenire sul codice del singolo sviluppatore.

Test generale del progetto

Oltre alle scansioni effettuate puntualmente (in automatico in logica di continuous integration) da ogni sviluppatore, per ogni merge in develop/master da una pull request viene eseguita una scansione SonarQube per controllare che lo stato del repository garantisca ancora una elevata qualità. Il risultato sarà visibile nella pagina principale del progetto, a disposizione per il controllo di qualità previsto da parte del Project Manager.

Test funzionali

Riteniamo, in generale, che i test funzionali del software siano da effettuare a cura del cliente a garanzia di imparzialità del processo e della rendicontazione.

Intesys effettua comunque delle attività pianificate di test funzionale di tipo "interno" quale ulteriore verifica, da un punto di vista della sicurezza, che le misure sopra descritte siano state correttamente implementate e risultino efficaci a mitigare le minacce modellate con la categorizzazione STRIDE.

Diritti degli interessati

In questa sezione descriviamo il nostro approccio relativamente ad una serie di misure implementative relative al GDPR che riteniamo DEBBANO ESSERE MESSE IN ATTO SEMPRE a prescindere dall'analisi del rischio in quanto non impattano tematiche di sicurezza-privacy dei dati ma sono necessarie per garantire all'interessato (la persona fisica di cui vengono trattati dati personali) la tutela di una serie di diritti.

I diritti che prendiamo in considerazione sono i seguenti:

- minimizzazione
- oblio (cancellazione totale)
- portabilità
- trasparenza (informazione e accesso ai propri dati)
- rettifica (modifica/cancellazione parziale)
- esattezza

Per ognuno dei sei diritti sopra menzionati sono definite delle precise misure di sicurezza che vengono applicate nello sviluppo del software. Le misure relative ai diritti degli interessati sono comprese tra le misure cosiddette "base".

Continuous security

Una metodologia per lo sviluppo di codice “sicuro” deve includere monitoraggio, controlli e azioni durante la vita in produzione del software.

In ottica di un processo di Continuous Security e in accordo con il documento dell'AGID "Linee guida per l'adozione di un ciclo di sviluppo di software sicuro", quando contrattualizzata con il cliente, viene applicata una procedura che prevede:

- una volta all’anno: rianalisi del rischio condivisa con il cliente con eventuale rivalutazione delle misure di sicurezza adottate e relativa valutazione delle modifiche da apportare al codice (security refactoring);
- una volta ogni tre mesi: valutazione generale dell'esistenza di Patch di sicurezza applicabili al software sviluppato;
- una volta ogni tre mesi: scansione delle eventuali vulnerabilità di tutte le librerie esterne utilizzate nei progetti;

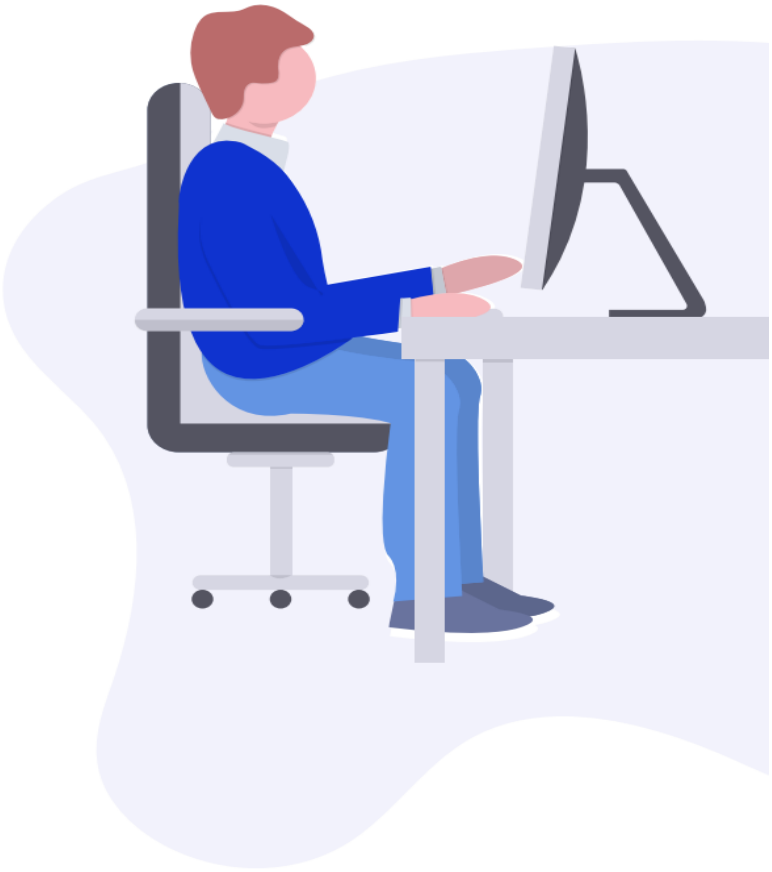
- una volta ogni tre mesi: coerenza delle librerie con la lista di tools approvata internamente.

La scansione è effettuata tramite DEPENDENCY CHECK, un Tool di Software Composition Analysis (SCA) sviluppato da OWASP che ha come obiettivo il rilevamento di vulnerabilità note all'interno delle dipendenze di un progetto. Questa scansione permette di avere evidenza di tutte le librerie software utilizzate con le relative versioni.

Relativamente alle librerie software è stata adottata una precisa Policy di gestione delle librerie di terze parti nel software aziendale che prevede:

- analisi delle vulnerabilità delle librerie di terze parti:
  - alla build di ogni nuova release
  - settimanalmente, con scansioni pianificate, per tutte le release che sono attualmente in esercizio presso gli ambienti di un cliente
- analisi delle vulnerabilità con conseguente:
  - quantificazione del livello di rischio connesso
  - condivisione con il cliente di eventuali scenari puntuali di rischio
  - definizione di azioni di remediation
- scelta centralizzata delle librerie software (stesse librerie per tutti gli sviluppatori)
- manutenzione regolare del catalogo interno delle librerie

Intesys



Intesys

Ci trovate qui

- Intesys
- @intesys_it
- 045 503 663
- info@intesys.it
- www.intesys.it

Visitate il nostro Journal

- intesys.it/journal/