# *Standard di sicurezza infrastrutturali per Applicazioni*

## Controllo Emissione

| | Ente Aziendale | Nome |
|---|---|---|
| **Proposto da** | DIDT/ITC/CISO | A. DE MARTINO |
| **Verificato da** | DIDT/ITC<br>DIDT/ITR<br>DIDT/GSC<br>DIDT/STW | E. NOTARCOLA<br>F. FIASCHI<br>R. PIGNIERI<br>S. GALDENZI |
| **Autorizzato da** | DIDT | F. DEL GRECO |

# Registro delle modifiche

| Rev. | Motivo | Autore delle modifiche | | Data |
|---|---|---|---|---|
| | | **Ente Aziendale** | **Nome** | |
| 1.0 | Prima stesura | AD/ITS/ITI/SIT | P. Tognozzi | 09/05/2011 |
| 2.0 | Standard autenticazione per applicazioni per smartphone (App) | AD/ITS/ITI/SIT | P. Tognozzi | 10/03/2014 |
| 3.0 | Revisione per ISO27001 | AD/ITS/ITI/SIT | P. Tognozzi | 18/04/2014 |
| 3.1 | Gestione timeout di sessione | AD/ITS/ITI | A. De Martino | 05/06/2015 |
| 3.2 | Aggiornamento sigle aziendali<br>Aggiunta capitoli 7, 8 | AD/ITS/ITI | A. De Martino | 10/05/2016 |
| 3.3 | Agg. par. 4.1 per Federazione e . cap.9 per crittografia. | AD/ITS/ITI | P. Tognozzi | 16/05/2017 |
| 3.4 | Agg. Variazione Organizzativa | AD/ITS/ITI | P. Tognozzi | 11/06/2018 |
| 3.5 | Ins. Par 6.1 e aggiornamento organizzativo | AD/ITS/ITC/CISO<br>AD/ITS/ITC/PPS | A. De Martino<br>P. Tognozzi | 19/02/2019 |
| 4.0 | Aggiornamento §7, schema metodologico, misure di sicurezza web, mobile, cloud | DGCO/ITS/ITC/CISO | A. De Martino | 12/12/2019 |
| 4.1 | Aggiornamento §10, requisiti per l'acquisto di servizi critici esterni | DIDT/ITC/CISO<br>DIDT/ITR/SCR | A. De Martino<br>M. Caleri | 03/08/2020 |

# Riferimenti

| Rif. | Nome del documento | Descrizione |
|---|---|---|
| 1 | UNI - ISO | UNI CEI ISO/IEC 27001:2014 - Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni – Requisiti |
| 2 | UNI - ISO | UNI CEI ISO/IEC 27002:2014 - Tecnologie informatiche - Tecniche per la sicurezza - Raccolta di prassi sui controlli per la sicurezza delle informazioni |
| 3 | ASPI_MN_ITS_SGSI | Manuale del Sistema di Gestione della Sicurezza delle Informazioni |
| 4 | ITS_ST_SYS01 | Standard e vincoli architetturali |
| 5 | ITS_DC-SLG06 | TAM Linee guida per l'integrazione di applicazioni |
| 6 | ITS_DC_BDL01 | Abilitazioni Applicative |
| 7 | ITS_ST_BDL01 | Standard di Nomenclatura degli oggetti relazionali |
| 8 | Regolamento (UE) n. 2016/679 | Regolamento generale sulla protezione dei dati, GDPR |
| 9 | ASPI_PR_ITC01_Change_IT | Gestione dei Cambiamenti dei Sistemi IT |
| 10 | ITS_ST_BDL02 | Linee Guida per la Gestione delle Basi Dati in ASPI |
| 11 | ITS_ST_APP01 | Ciclo di vita del software |

# Indice

# 1 Scopo del documento

Questo documento indica gli standard di sicurezza e infrastrutturali che devono essere rispettati ogni volta che viene implementata una nuova applicazione (realizzata internamente o acquistata) oppure vengono realizzate modifiche ad applicazioni esistenti.

