Public

PROTEZIONE DI BT

Standard relativo ai Controlli per le Terze Parti

Versione: 1.1

Proprietario: Mark Tilston

Il presente standard stabilisce i controlli di sicurezza di base per le Terze parti con cui collaboriamo.

Viene pubblicato e comunicato a tutte le parti applicabili, sarà di proprietà dell'"Esperto in materia" che lo revisionerà almeno una volta all'anno per assicurarsi che sia sempre in linea con i requisiti delle parti interessate e con gli obiettivi commerciali descritti nell'ISMS di BT.

Si applica a tutte le Terze part che lavorano per o per conto del Gruppo BT, compresi Openreach, EE e PlusNet.

Per semplicità, nel presente documento ci limiteremo all'uso della sigla 'BT'.

Introduzione

BT ci tiene a creare un ambiente sicuro di cui sia i clienti che i dipendenti possano fidarsi. Il nostro obiettivo è quello di proteggere tutti i nostri dati e sistemi da distruzione, danni, modifica o diffusione accidentali o dolosi. Per raggiungere l'obiettivo prefissato implementiamo idonee misure di controllo delle Terze Parti, volte a tutelare la riservatezza, l'integrità e la disponibilità dei nostri dati e sistemi.

A chi si applica?

Il presente standard si applica a tutte le Terze Parti che lavorano per per conto di BT, che entrano in contatto con le informazioni o i dati BT, i quali vengono consultati, trattati, archiviati o distribuiti dal terzo. Il presente standard potrebbe subire modifiche a cadenza periodica, previa consultazione interna.

Definizione dei termini:

Termine	Spiegazione
deve/devono	Questa espressione, o i termini 'RICHIESTO/NECESSARIO' o 'DOVRÀ', indica un requisito assoluto
non deve/non devono	Questa espressione, o l'espressione 'NON DOVRÀ', indica un divieto assoluto
può/potrebbe/possono/potrebbero	Questo termine, o l'aggettivo 'OPZIONALE', indica che l'indicazione fornita è effettivamente opzionale
dovrebbe/dovrebbero	Questo termine, o l'aggettivo 'CONSIGLIATO', indica che sussiste un valido motivo in determinate circostanze per ignorare una determinata indicazione, ma le implicazioni verranno pienamente comprese e attentamente valutate prima di scegliere un'opzione diversa.
non dovrebbe/non dovrebbero	Questa espressione, o l'espressione "NON CONSIGLIATO", indica che verrà fatto ogni ragionevole sforzo per soddisfare i requisiti di una misura di controllo, ma non sempre sarà possibile evitare l'azione descritta in tutti i casi. Nei casi in cui non sia possibile soddisfare un controllo, le implicazioni verranno valutate e pienamente comprese.

Ambito di applicazione

Il presente documento descrive ad alto livello i controlli di sicurezza minimi richiesti per gestire la sicurezza nell'ambito della catena di fornitura di BT e delle Terze parti.

Il Personale di BT potrà trovare gli standard di supporto e linee di base, documenti di processo e linee guida che descrivono come implementare controlli, i quali dovranno essere letti in combinazione con il presente standard sul sito web dedicato alla sicurezza.

Gli Stakeholder BT che desiderano esentare una Terza parte dal rispetto del presente standard devono presentare richiesta tramite il Processo esenzioni

Cosa include il presente documento?

1. Ruoli e Responsabilità.

Tutte le Terze parti devono conoscere e aver compreso i requisiti di cui al presente standard e a ciascuno spetta la responsabilità di garantire che tutti i soggetti coinvolti nella prestazione di un servizio a BT conoscano i requisiti applicabili del presente standard e li rispettino.

Spetta agli Stakeholder BT vigilare sulla conformità al presente standard e collaborare con le relative Terze parti per migliorare il livello di conformità e implementare misure di mitigazione qualora vengano individuate delle lacune.

Spetta ai Manager BT assicurarsi che tutti i loro collaboratori conoscano i requisiti di cui al presente standard e li rispettino, unitamente alle politiche e agli standard associati.

2. Governance.

2.1. La Terza parte deve disporre di un quadro di sicurezza standard di settore, coerente e consolidato, in tema di governance della sicurezza informatica e delle informazioni, comprensivo di quanto indicato di seguito:

- Politiche e procedure appropriate sulla sicurezza delle informazioni e sicurezza informatica, approvate e comunicate
- Una strategia in tema di sicurezza delle informazioni
- Requisiti giuridici e normativi pertinenti, in relazione alla sicurezza delle informazioni e sicurezza informatica (privacy inclusa), condivisi e organizzati
- Processi per la governance e gestione dei rischi che indirizzano rischi di sicurezza dell'informazione e sicurezza informatica

2.2. La Terza parte deve assicurarsi che vengano definiti ruoli e responsabilità idonei in relazione alla sicurezza informatica e delle informazioni e che questi vengano implementati. Deve essere compreso quanto segue:

