Linee guida per la sicurezza delle applicazioni - Progettazione

InfoCert
TINEXTA GROUP

SOMMARIO

1 NOVITÀ INTRODOTTE RISPETTO ALLA PRECEDENTE EMISSIONE

VERSIONE/RELEASE N°:	2	**Data Versione/Release:**	18/08/2020
Descrizione modifiche:	Revisione generale del documento		

VERSIONE/RELEASE N°:	1	**Data Versione/Release:**	gg/mm/2017
Descrizione modifiche:	Prima emissione		

2 SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO

2.1 MOTIVAZIONI

Lo scopo di questa politica è il seguente:
- fornire le indicazioni a cui attenersi nella progettazione e manutenzione dei prodotti InfoCert
- assicurare il rispetto di leggi e normative

In questo documento sono presentati i requisiti di sicurezza che devono essere considerati nel progettare un prodotto/servizio, sia esso completamente nuovo oppure una revisione o estensione di qualcosa già esistente.

Va da sé che queste linee guida non vogliono e non possono sostituire testi e siti specializzati, a cui si rimanda per le questioni tecniche di dettaglio, per gli approfondimenti teorici e, soprattutto, per un costante aggiornamento con lo stato dell'arte delle vulnerabilità e delle tecniche di sviluppo.

Quanto contenuto in questo documento si applica anche alle applicazioni o parti di esse il cui sviluppo sia stato dato in outsourcing a terze parti. Ove possibile si applica anche ai package acquistati.

2.2 DESTINATARI

La politica si applica a tutto il personale e/o terze parti impegnate nel progettare ed erogare prodotti e servizi per conto InfoCert e per terzi.

Sono interessate tutte le strutture aziendali.

2.3 VALIDITÀ

La politica entra in vigore il 01/10/2011.

2.4 AGGIORNAMENTO DELLA POLITICA E VIOLAZIONI

L'aggiornamento del documento viene valutato almeno annualmente. La gestione delle violazioni alle politiche di sicurezza aziendali è regolata dalle norme in vigore che regolano i contratti di lavoro.

3 RIFERIMENTI NORMATIVI E STANDARD

3.1 Standard e norme di riferimento

Si riporta una sintesi non esaustiva della legislazione e degli obblighi normativi e contrattuali che contribuiscono alla forma e al contenuto di questa politica:

- Framework Nazionale Cybersecurity 2.0
- ISO 27001:2013
- NIST SP 800-53 rev.4
- GDPR (UE 2016/679, Regolamento Generale sulla Protezione dei Dati)

4 POLITICA

Tutti i prodotti/servizi dovrebbero attenersi ai seguenti requisiti. Eventuali scostamenti devono essere esplicitamente giustificati.

I requisiti che si riferiscono alla manutenzione del prodotto/servizio possono essere ignorati esclusivamente in sede di progettazione di un prodotto/servizio totalmente nuovo.

In qualche caso specifico è possibile che il requisito, per la particolare tipologia di prodotto/servizio, risulti non applicabile.

In tal caso il motivo dell'esclusione del controllo deve essere riportato nella documentazione di progetto.

4.1 Normative e requisiti

Nello sviluppare il prodotto/servizio devono essere prese in considerazione le eventuali norme (leggi, regolamenti, standard) che regolano la materia oggetto del prodotto/servizio.

Nel redigere il progetto devono essere esplicitati gli ulteriori requisiti derivanti dalle norme settoriali.

Le norme possono richiedere l'applicazione di requisiti ulteriori rispetto a quelli qui elencati (per es. certificazioni di sicurezza di prodotti o dispositivi su cui il prodotto/servizio si basa).

Ogni prodotto/servizio deve essere corredato da una Data Protection Impact Analysis, individuando i rischi (minacce, probabilità e impatto) per i diritti delle persone i cui dati vengono trattati.

I dati devono essere preventivamente classificati per valutarne le esigenze di riservatezza.

Nel progettare il prodotto/servizio va delimitato l'ambito di utilizzo. Vanno quindi identificate (in riferimento alla normativa sulla privacy o alle specifiche richieste di un cliente, nel caso di forniture di servizi e/o prodotti personalizzati) le tipologie di dati che verranno trattati e selezionati i controlli, tra quelli contenuti in questo documento, che si adattano alla specifica tipologia.

Se l'ambito non è prevedibile, occorrerà progettare il prodotto/servizio ipotizzando il “worst case”.

4.1.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- ISO 27001:2013: A.14.1.1, A.14.2.1,
- NIST SP 800-53 rev.4: PL-8, SA-8, SA-15, SA-17
- GDPR: Art. 5, 6, 9, 11, 30, 32

4.2 Valutazione del rischio

Devono essere valutati i rischi (minacce, probabilità e impatto) per l’azienda, per i clienti e per gli utenti, al fine di selezionare i controlli adeguati.

La combinazione tra la classificazione dei dati trattati, gli eventuali impatti in tema di Data Protection e l’ambito di utilizzo, determinano i rischi che possono derivare all’azienda in termini di reputazione, danno economico, violazione normativa, sanzioni etc.