# 2 Campo d'applicazione

Il documento si applica a tutte le applicazioni software di proprietà di Autostrade per l'Italia S.p.A (di seguito ASPI)
Il documento rappresenta il riferimento in materia, per le applicazioni di proprietà delle altre Società.

# 3 Abbreviazioni e definizioni

| Abbreviazione | Definizione |
|---|---|
| **Responsabile Informatico** | Rif.9 |
| **Sicurezza Logica** | SICUREZZA SISTEMI operante all'interno di ITS/IT Operation; referenti IT per la gestione della sicurezza logica |
| **Sicurezza IT** | Attività svolte nell'ambito della struttura IT Services/CISO che riporta alla funzione IT e Sviluppo Tecnologico. |
| **Verifica abilitazioni** | Struttura DGCS/ITS/ITC/PPS operante all'interno di ITS/IT Service. |
| **Gestione Sistemi** | Sviluppo ed Esercizio Sistemi operante all'interno ITS/IT Operation; referenti IT per la gestione sistemi (linux, unix, zos, microsoft) |
| **Gestione Rete** | Sviluppo ed Esercizio Reti operante all'interno ITS/IT Service; referenti IT per la gestione della rete |
| **Data Modeling** | Applic. Area Tecnica e Data warehouse operante all'interno di ITS/Gest. Svil.Applicaz. Traffico e DWH |

# 4 Misure di sicurezza

Di seguito vengono elencate le misure di sicurezza che ogni applicazione deve rispettare.
Tali misure sono in linea con le best practice più diffuse nel settore.

## 4.1 Autenticazione

Come sistema di autenticazione deve essere usato preferibilmente il sistema ISAM (IBM Security Access Manager) per le applicazioni WEB e per le applicazioni per smartphone APP (Rif. 5).
Se questo non è possibile (ad es. in caso di pacchetti software acquistati) è possibile utilizzare Active Directory in modalità Secure (LDAPs), per evitare il passaggio delle credenziali in chiaro. Quando le modalità possono essere perseguite entrambe il Responsabile Informatico deve concordare la scelta con Sicurezza Logica.
Qualora si usi come autenticazione ISAM, l'ultimo accesso è registrato in automatico dal prodotto e quindi non è necessario implementarlo applicativamente come descritto nel par. 3.

Nel caso di servizi, acquistati dall'esterno e resi disponibili tramite un'infrastruttura di terzi non gestita aziendalmente (ad es. SaaS, Software as a Service), è possibile permettere l'autenticazione ai dipendenti utilizzando le credenziali aziendali tramite meccanismi di Federazione, utilizzando il protocollo standard SAML (Security Assertion Markup Language). In questo caso, il fornitore esterno agisce da Service Provider e fornisce il servizio, mentre ASPI agisce da Identity Provider e fornisce i meccanismi di autenticazione/autorizzazione, permettendo all'utente di utilizzare le proprie credenziali aziendali. Le modalità di implementazione dei meccanismi di Federazione verranno dettagliati in specifici documenti, per il momento il Responsabile Informatico deve concordare questa soluzione e le relative modalità implementative con Sicurezza Sistemi.
E' possibile implementare analoghi meccanismi di Federazione anche nel verso opposto, cioè quando il servizio viene offerto da un'applicazione di ASPI o di una società del Gruppo (che in questo caso agisce quindi da Service Provider) e deve permettere l'accesso ad utenti di società esterne che vogliono utilizzare i propri meccanismi di autenticazione (e in questo caso agisce da Identity Provider). Anche in questo caso le modalità di implementazione dei meccanismi di Federazione verranno dettagliati in specifici documenti, per il momento il Responsabile Informatico deve concordare questa soluzione e le relative modalità implementative con Sicurezza Logica.