- Un Responsabile capo della sicurezza delle informazioni (Chief Information Security Officer) a tempo pieno (o figura equivalente) che abbia un'anzianità sufficiente e sia responsabile del programma di sicurezza delle informazioni
- Un gruppo di lavoro di alto livello, un comitato o un organo equivalente che coordini le attività di sicurezza delle informazioni presso la Terza parte, opportunamente presieduto da un membro senior dello staff e che si riunisca regolarmente
- Una figura specializzata in sicurezza delle informazioni con ruoli e responsabilità adatti e ben definiti

2.3. La Terza parte deve garantire la responsabilità individuale in merito alle informazioni e ai sistemi assicurandosi che la proprietà di ambienti, informazioni e sistemi aziendali critici sia affidata a soggetti idonei e competenti

2.4. La Terza parte deve assicurarsi che BT verrà informata (per iscritto), nel più breve tempo possibile e nel rispetto della legge, in caso dovesse essere oggetto di un'operazione di fusione, acquisizione o di qualsivoglia altro cambio di proprietà

3. Gestione degli Incidenti.

3.1. La Terza parte deve disporre di un quadro coerente e consolidato per la gestione degli incidenti, a garanzia che tali eventi vengano gestiti, contenuti e mitigati in maniera adeguata, e che copra i seguenti aspetti:

- Garantire che ogni membro del personale conosca il proprio ruolo e la procedura da implementare in caso sia richiesta una risposta
- Garantire che gli incidenti vengano comunicati nel rispetto di criteri coerenti e prestabiliti
- Garantire che l'impatto dell'incidente risulti chiaro
- Garantire che, in caso di necessità, verranno svolte adeguate indagini, internamente o ad opera di uno specialista in scienza forense
- Garantire che tutte le lezioni apprese dagli incidenti verificatisi vengano incorporate in una *best practice*.
- Garantire che le informazioni correlate a un incidente che coinvolge BT vengano trattate come "Riservate".

3.2. La Terza parte adotterà tutte le misure ragionevoli per garantire che uno o più soggetti idonei vengano nominati responsabili e fungano da Punto di contatto per il rischio per la sicurezza, la gestione degli incidenti e la gestione della conformità. La Terza parte dovrà comunicare allo Stakeholder BT i dettagli di contatto del/dei soggetto/i e qualsiasi eventuale relativa modifica. Tali dettagli devono comprendere: -
Nome, responsabilità, ruolo e indirizzo e-mail di gruppo e/o numero di telefono

3.3. La Terza parte informerà lo Stakeholder BT, entro tempi ragionevoli dal momento in cui sarà venuta a conoscenza di un eventuale incidente che ha un impatto sul servizio da rendere a BT o sulle Informazioni BT, e in qualsiasi caso entro e non oltre (12) ore dal momento in cui l'Incidente verrà portato all'attenzione della Terza parte.

3.4. Senza ritardi immotivati, la Terza parte prenderà misure correttive appropriate e tempestive per mitigare eventuali rischi e gli effetti collegati all'incidente al fine di ridurre la gravità e la durata di tale evento.

3.5. La Terza parte redigerà un rapporto per lo Stakeholder BT in relazione a qualsivoglia incidente che possa avere un impatto sul servizio da rendere a BT o sulle Informazioni BT. Detto rapporto dovrebbe comprendere almeno i seguenti dati:

- data e ora
- luogo
- tipo di incidente
- impatto
- classificazione delle informazioni colpite (Cfr. Standard relativo alla Classificazione dell'Informazione e Trattamento dei Dati per le terze parti)
- stato
- esito (incluse le raccomandazioni di risoluzione o le misure prese).

3.6. Qualora venga utilizzata una quarta parte per la prestazione del servizio, e detta parte abbia accesso o elabori le Informazioni BT, la Terza parte deve concordare con lo Stakeholder BT quali informazioni potranno essere condivise. La Terza parte deve garantire di avere un rapporto contrattuale con la quarta parte e deve altresì assicurarsi che detta quarta parte disponga di un quadro per la sicurezza standard di settore.

4. Gestione delle Modifiche.

4.1. La Terza parte deve assicurarsi che tutte le modifiche IT vengano approvate, registrate e testate, incluso il ritiro di modifiche non andate a buon fine, prima dell'implementazione al fine di impedire

l'interruzione del servizio o violazioni alla sicurezza. Deve altresì assicurarsi che esista una procedura per implementare aggiornamenti di emergenza in modo controllato.

4.2. La Terza parte deve garantire che le modifiche vengano riportate anche negli ambienti di Produzione e DR.

4.3. La Terza parte deve informare immediatamente BT di tutte le modifiche sostanziali apportate al servizio quali, a titolo esemplificativo ma non esaustivo, modifiche al suo metodo di accesso tramite i firewall, compresa la fornitura della conversione degli indirizzi di rete.

4.4. La Terza parte deve garantire che le risorse organizzative verranno sottoposte a manutenzione e riparazione mediante l'uso di strumenti registrati, approvati e controllati.

4.5. La Terza parte deve assicurarsi che la manutenzione in remoto delle risorse organizzative venga approvata, registrata ed eseguita in modo tale da prevenire accessi non autorizzati.