4.3 Integrità dei dati

L’integrità dei dati deve essere assicurata “at rest”, “in transit” ed “end-to-end”. In particolare:

- bisogna garantire, utilizzando HTTPS o tecniche di firma, che il dato trasmesso non venga alterato quando transita sulla rete. Utilizzare il protocollo TLS 1.2 o superiore.

- l'aggiornamento dei dati memorizzati deve essere consentito solo ai soggetti autorizzati e bisogna evitare che possano essere effettuate modifiche non volute, per errore o per dolo

- l'integrità dei dati memorizzati, quale che sia il dispositivo fisico, deve essere assicurata mediante il controllo degli accessi e adottando tecniche che permettano di rilevare cambiamenti non voluti (tecniche che possono essere embedded nei prodotti di base adottati). Questo include, ove applicabile, le tecniche di controllo del buon esito delle transazioni. Vanno inoltre definite politiche di backup e ritenzione dei dati

- nel caso di utilizzo di package sviluppati da terzi, devono essere implementati meccanismi automatici atti a controllare l'integrità e autenticità dei prodotti installati

4.3.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- Framework Nazionale Cybersecurity 2.0: PR.DS-6, PR.MA-1
- ISO 27001:2013: A.11.2.4, A.14.1.2, A.14.1.3
- NIST SP 800-53 rev.4: SC-16, SI-7
- GDPR: Art. 5, 32

4.4 Riservatezza dei dati

La riservatezza dei dati deve essere assicurata "at rest", "in transit" ed "end-to-end". In particolare:

- va garantito che i dati personali non siano leggibili da soggetti non autorizzati durante il loro transito in rete. Questo può essere ottenuto tramite la cifratura dei dati, con l'utilizzo del protocollo HTTPS oppure tramite VPN, purché i capi della connessione sicura siano sotto il controllo di soggetti autorizzati

- per le altre tipologie di dati, non soggetti al GDPR, la valutazione dell'opportunità o meno di applicare tecniche di protezione del traffico dipende da quanto emerso nel trattare i requisiti riportati nel paragrafo precedente. Tuttavia, l'uso del protocollo HTTPS è fortemente raccomandato

- la lettura dei dati memorizzati deve essere consentita solo ai soggetti autorizzati. È quindi necessario prevedere la profilatura dei soggetti (system administrator, DBA, utenti finali, altri eventuali), stabilendo per ciascun profilo a quali dati e per quali operazioni l'accesso è consentito. Va inoltre garantita la segregazione dei dati, cioè l'impossibilità per l'utente X di accedere ai dati dell'utente Y quando X≠Y. Tale segregazione si applica anche ai dispositivi di salvataggio, per consentirne il trattamento selettivo in caso di cancellazione e di ripristino

- i dati particolari, quali quelli che possono rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, i dati giudiziari e quelli relativi ai mezzi di pagamento, devono essere crittografati anche quando a riposo. La cifratura di altre tipologie di dati va valutata sulla base della tipologia e delle minacce.

- tutti i requisiti descritti in questo paragrafo devono essere garantiti anche sui supporti di backup e su ogni altro supporto su cui i dati transitino o risiedano, incluse le copie (totali o parziali) predisposte per sviluppi, test e collaudi

4.4.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- ISO 27001:2013: A.14.1.2, A.14.1.3
- GDPR: Art. 5, 9, 32

4.5 Disponibilità del servizio e dei dati

Il prodotto/servizio deve prevedere e stabilire i propri requisiti in termini di disponibilità, specificando i seguenti requisiti:

- alta affidabilità
- massimo tempo accettabile di indisponibilità
- Recupero dal Disastro (Disaster recovery)
- Continuità Operativa (Business Continuity)

4.5.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- ISO 27001:2013: A.14.1.2, A.14.1.3
- GDPR: Art. 5, 32

4.6 Cancellazione dei dati

Deve essere prevista la cancellazione fisica e/o logica dei dati.

Per i dati che non è più lecito conservare, deve esserne prevista la cancellazione, da tutti i dispositivi, inclusi quelli di backup.

4.6.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- GDPR: Art. 5, 30, 32

4.7 Autenticazione e time-out

L'interazione con l'utente, qualora non sia puramente informativa, deve prevederne l'autenticazione.

Per i dati sensibili deve essere usata la strong authentication (multifattore).

Le modalità di autenticazione (semplice o strong) vanno proporzionate alla tipologia dei dati trattati.