**Qualora non sia possibile realizzare quanto indicato è necessario che il Responsabile informatico ne discuta con Sicurezza IT e Sicurezza Logica, per concordare la soluzione da seguire e segnalare a Verifica Abilitazioni la nuova modalità per la verifica periodica.**

## 4.2 Autorizzazione

Le autorizzazioni devono essere gestite in una delle modalità previste:

1) proprietaria ASPI, che prevede tabelle di DB relazionale (Rif. 6) indipendentemente dal tipo di autenticazione.

**N.B.**: è sempre a carico dell'applicazione la verifica che l'utenza sia autorizzata con opportuno profilo

2) gruppi AD organizzati per una applicazione XXX sotto: OU=**XXX**, OU=Applicazioni, DC=gruppo,DC=autostrade,DC=it. Normalmente se si sceglie questa tipologia l'autenticazione è AD.

3) gruppi LDAP (importati in TAM). Questa modalità può essere scelta se l'autorizzazione è TAM.

Eccezione a queste modalità sono l'ambiente di Datawarehouse, SAP/R3 (Ruoli R3) e Domino (ACL-Domino).
Qualora non sia possibile realizzare quanto indicato è necessario che il Responsabile informatico ne discuta con Sicurezza IT e Sicurezza Logica, per concordare la soluzione da seguire.

#### 4.2.1 Profili Autorizzativi

Esistono alcuni profili che ogni applicazione deve prevedere e per questo è necessario identificarli univocamente indipendentemente dal sistema.

I profili in questione sono:

1) quello per helpdesk/sistemisti che deve prevedere le funzioni minime (solo lettura) per effettuare tutti i controlli di primo livello in caso di malfunzionamento, che il responsabile informatico ritiene opportuno.
2) quello per il responsabile informatico che deve prevedere quelle funzioni, concordate con il responsabile utente, che permettano di risolvere problemi particolari. In questo caso se ne possono fare: uno in sola visualizzazione e l'altro anche in scrittura.

Per individuare facilmente questi profili il loro codice o parte di esso dovrà contenere:

1) **HDK** - Help e Sistemisti
2) **VSW** - Visual. Sw Applicat**.** e **GSW** -Gestore Sw Applicat

### 4.3 Gestione ultimo accesso

Per alcune applicazioni è necessario implementare applicativamente la memorizzazione dell'ultimo accesso. La modalità da seguire dipende dal tipo di autorizzazione scelta.

#### 4.3.1 Applicazioni con autorizzazione proprietaria ASPI

All'interno delle tabelle proprietarie è prevista la tabella **AUTOST.TGAB11_LST_LGN** in cui l'applicativo deve memorizzare (insert o update) la data e ora di ultimo accesso dell'utente all'applicazione .

### 4.3.2 Applicazioni con autorizzazione Gruppi AD o Gruppi LDAP

Queste applicazioni se hanno un db devono usare la tabella: **AUTOST.TGAB20_LST_LGN_X05** in cui l'applicativo deve memorizzare (insert o update) la data e ora di ultimo accesso.

## 4.4 Banche Dati

Nel caso sia necessario creare un nuovo schema o modificarne uno esistente è necessario rivolgersi a Data Modeling secondo quanto indicato nell'apposito documento (Rif.10)

Per ulteriori dettagli sugli standard degli oggetti delle Banche Dati e le modalità d'accesso deve essere rispettato quanto riportato nel documento (Rif. 7)

## 4.5 Timeout sessione

La sessione utente deve scadere al massimo dopo **20m** minuti di inattività. Nel caso si usi come autenticazione TAM, il timeout è gestito da TAM.
Per esigenze particolari legate al contesto dell'applicazione è possibile specificare un timeout diverso, il Responsabile Informatico dovrà inserirlo nei requisiti di progetto valutando i rischi che ne derivano.

# 5 Standard Infrastrutturali

L'infrastruttura deve rispettare quanto riportato nel documento specifico (Rif. 4).
Qualora non sia possibile realizzare quanto previsto dal documento è necessario che il Responsabile informatico ne discuta con Gestione Sistemi.