5. Gestione delle Minacce e dei Rischi informatici

5.1. La Terza parte deve assicurarsi che esista un quadro di valutazione delle minacce e dei rischi alla sicurezza informatica sempre aggiornato volto a garantire che il profilo di rischio alla sicurezza informatica delle operazioni, risorse, sedi e risorse umane dell'organizzazione risulti compreso e ben gestito. Per raggiungere questo obiettivo dovrà:

- Valutare le vulnerabilità delle risorse
- Individuare le minacce sia interne che esterne
- Valutare la sensibilità delle informazioni e dei dati in oggetto
- Valutare il potenziale impatto sulle attività dell'azienda
- Le minacce, le vulnerabilità, le probabilità e l'impatto vengono utilizzati per determinare il rischio?
- Garantire che il quadro di gestione delle minacce e dei rischi informatici sia accettato e condiviso a un livello adeguato nell'organizzazione.

5.2. La Terza parte deve garantire che a tutti i rischi e alle minacce identificati in fase di valutazione delle minacce e dei rischi alla sicurezza informatica venga data la giusta priorità e che vengano prese le dovute misure per mitigare tali rischi entro tempi ragionevoli.

5.3. La Terza parte dovrà informare lo Stakeholder BT qualora non fosse in grado di rimediare a o ridurre eventuali aree sostanziali di rischio che potrebbero avere un impatto sul servizio reso.

6. Gestione delle Identità e Controllo degli Accessi

6.1 La Terza parte deve implementare un quadro coerente e consolidato per la gestione sicura delle identità e delle credenziali da parte di personale autorizzato:

- Concedendo, riabilitando, modificando e disabilitando i diritti di accesso esclusivamente in base ad autorizzazioni documentate e approvate.
- Garantendo che gli account inattivi vengano disabilitati.
- Disabilitando gli account dei membri del personale che non sono più dipendenti dell'azienda.
- Tramite analisi periodiche degli accessi che garantiscano che ogni accesso sia idoneo allo scopo.
- Rinnovo della certificazione per l'accesso degli account utente almeno su base annuale e degli account con privilegi almeno ogni trimestre.

6.2 La Terza parte deve garantire che l'accesso remoto venga gestito in modo che solo i soggetti autorizzati possano connettersi in remoto ai sistemi della Terza parte e che le connessioni siano

protette e non consentano la fuga di dati. Dovrà altresì garantire l'applicazione di un sistema di controllo degli accessi adeguato, come l'autenticazione a più fattori.

L'autenticazione a due fattori dovrebbe essere ottenuta usando un ID utente, una password e uno dei seguenti metodi:

- Un generatore di password monouso(One-time password generator), che richiede un codice PIN/password specifico dell'utente per visualizzare la password monouso.
- Una smart card con chip conforme alla norma ISO 7816 e un software e lettore di schede associato. Le smart card contactless non sono consentite.
- Autenticazione basata su certificato emesso nel rispetto della propria politica sui certificati Infosec.

Per fugare ogni dubbio, se l'accesso con privilegi a scopo di assistenza viene fornito tramite accesso in remoto, ciò dovrà avvenire mediante connessione protetta e autenticazione a due fattori.

6.3 La Terza parte deve assicurarsi che i permessi e le autorizzazioni di accesso per tutti i sistemi (compresi gli strumenti, le applicazioni, i database, i sistemi operativi, gli hardware, ecc.) vengano gestiti integrando i principi dei privilegi minimi e della separazione dei compiti.

6.4 La Terza parte deve assicurarsi che ogni transazione possa essere ricollegata esclusivamente a un unico soggetto identificabile e, in caso di credenziali condivise, che siano stati implementati adeguati controlli di compensazione (incluse le procedure per gli accessi in caso di emergenza).

6.5 La Terza parte deve assicurarsi che tutte le autenticazioni vengano gestite in modo proporzionale al rischio della transazione, ovvero utilizzando password di lunghezza e complessità adeguata, modificando le password a intervalli regolari, usando l'autenticazione a più fattori, tramite una gestione sicura delle credenziali di accesso e mediante altre misure di controllo.

6.6 Devono altresì essere implementate delle misure di controllo adeguate per la gestione delle autenticazioni non andate a buon fine, comprese le notifiche a schermo, login negati e blocco di utenti.

6.7 Devono essere implementati processi e misure di controllo per la gestione e l'autorizzazione di account guest e usati per l'assistenza.

7. Gestione degli Asset informativi

7.1. La Terza parte deve disporre di un inventario degli asset informativi (che, ove applicabile, dovrebbe includere tutte le apparecchiature di BT ospitate presso sedi di terzi) e garantire l'esecuzione di un test almeno una volta all'anno per verificare che detto inventario sia aggiornato, completo e accurato.

7.2. La Terza parte deve garantire che nell'inventario degli asset informativi venga catalogato quanto segue:

- Dispositivi e sistemi fisici, applicazioni e piattaforme software, sistemi informatici esterni
- Alle risorse (ad esempio, hardware, dispositivi, dati, tempo e software) deve essere assegnato un diverso livello di priorità in base alla relativa classificazione, criticità e al valore commerciale
- Flussi di dati relativi all'organizzazione e alla comunicazione, inclusi i flussi di terzi/esterni
- Processi manuali nell'ambito dei quali vengono gestiti dati BT o relativi ai Clienti BT.