Nel caso in cui il prodotto/servizio non si appoggi ad un sistema di autenticazione centralizzato, deve rispettare le seguenti regole:

- deve assicurare che le credenziali siano conformi alla password policy aziendale ed alla normativa
- non deve memorizzare le password

- deve consentire la modifica della password
- deve adottare una politica di scadenza delle password
- deve limitare il numero di tentativi di accesso con credenziali errate (dopo un certo numero di tentativi, non superiore a 10, l'account deve essere disabilitato)
- deve prevedere un intervallo tra un tentativo di autenticazione e il successivo (un ritardo di 5s tra un tentativo di autenticazione e l'altro riduce di parecchio l'efficacia degli attacchi “brute force” e “Dictionary”)
- deve implementare un time-out di chiusura delle sessioni, in caso di perdurante inattività dell'interlocutore (umano o sistema). L'intervallo per l'attivazione del time-out dovrebbe essere configurabile, tuttavia dovrebbe essere non superiore a 15 minuti

4.8 Logging

Le attività devono essere loggate, sia a fini di debugging che di tracciamento delle attività. È opportuno prevedere un logging configurabile a più livelli.

Il livello minimo deve permettere di risalire a:

- chi ha fatto una determinata operazione
- quando l'ha fatta
- su che oggetti.

Deve essere valutata la necessità che il timestamp del log sia fornito da una marca temporale, verificando eventuali obblighi di legge ed eventuali considerazioni di opportunità in caso di contestazione.

Devono essere definite le esigenze di conservazione dei log sulla base dei vincoli normativi. In particolare, nell'ambito della privacy, della Certificazione Digitale e della PEC, il progetto deve stabilire tempi e modalità per la conservazione dei log.

4.8.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- GDPR: Art. 5

4.9 Segregazione degli ambienti

Gli ambienti di sviluppo, test e produzione devono essere separati per ridurre il rischio di accesso o cambiamenti non autorizzati.

4.9.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- Framework Nazionale Cybersecurity 2.0: PR.DS-7
- ISO 27001:2013: A.12.1.4

4.10 Ciclo di vita dei dati e del software

Deve essere definito un processo per la gestione del ciclo di vita del software e dei dati.

Devono essere definite e documentate le modalità per tenere traccia del ciclo di vita dei dati personali (dalla raccolta alla conservazione, fino alla distruzione).

Ogni modifica della tipologia dei dati che il prodotto/servizio tratta deve essere verificata contro tutti i requisiti elencati nel presente documento. Il prodotto/servizio, inizialmente progettato per trattare solo dati pubblici può, per esempio, essere esteso a trattare anche dati personali o dati sanitari. Questa estensione comporta una

revisione del progetto per assicurarne la validità al nuovo contesto applicativo.

I cambiamenti ai sistemi all'interno del ciclo di vita devono essere tenuti sotto controllo attraverso l'utilizzo di procedure formali di controllo dei cambiamenti.

Solo le modifiche approvate formalmente possono essere implementate. Tutte le modifiche devono essere documentate, valutandone i potenziali impatti dal punto di vista della sicurezza.

Quando avvengono dei cambiamenti nelle piattaforme operative, le applicazioni critiche per il business devono essere riesaminate e sottoposte a test per assicurare che non ci siano impatti negativi sulle attività operative dell'organizzazione o sulla sua sicurezza.

4.10.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- Framework Nazionale Cybersecurity 2.0: PR-ID.DM-1, PR.IP-2
- ISO 27001:2013: A.14.2.2, A.14.2.3, A.14.2.6
- NIST SP 800-53 rev.4: SA-3, SA-10, MA-2

4.11 Non ripudio

Deve essere valutata la necessità di funzionalità di non ripudio. Ad esempio, devono essere firmati contratti con le cosiddette clausole vessatorie.

4.12 Licenze

Il prodotto/servizio deve rispettare le condizioni di licenza del software di terzi adottato nella realizzazione.

4.13 Vulnerabilità

Il prodotto/servizio non deve contenere vulnerabilità note.

Laddove possibile, deve essere previsto, in fase di progetto, l'utilizzo di appositi tools per individuare e correggere eventuali vulnerabilità già durante la fase di sviluppo.

4.13.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- NIST SP 800-53 rev.4: SA-11

4.14 Sviluppo affidato all'esterno

Infocert deve supervisionare e monitorare l'attività di sviluppo dei prodotti/servizi affidata all'esterno.

Prima di firmare il contratto con il fornitore, deve condurre una verifica in merito all'affidabilità del fornitore stesso e ai processi che esso utilizza per progettare, sviluppare, testare, etc

4.14.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- ISO 27001:2013: A.14.2.7
- NIST SP 800-53 rev.4: SA-12

4.15 Test

Durante lo sviluppo devono essere effettuati test relativi alle funzionalità di sicurezza del prodotto/servizio.

Devono essere stabiliti dei programmi di test e di accettazione (e i criteri ad essi relativi) per i nuovi prodotti/servizi, per gli aggiornamenti e per le nuove versioni.

I dati utilizzati per effettuare i test devono essere scelti con attenzione, protetti e tenuti sotto controllo.

4.15.1 RIFERIMENTI NORMATIVI

La presente raccomandazione copre i seguenti controlli normativi:

- ISO 27001:2013: A.14.2.8, A.14.2.9, A.14.3.1
- NIST SP 800-53 rev.4: CM-2