# 6 Documentazione da produrre per il passaggio in produzione

Per il passaggio in produzione devono essere prodotti due documenti:

**XXX_procedure sistemistiche di esercizio.doc** a cura di Gestione Sistemi e/o Gestione rete

dove XXX è il codice GCS del software

**XXX_procedure applicative di esercizio.doc** a cura del Responsabile Informatico in collaborazione con IT Operation e Service Management per gli aspetti di Architettura e Livelli di Servizio.

dove XXX è il codice GCS del software

### 6.1 Applicazioni Privacy

Per il passaggio in produzione di applicazione di Privacy oltre la documentazione di cui al paragrafo precedente è necessario produrre il documento (Rif. 9):

**Criteri_Gestione_Dati_personali**, il cui template è rintracciabile nella INTRANET nella sezione 'Portali e Applicazioni - Sistemi Servizi IT - Documentazione ITS'- Template per richieste

Tale documento deve essere allegato in GCS.

# 7 Principi di sviluppo sicuro

## 7.1 Criteri generali per lo sviluppo di applicazioni software[1]

| | |
|---|---|
| Autenticazione | Implementare meccanismi di mutua autenticazione con il server.<br>Utilizzare meccanismi di autenticazione robusta, chiavi di cifratura sufficientemente lunghe e impedire l'utilizzo di quelli obsoleti come l'SSL.<br>In caso di connessioni TLS, validare il certificato e verificarne i campi.<br>Cifrare le credenziali eventualmente memorizzate.<br>Le password non devono essere cablate nel codice dell'applicazione.<br>Integrazione con sistemi di autenticazioni aziendali. |
| Crittografia e sicurezza delle comunicazioni | Le chiavi di cifratura non devono essere statiche. È opportuno che la cifratura sia realizzata con parole chiave fornite dinamicamente.<br>Cifrare i dati memorizzati in locale e quelli in transito.<br>Ridurre al minimo i flussi di comunicazione con altre applicazioni. Se l'interazione è necessaria, prevedere meccanismi di comunicazione sicura.<br>Introdurre controlli lato server, nonostante siano presenti controlli lato client, per ridurre eventuali punti di debolezza nelle comunicazioni (es. mutua autenticazione, verifica del CN del certificato, verifica della catena di certificazione, meccanismi di blocco temporaneo del IP in caso di errori ripetuti, ecc.).<br>Inibire la condivisione predefinita di dati critici su supporti esterni o in rete. |
| Gestione della sessione | Inibire la funzionalità di autocomplete nei campi username/password.<br>Eliminare la cache alla chiusura dell'applicazione.<br>Impostare un timeout di sessione ragionevolmente breve per inattività.<br>Se la sessione è terminata inaspettatamente è necessario cancellarne i dati e prevedere una nuova autenticazione.<br>Utilizzare attributi specifici per la gestione dei cookies (es. secure, httponly). |
| Linee guida generali | L'applicazione deve funzionare con i permessi minimi necessari per l'accesso alle sue risorse.<br>L'applicativo deve effettuare controlli formali sull'input dell'utente tramite l'implementazione di opportuni di opportuni meccanismi applicativi per la validazione dell'input. Inoltre, è necessario utilizzare tecniche di input sanitization ovvero convertire automaticamente l'input in una forma sicura, in una logica di whitelist.<br>Evitare race conditions.<br>Realizzare controlli per rilevare attacchi di escalation di privilegi (es. jailbreak/rooting)<br>Il codice eseguibile deve essere offuscato.<br>Utilizzare strutture dati adeguate per i dati critici.<br>Utilizzare Address Space Layout Randomization (ASLR) per impedire il buffer overrun<br>Evitare l'utilizzo del metodo di swizzling.<br>I messaggi di errore non devono contenere informazioni utilizzabili da un potenziale attaccante. |