8. Accesso ai Sistemi BT

8.1 La Terza parte dovrà operare nel rispetto di tutte le istruzioni rilevanti che le verranno fornite relativamente all'accesso ai Sistemi BT e al relativo utilizzo.

8.2 La Terza parte è tenuta a comunicare a BT, entro e non oltre 24 ore, quando un soggetto facente parte della sua organizzazione non avrà più necessità di accedere alle risorse.

8.3 La Terza parte dovrà garantire che l'identificazione degli utenti, le password, i PIN, i token e l'accesso alle conferenze siano collegati ai singoli membri del relativo personale e che non vengano condivisi. I dettagli devono essere conservati in modo sicuro e separato dal dispositivo utilizzato per accedere. Se un'altra persona viene a conoscenza di una password non sua, tale password deve essere modificata immediatamente.

Connettività tra sistemi

8.4 Il collegamento tra domini ai Sistemi BT non è ammesso se non specificatamente approvato e autorizzato da BT.

8.5 La Terza parte deve compiere ogni ragionevole sforzo per garantire che nei Sistemi BT non vengano introdotti virus o malware (secondo il significato generalmente attribuito a tali espressioni nel settore informatico).

8.6 In caso di connettività tra i sistemi di BT e della Terza parte, tale connettività dovrà avvenire per mezzo di collegamenti sicuri in cui i dati saranno protetti mediante crittografia, secondo quanto specificato nella **Sezione 11 Crittografia**.

8.7 La Terza parte deve garantire che i sistemi e le infrastrutture utilizzati siano contenuti in una rete logica dedicata. Tale rete deve essere costituita unicamente dai sistemi dedicati alla fornitura di una struttura di trattamento dati sicura.

9. Sicurezza fisica presso le Sedi di Terzi

9.1 La Terza parte deve disporre di un processo di accesso fisico che copra le autorizzazioni e i metodi di accesso alle sedi della Terza parte stessa (siti, edifici e aree interne) in cui vengono prestati i servizi, o in cui sono conservate e trattate le Informazioni BT. Il metodo di accesso dovrebbe comprendere uno o più dei seguenti elementi:

- Una tessera identificativa della Terza parte autorizzata, munita di foto chiaramente visibile e riconducibile al suo proprietario.
- Una tessera elettronica di accesso autorizzato per accedere alle zone applicabili della sede in oggetto.
- Un accesso di sicurezza tramite tastierino, dotato delle seguenti funzioni: autorizzazione, diffusione dei cambi di codice (il che deve verificarsi almeno una volta al mese), cambi di codice ad hoc.
- Riconoscimento biometrico

9.2 La Terza parte deve disporre di processi e procedure per il controllo e il monitoraggio di visitatori e altri soggetti esterni, inclusi i Terzi che possono accedere fisicamente ad aree protette o a scopo di controllo ambientale, manutenzione degli allarmi e addetti alle pulizie.

9.3 Le aree protette presso le sedi delle Terze parti utilizzate per la prestazione del servizio (ad esempio, locali per le comunicazioni di rete) dovranno essere separate dalle aree ad accesso generale e protette mediante appropriati sistemi di controllo degli ingressi a garanzia che solo il personale autorizzato potrà accedere. L'accesso a tali aree deve essere verificato regolarmente e, almeno una volta all'anno, deve essere svolta una valutazione per confermare o meno i diritti di accesso a tali aree.

9.4 La Terza parte dovrà disporre di sistemi di sicurezza TVCC nei luoghi in cui le Informazioni BT vengono conservate e gestite.

9.5 Le registrazioni del sistema TVCC devono essere conservate per un minimo di 20 giorni. Tuttavia, tale periodo può essere prolungato nelle seguenti situazioni:

- Se le prove video del sistema TVCC devono essere conservate per un'indagine penale o relativa a un incidente; o
- Se specificato quale requisito obbligatorio nel rispetto della legge.

9.6 Tutte le registrazioni del sistema TVCC e i registratori devono essere sistemati in un luogo sicuro per evitare che vengano modificati o cancellati o che gli schermi del sistema TVCC possano essere "casualmente" visti. L'accesso alle registrazioni deve essere controllato e limitato solo ai soggetti autorizzati.

9.7 La Terza parte deve aver implementato appropriate misure per garantire la sicurezza fisica, rispetto a quanto segue:

- Misure di prevenzione antincendio tra cui, a titolo esemplificativo ma non esaustivo, allarmi e attrezzature di rilevazione ed estinzione.
- Condizioni climatiche, tenendo in considerazione aspetti quali temperatura, umidità ed elettricità statica, gestione, monitoraggio e risposta a condizioni estreme (come lo spegnimento automatico o gli allarmi).
- Attrezzature di controllo tra cui, a titolo esemplificativo ma non esaustivo, climatizzazione e rilevamento acqua.
- Prevenzione di danni dovuti all'acqua, posizionamento dei serbatoi dell'acqua, delle tubature, ecc. presso la sede.