[1] Per maggiori approfondimenti:
https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

| | |
|---|---|
| Logging e<br>Test di vulnerabilità | Escludere dai log i campi relativi alle credenziali e non loggare i dati critici.<br>Verificare che le librerie esterne prodotte da terze parti siano prive di vulnerabilità.<br>I dati di test devono essere rimossi (.apk, .ipa, ecc.).<br>Effettuare analisi statica e dinamica del codice.<br>Effettuare penetration test prima del rilascio in produzione. |

*Tabella 1. Criteri generali per lo sviluppo di applicazioni software*

## 7.2 Misure di sicurezza per le applicazioni web


TOP10_Owasp_web.xlsx

## 7.3 Misure di sicurezza per le applicazioni mobile


TOP10_Owasp_mobile.xlsx

## 7.4 Misure di sicurezza Privacy


Misure di sicurezza Privacy.xlsx

## 7.5 Misure di sicurezza Cloud


Misure di sicurezza Cloud.xlsx

# 8 Processo per la gestione dei cookies

Per la realizzazione di un sito web per servizi esposti al pubblico è necessario predisporre apposite pagine di privacy policy e cookie policy in base alla tipologia di cookies utilizzati.
Il seguente processo rappresenta una guida per la scelta delle tipologie di polices da adottare.

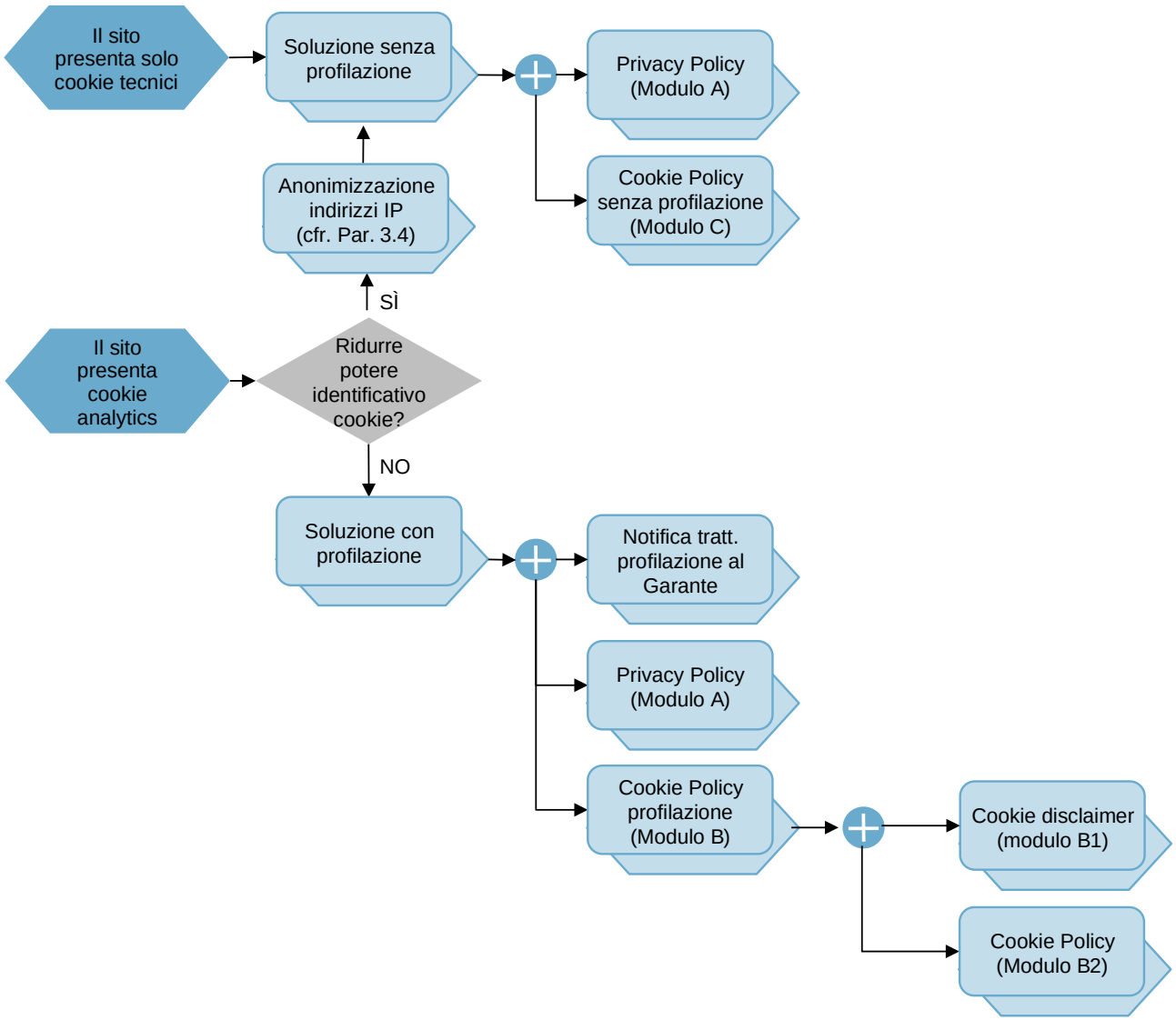


Figura 1- Processo di gestione dei cookie

### 8.1 Descrizione del processo

La seguente tabella descrive le singole azioni previste dal processo di gestione dei cookie e riporta:

- L'ID progressivo della singola azione
- L'azione correlata
- La descrizione che, nel caso nel caso in cui termini, è evidenziata dalla parola **fine del processo**.

| | | |
|---|---|---|
| **1** | Il sito presenta solo cookie tecnici | ASPI verifica se il sito utilizza esclusivamente cookie tecnici che assolvono a sole funzioni di ausilio alla navigazione e non effettua nessuna azione di analisi dei comportamenti degli utenti o di tracciamento delle operazioni effettuate |
| **1.1** | Soluzione senza profilazione | ASPI adotta la modulistica specifica predisposta per la gestione dei soli cookie tecnici:<br>• Privacy Policy<br>• Cookie policy senza profilazione |
| **1.2.** | Privacy Policy (modulo A) | ASPI inserisce sul sito web la Privacy Policy dedicata e ne segnala, tramite un link, la presenza nella home page |
| **1.3.** | Cookie Policy (modulo C) | ASPI inserisce sul sito web la Cookie Policy dedicata e ne segnala, tramite un link, la presenza nella home page **fine del processo** |
| **2** | Il sito presenta cookie analytics | ASPI verifica se il sito utilizza cookie di tipo analytics che possono analizzare il comportamento degli utenti o tracciare il tipo di operazioni effettuate sul sito |
| **3** | Riduzione potere identificativo cookie | ASPI, una volta confermata la presenza di cookie di tipo analytics, adotta una delle seguenti azioni:<br>• procede con l'anonimizzazione dell'indirizzo IP<br>• mantiene la soluzione con profilazione |
| **3.1** | Anonimizzazione dell'indirizzo IP | ASPI procede ad anonimizzare l'indirizzo IP[2], successivamente, procede implementando le soluzioni descritte nei punti 1.2 e 1.3 **fine del processo** |

[2] per procedere con l'anonimizzazione degli indirizzi IP è necessario impostare una specifica funzione reperibile a questa URL https://support.google.com/analytics/answer/2763052?hl=it&ref_topic=2919631