9.8 La Terza parte deve assicurarsi che l'accesso fisico alle aree in cui si trovano le Informazioni BT venga effettuato con smart card o carte di prossimità (o sistemi di sicurezza equivalenti o migliori), oltre a effettuare dei controlli almeno una volta al mese per garantire che questo tipo di accesso sia consentito solo a soggetti autorizzati.

9.9 La Terza parte deve garantire che sia vietato fotografare e/o acquisire immagini di qualsivoglia Informazione BT. Qualora l'acquisizione delle immagini sia richiesta per motivi di lavoro, sarà necessario ottenere prima l'autorizzazione scritta dello Stakeholder BT.

Fornitura di un ambiente per la custodia (hosting environment) delle apparecchiature BT.

9.10 Qualora fornisca un'area ad accesso sicuro presso la sua sede per la custodia (hosting) delle apparecchiature BT o dei Clienti BT, la Terza parte deve:

- Fornire a BT una planimetria degli spazi assegnati nell'area sicura della sede.

- Garantire che gli armadietti di BT e dei clienti di BT presso la sede rimangano sempre chiusi e vi possa accedere solo il personale BT autorizzato, i rappresentanti approvati da BT e il personale del Terzo pertinente.
- Mettere in atto una procedura di gestione delle chiavi sicura.

9.11 BT dovrà fornire alla Terza parte quanto segue:

- Un documento riportante le risorse fisiche di BT e/o dei clienti di BT conservate presso la sede del Terzo.
- I dettagli relativi ai dipendenti di BT, ai subappaltatori e agli agenti che hanno necessità di accedere alla sede del Terzo (su base continuativa).

10.Classificazione e Protezione dei Dati.

10.1 La Terza parte deve implementare uno schema/quadro per la gestione e la classificazione delle informazioni coerente e consolidato (in linea con le *best practice* del settore / i requisiti BT) comprensivo dei seguenti elementi:

- Linee guida per la gestione delle informazioni
- Le informazioni devono essere protette in linea con il livello di classificazione assegnato
- Garanzia che tutto lo staff sappia che le Informazioni BT non dovranno essere utilizzate per scopi diversi da quelli per cui sono state fornite.
- Le informazioni di BT dovrebbero essere gestite nel rispetto dello Standard relativo alla Classificazione dell'Informazione e Trattamento dei Dati per le terze parti.

11. Crittografia.

11.1 La Terza parte deve garantire che, se il livello di rischio richiede la crittografia, i dati verranno opportunamente crittografati (sia quelli in transito che quelli inattivi) e che le eventuali chiavi di crittografia utilizzate siano progettate e implementate in modo da soddisfare i requisiti di sicurezza specificati al livello 2 o superiore dello Standard FIPS 140-2 di NIST.

11.2 Le chiavi crittografiche devono avere una lunghezza pari o superiore a quella indicata di seguito:

- Le chiavi simmetriche (ad es. AES) devono essere lunghe almeno 256 bit.
- Le chiavi asimmetriche (ad es. RSA) devono essere lunghe almeno 2048 bit.
- Le chiavi a curva ellittica devono essere lunghe almeno 224 bit.

11.3 Qualora il NIST dovesse annunciare che un certo algoritmo di crittografia non è più sicuro, questo non dovrà essere utilizzato per le nuove versioni. Le versioni esistenti che fanno uso di algoritmi di crittografia obsoleti devono essere sottoposte a revisione continua e per queste deve essere previsto un piano di migrazione per passare ad algoritmi più sicuri.

11.4 Per la crittografia simmetrica è possibile utilizzare i seguenti algoritmi: 3DES-168 (se non stabilito da uno standard internazionale), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed e ARIA.

11.5 Utilizzare hash sottoposti a salting per proteggere i dati archiviati, ovvero le password. L'hashing può essere utilizzato anche per anonimizzare i dati prima che vengano trattati, ad esempio gli MSISDN o i dati relativi ai pagamenti. I seguenti algoritmi di hashing non sono consentiti: MD2, MD4, MD5 e SHA-1.

11.6 Gestione delle chiavi - Creazione e uso

- Le chiavi di sessione e i nonce devono essere create servendosi di un generatore di numeri pseudo-casuali. Questa operazione deve essere definita usando almeno un numero di bit di entropia o l'imprevedibilità di un messaggio uguale al numero di bit effettivi di sicurezza forniti dall'algoritmo che userà la chiave.
- È vietato usare una chiave più corta di 64 bit combinandola in modo non crittografico con la stessa chiave di 64 bit per ottenere 128 bit.
- Tutti i bit della chiave devono essere utilizzati dall'algoritmo
- La spaziatura interna o altri bit utilizzati dall'algoritmo non dovranno essere presi in considerazione per il calcolo della lunghezza della chiave

11.7 Gestione delle chiavi - Casualità

- Utilizzare una fonte solida di dati casuali per produrre chiavi di sessione da usare nelle parti simmetriche della crittografia ibrida, oppure per produrre sali o vettori di inizializzazione.
- È possibile utilizzare dei generatori di numeri pseudo-casuali (PRNG), ma per essere considerato sicuro, un PRNG non deve permettere ai malintenzionati di:
  - Riuscire a indovinare il risultato successivo del generatore, conoscendo quello precedente
  - Calcolare gli stati precedenti del generatore, conoscendone quello corrente
  - Distinguere il risultato del PRNG dalla vera casualità. (Non è consentito l'uso della funzione rand()).

11.8 Gestione delle chiavi - Scambio chiavi

- Le chiavi di sessione che vengono generate per l'uso con un algoritmo simmetrico devono essere scambiate servendosi di un protocollo di scambio chiavi sicuro

11.9 Gestione delle chiavi - Archiviazione chiavi

- Nei casi in cui vengono usate delle chiavi per proteggere i dati inattivi, la chiave di crittografia dati (DEK) deve essere protetta da una chiave di crittografia chiave (KEK) che deve essere conservata su un server separato oppure in un Trusted Platform Module (TPM).
- Se la KEK viene conservata su un server separato, deve essere protetta nella fase di transito verso il server in cui sono ospitati i dati.

11.10 Gestione delle chiavi - Rotazione delle chiavi (rigenerazione)

- Al termine della sua vita utile, una chiave deve poter essere rigenerata nel rispetto delle *best practice* del settore.
- I dati da proteggere con la chiave rigenerata devono poter essere ri-crittografati.
- Deve essere possibile eseguire una rigenerazione ad-hoc della chiave e una nuova crittografia dei dati qualora si sospetti che la chiave di crittografia originale sia stata compromessa.
- Per AES GCM, la probabilità che la funzione di crittografia autenticata venga invocata con lo stesso IV e la stessa chiave su due (o più) set distinti di dati di input non dovrà essere maggiore di 232

11.11 Gestione delle chiavi - Moduli di sicurezza hardware (HSM)

- Le chiavi di crittografia devono essere caricate su un HSM usando delle smart card.
- Le smart card devono richiedere un PIN per consentire l'accesso.
- I PIN devono essere scelti in base a quanto indicato nella politica di controllo degli accessi.
- I PIN e le smart card devono essere conservati in un luogo sicuro supervisionato dal team Infosec.
- L'estrazione delle chiavi crittografiche da un HSM non deve essere consentita.

- Gli HSM devono distruggere le chiavi crittografiche in essi contenute qualora venga fatto un tentativo di accedervi.
- Per gli HSM che contengono chiavi molto sensibili, i PIN e le smart card utilizzati per proteggerli devono essere configurati e conservati solo dai membri dello staff addetto alla sicurezza tecnologica.
- Se l'HSM verrà utilizzato per proteggere dati molto sensibili, per potervi apportare delle modifiche dovrà essere richiesto un quorum minimo di 2 smart card e i PIN associati. I membri del quorum devono essere esaminati a livello di *enhanced screening*.

11.12 Certificati digitali

- Per i certificati deve essere impostato l'attributo Punto di distribuzione elenco revoche di certificati (CDP).
- Per determinare lo stato di un certificato, si deve usare l'Online Certificate Status Protocol (OCSP) o il Certificate Revocation List (CRL).
- I proprietari dei certificati devono monitorare la validità e la scadenza dei loro certificati a garanzia che non si verifichino errori ai sistemi dovuti a una scadenza prevista.
- Coloro che usufruiscono dei certificati (client) devono monitorare la validità e la scadenza dei certificati utilizzati a garanzia che non si verifichino errori ai sistemi dovuti a una scadenza prevista.
- Selezionare una durata dei certificati appropriata allo scopo.
- La durata del certificato deve essere stabilita prima dell'emissione.
- Non è consentito usare un'identità standard (client, server) 1024

11.13 Dati in transito

- In genere i dati in transito vengono crittografati usando la crittografia di tipo Transport o Payload (Message o Selective Field). I meccanismi di crittografia di tipo Transport includono, a titolo esemplificativo ma non esaustivo:
- Transport Layer Security (TLS)
- Tunnelling sicuro (IPSec)
- Secure Shell (SSH)
- Per questo tipo di crittografia, la componente simmetrica deve essere conforme alla sezione 12.14 del presente standard.
- I Transport Security Protocol devono essere configurati in modo da evitare la negoziazione di algoritmi più deboli e/o chiavi più corte, quando entrambi gli end point supportano un'opzione più forte.
- L'uso del protocollo SSL non è consentito in quanto esistono svariate vulnerabilità note che lo riguardano.
- I vettori di inizializzazione dei cifrari a flusso e AES in modalità CBC non devono essere prevedibili.
- Il nonce/IV in AES GCM deve soddisfare il seguente requisito di "unicità":
  - Il rispetto del seguente requisito è fondamentale per garantire la sicurezza di GCM
  - Configurare i Transport Security Protocol (ad esempio usando bit di direzione) per impedire attacchi con testo in chiaro noti da messaggi noti restituiti, ad esempio "nulla da dichiarare".
  - Eseguire la verifica di identità reciproca durante la configurazione del trasporto.
  - Per i dati brevi sensibili che richiedono la crittografia di tipo Payload (chiavi di crittografia, password, informazioni sulle carte di pagamento), usare la crittografia asimmetrica con chiavi e algoritmi delle lunghezze minime indicate nel presente documento.
  - I dati di gestione dei sistemi devono essere crittografati durante la fase di transito.
  - Le seguenti opzioni TLS non sono consentite: TLS v1.0, TLS v1.2, v6.0, TLS v6.1 e SSL (tutte le versioni)