| | | |
|---|---|---|
| **3.2** | Soluzione con profilazione | ASPI decide di mantenere per ragioni di marketing o per conoscere le abitudini di navigazione degli utenti i cookie analytics e procede per adempiere agli obblighi normativi previsti dal provvedimento. |
| **3.2.1** | Notifica trattamento profilazione Garante | ASPI aggiorna la propria notificazione integrando lo specifico trattamento riferito alla profilazione compilando la Tabella 6 - Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi |
| | | |
| **3.2.2.** | Privacy Policy (modulo A) | ASPI inserisce sul sito web la Privacy Policy dedicata e ne segnala, tramite un link, la presenza nella home page |
| **3.2.3** | Cookie Policy (modulo B) | ASPI inserisce sul sito web:<br>• il cookie disclaimer<br>• la cookie policy per profilazione |
| **3.2.3.1.** | Cookie disclaimer (modulo B1) | ASPI posiziona il cookie disclaimer con il link alla cookie policy, all'interno di un banner dinamico che abbia le seguenti caratteristiche:<br>• dimensioni tali da rendere il banner facilmente visibile, o - in alternativa -espandibile (ad esempio, strip auto-espandibile o Pushbar)<br>• caratteri (font) più evidenti rispetto a quello del sito<br>• un colore del fondo contrastante rispetto allo sfondo del sito |
| **3.2.3.2** | Cookie policy profilazione (modulo B2) | Tramite link diretto presente nel cookie disclaimer o in fondo alla home page del sito web, ASPI posiziona la cookie policy dedicata nella quale sono evidenziati quei cookie per i quali è possibile esprimere il consenso e che, in caso di diniego sono tecnicamente esclusi. **fine del processo** |

## 8.2 ALLEGATI

Nella seguente tabella si riportano i titoli degli allegati che costituiscono l'insieme dei documenti referenziati e/o citati a vario titolo all'interno del presente Manuale e alla cui lettura si rimanda per ogni altro approfondimento

| | | |
|---|---|---|
| **1** | MODULO A – Privacy Policy |  MODULO A – Privacy Policy.doc |

| | | |
|---|---|---|
| **2** | MODULO B – Cookie Policy profilazione | Modulo B Cookie Policy profilazione.do |
| **3** | MODULO C – Cookie Policy senza profilazione | Modulo C Cookie policy senza profilazic |

## 9 Linee guida per l'utilizzo della crittografia

Le linee guida per la l'utilizzo della crittografia sono definite nel §14 del documento ITS_ST_SYS01_"Standard e Vincoli Architetturali"

## 10 Requisiti necessari per acquisto servizi critici esterni

Nel caso di acquisto dall'esterno di servizi considerati critici per il business aziendale, ed in particolare se tali servizi vengono erogati da sedi / data center diversi da quelli aziendali, devono essere previsti all'interno del capitolato tecnico un insieme aggiuntivo di requisiti di sicurezza volti a garantire il rispetto delle misure aziendali di sicurezza in particolare in ottica certificazione ISO 27001 e normativa GDPR.
Si citano come esempio i servizi erogati da fornitori terzi di Security Operation Center, di Business Continuity / Disaster Recovery oppure IaaS/PaaS/SaaS da data center esterni, di connettività alla rete internet.

Di seguito si riportano un insieme di requisiti identificati da ASPI che dovranno essere:

- Selezionati dal referente tecnico del contratto in base alla tipologia di servizio acquistato
- Riportati all'interno del capitolato tecnico di acquisto in un capitolo dedicato.
- Costituire elemento di valutazione tecnica per l'attribuzione del punteggio di gara.

| *ID* | *Categoria* | *Requisito* |
|---|---|---|
| **1** | Servizio | Il servizio deve essere erogato 24x7x365 da personale operativo e contattabile in caso di problemi o malfunzionamenti |
| **2** | | Il servizio offerto dal Fornitore deve essere erogato da centri di controllo operativo localizzati in territorio italiano/europeo e da personale italiano/europeo che parla italiano o inglese. |