- Le seguenti opzioni SSH (SFTP) non sono consentite: SSH v1
- Le seguenti opzioni IPSec non sono consentite: IKE Versione 1

11.14 Dati inattivi

- I dati inattivi includono i dati salvati in file, database, posizioni temporanee o di swap e su qualsiasi dispositivo inclusi, a titolo esemplificativo ma non esaustivo, PC, laptop e altri dispositivi portatili, server, nastri, SAN, USB, CD, DVD, floppy disk e altri soluzioni amovibili per l'archiviazione.
- I dati definiti riservati o di classe superiore salvati nella memoria non volatile di un dispositivo devono essere crittografati.
- Le informazioni sulle carte di pagamento salvate nella memoria non volatile di un dispositivo devono essere crittografate.
- Se i dati delle chiavi simmetriche vengono conservati protetti da una chiave asimmetrica, la chiave asimmetrica deve avere la stessa forza, misurata in bit di sicurezza, della chiave simmetrica.
- Nella documentazione dei sistemi devono essere indicati la classificazione dei dati e i volumi salvati nel sistema.
- Le chiavi usate per decrittografare non devono essere salvate, compreso il relativo backup, con i dati che decifrano. Prima della distribuzione sui sistemi di produzione, i software devono essere completamente testati.

12. Prevenzione della fuga di dati.

12.1 La Terza parte deve disporre di un quadro coerente e consolidato per garantire la protezione dei dati da fughe accidentali assicurandosi che detta protezione includa (senza limitarsi a) i seguenti vettori:

- E-mail
- Internet / Web Gateway (inclusa l'archiviazione online e la webmail)
- Porte USB, ottiche e altre tipologie / sistemi di archiviazione portatili, ecc.
- Mobile Computing e BYOD
- Servizi di accesso remoto
- Meccanismi di condivisione file e social media

NB: I dispositivi portatili / supporti amovibili dovrebbero essere disabilitati per impostazione predefinita e abilitati esclusivamente per motivi aziendali legittimi. Tutti i dati archiviati sui dispositivi portatili o sui supporti amovibili devono essere crittografati in misura proporzionale al rischio. I dispositivi non autorizzati devono essere disconnessi dalla rete (dalla rete aziendale del vendor o dai sistemi/rete di BT) oppure utilizzati per accedere a informazioni non pubbliche. Per maggiori informazioni sulla gestione dei supporti amovibili, consultare lo Standard relativo alla Classificazione dell'Informazione e Trattamento dei Dati per le terze parti.

13. PCI DSS

13.1 La Terza parte deve garantire che, qualora fosse coinvolta nella gestione di dati relativi alle carte di pagamento, opererà secondo quanto indicato nel PCI-DSS.

14.Cloud / Online Computing.

14.1. La Terza parte deve essere certificata conforme all'ultima versione della norma ISO27017 oppure deve disporre di un quadro coerente e consolidato per garantire che tutti gli usi della tecnologia Cloud e i dati non pubblici archiviati nel Cloud siano approvati e sottoposti ad adeguati controlli equivalenti all'ultima versione del Cloud Controls Matrix (CCM) della Cloud Security Alliance.

14.2. Nei *Service Level Agreement* di rete e infrastruttura (in-house o in outsourcing) dovranno essere chiaramente documentati i controlli di sicurezza, i livelli di capacità e servizio e i requisiti dell'azienda o del cliente

14.3. La Terza parte deve implementare delle misure di sicurezza su tutti gli aspetti del servizio prestato, per tutelare la riservatezza, disponibilità, qualità e integrità riducendo al minimo la possibilità di accesso da parte di soggetti non autorizzati (ad es., altri clienti nel Cloud) alle Informazioni BT e ai servizi utilizzati da BT.

15. Social Media

15.1. La Terza parte deve disporre di un quadro coerente e consolidato relativo all'uso accettabile di social media personali e aziendali. Detto quadro deve comprendere i seguenti aspetti:

- Garanzia che il personale non pubblichi nulla di diffamatorio, osceno o offensivo nei confronti dell'azienda e dei suoi clienti
- Uso dei loghi aziendali o dei clienti senza autorizzazione
- Esposizione di informazioni non pubbliche relative all'azienda o ai clienti senza consenso
- Pubblicazione di opinioni relative all'azienda e ai suoi clienti che potrebbero ragionevolmente essere interpretate come commenti ufficiali dell'azienda o dei suoi clienti
- Divieto di diffondere qualsivoglia Informazione BT contrassegnata come "Riservata" o "Strettamente riservata".