| | | |
|---|---|---|
| **3** | | Il Fornitore deve essere in grado di fornire un servizio contestualizzato sul cliente, separandolo fisicamente o logicamente da quello erogato per altri eventuali clienti e garantendo una completa separazione di ruoli e responsabilità tra ASPI e il Fornitore. |
| **4** | Infrastruttura | I datacenter / locali fisici utilizzati dal Fornitore del servizio devono essere di proprietà del Fornitore stesso. |
| **5** | | I datacenter utilizzati dal Fornitore del servizio devono essere localizzati all'interno del territorio italiano/europeo. |
| **6** | | I datacenter / locali fisici utilizzati dal Fornitore del servizio devono prevedere adeguate misure di sicurezza, alta affidabilità, ridondanza e disaster recovery. In particolare, è richiesto il possesso della certificazione ISO 27001:2013 relativa ai datacenter /locali fisici utilizzati. |
| **7** | | I datacenter utilizzati dal Fornitore del servizio devono prevedere una connettività di rete ridondata anche tramite provider differenti a livello di connessione verso internet, oltre che connettività ridondata a livello di connettività con i Data Center di ASPI. |
| **8** | Team | Tutto il personale del Fornitore dedicato al servizio deve essere alle dirette dipendenze del Fornitore. |
| **9** | | Tutto il personale del Fornitore dedicato al servizio deve avere un livello di esperienza, competenze e formazione adeguato, in linea con il proprio ruolo nel gruppo di lavoro. |
| **10** | | Il personale del Fornitore dedicato al servizio deve possedere certificazioni specifiche sulle tecnologie / soluzioni erogate verso ASPI. |
| **11** | | Costituirà titolo preferenziale il possesso delle seguenti certificazioni da parte del personale dedicato al servizio:<br><br>- <indicare certificazioni specifiche in base al servizio> |
| **12** | | Il Fornitore deve garantire un numero adeguato di personale operativo dedicato al servizio in ogni fascia oraria. |
| **13** | Comunicazioni | Per tutte le comunicazioni deve essere utilizzata la lingua italiana / inglese. |
| **14** | | Per la gestione e registrazione delle attività eseguite dal Fornitore dovrà essere utilizzato un sistema di ticketing e di rendicontazione. |
| **15** | | Il Fornitore deve garantire un servizio di contatto telefonico attivo 24x7 utilizzabile dalle strutture ASPI competenti in caso di problemi. |
| **16** | | Il Fornitore deve garantire servizi di contatto via posta e/o instant messaging attivi 24x7 utilizzabili dalle strutture ASPI competenti in caso di problemi. |
| **17** | | Il Fornitore, nel caso di segnalazioni provenienti dalle strutture ASPI competenti deve fornire risposta attraverso lo stesso canale nel momento della chiusura della segnalazione stessa, includendo nella risposta la motivazione della chiusura ed eventualmente un report che includa tutte le informazioni utili e le azioni effettuate per la gestione dell'evento stesso. |
| **18** | Gestione e manutenzione | Il Fornitore deve provvedere a manutenere il servizio erogato verso ASPI allo stato dell'arte e a concordare con ASPI gli interventi di aggiornamento del servizio stesso, con particolare riferimento agli interventi che comportano un fermo temporaneo del servizio erogato. |
| **19** | Reportistica | Il Fornitore deve produrre periodicamente adeguata reportistica del servizio erogato verso ASPI. La periodicità di tale reportistica deve essere preventivamente concordata con le strutture competenti di ASPI. |
| **20** | | Il Fornitore deve garantire ad ASPI la possibilità di concordare template di reportistica customizzati sia a livello grafico (layout) che di informazioni rappresentate. |
| **21** | | La reportistica deve essere prodotto in formato di testo "statico" (ad es. documento pdf) |

| | | |
|---|---|---|
| **22** | | Il Fornitore deve fornire entro la data di termine del contratto il riepilogo complessivo del servizio erogato. |
| **23** | Certificazioni | Il Fornitore deve possedere certificazione ISO 27001 in corso di validità relativamente ai servizi erogati. |
| **24** | Referenze | Il Fornitore deve dimostrare precedenti esperienze nell'erogazione di servizi analoghi a quello richiesto, effettuati presso organizzazioni di medio/grande dimensione a livello nazionale e/o internazionale. |
| **25** | Audit | Il Fornitore deve garantire ad ASPI la possibilità di effettuare audit di seconda parte. Previ accordi puntuali tra ASPI e il Fornitore, dovrà essere garantita anche la possibilità di effettuare da parte di personale ASPI visite ispettive onsite presso i data center / locali del Fornitore dedicati al servizio erogato. |

----- Fine del documento -----