16.Configurazione dei Sistemi.

16.1. La Terza parte deve disporre di un quadro coerente e consolidato a garanzia che i sistemi siano adeguatamente configurati (sia quelli di Terzi che quelli forniti a BT) che comprenda i seguenti aspetti:

- I sistemi e i dispositivi di rete sono configurati in modo da funzionare secondo i principi di sicurezza (ad esempio, principio di minima funzionalità e di assenza di software non autorizzati)
- Garanzia che tutti i dispositivi siano settati sullo stesso orario corretto
- I sistemi devono essere privi di software dannosi
- Le build e i dispositivi vengono sottoposti a un controllo e monitoraggio appropriato per garantirne l'integrità

17. Sviluppo software sicuro.

17.1. La Terza parte deve garantire che gli ambienti produttivi e non vengano adeguatamente controllati, assicurandosi che vengano prese le seguenti misure:

- Segregazione degli ambienti dedicati ala produzione e non con separazione dei compiti
- Nessun dato attivo deve essere utilizzato nell'ambito di test a meno che il titolare dei dati non abbia espresso il suo consenso e previa implementazione di controlli adeguati all'ambiente di produzione
- Separazione dei compiti tra produzione e non produzione

17.2. La Terza parte deve disporre di un quadro coerente e consolidato relativo allo Sviluppo dei sistemi per evitare vulnerabilità alla sicurezza e violazioni alla sicurezza informatica, comprensivo dei seguenti aspetti:

- I sistemi devono essere sviluppati in linea con le *best practice* di sviluppo sicuro (ad esempio, OWASP).
- Il codice deve essere archiviato in modo sicuro e soggetto ad attività di garanzia della qualità.
- Il codice deve essere adeguatamente protetto da modifiche non autorizzate una volta terminate le procedure di prova e mandato in produzione

17.3. Qualora sia necessario un *Escrow* (garanzia) per tutelare tutte le parti, i beni della prima e della terza parte (ovvero per la proprietà intellettuale / il codice sorgente, ecc.), la Terza parte deve disporre di un quadro coerente e consolidato comprensivo dei seguenti aspetti:

- Stipulazione di un *Escrow agreement* con un *Escrow agent* che goda di buona reputazione, abbia una posizione neutrale e sia indipendente
- Condivisione continua di aggiornamenti del codice sorgente con l'*Escrow agent* a garanzia che le informazioni necessarie siano sempre aggiornate
- Archiviazione sicura del codice sorgente e di altri materiali fino a che non vengono soddisfatte le condizioni di rilascio
- Condizioni di rilascio adeguate
- Aggiornamenti continui, pagamenti adeguati e revisioni dell'*Escrow agreement*.

18. Protezione anti-malware.

18.1. La Terza parte deve garantire l'applicazione della protezione anti-malaware più aggiornata possibile a tutte le risorse IT pertinenti al fine di evitare l'interruzione dei servizi o violazioni alla sicurezza, oltre a garantire l'attivazione di attività di sensibilizzazione degli utenti appropriate.

NB: L'anti-malware deve includere, a titolo esemplificativo e non esaustivo, il rilevamento di codice mobile non autorizzato, virus, spyware, software di registrazione delle chiavi, botnet, worm, trojan, ecc.

19. Gestione delle Vulnerabilità.

19.1. La Terza parte deve disporre di un quadro coerente e consolidato per la gestione delle vulnerabilità comprensivo dei seguenti aspetti:

- Politiche e procedure di processo
- Ruoli e responsabilità definiti
- Strumenti idonei come quelli per il rilevamento delle intrusioni e di scansione delle vulnerabilità.

19.2. Il quadro di gestione delle vulnerabilità della Terza Parte deve garantire il monitoraggio regolare di

quanto segue, per rilevare potenziali attacchi alla sicurezza informatica

- Sistemi e risorse chiave
- Connessioni non autorizzate
- Software / applicazioni non autorizzati
- Attività in rete.

19.3. Il quadro di gestione delle vulnerabilità della Terza Parte deve garantire che:

- Siano stati stabiliti dei processi per ricevere, analizzare e rispondere alle vulnerabilità dell'organizzazione, derivanti da fonti interne ed esterne (ad esempio, test interni, bollettini sulla sicurezza o ricercatori sulla sicurezza)
- Devono essere consentiti solo strumenti, tecnologie e utenti autorizzati
- Le vulnerabilità individuate vengono mitigate o documentate come rischi accettati.

19.4. La Terza parte deve garantire che vengano applicati i patch di sicurezza più recenti a sistemi / risorse / reti / applicazioni in modo tempestivo a garanzia che:

- La Terza parte utilizzi i patch ottenuti direttamente dai vendor per i sistemi proprietari e patch che siano (i) digitalmente firmati o (ii) verificati tramite l'uso di un hash del vendor (gli hash MD5 non possono essere usati) per il pacchetto di aggiornamento in modo tale che il patch possa essere identificato come proveniente da una community di supporto rispettabile per i software open source.
- La Terza parte testi tutti i patch su dei sistemi che rappresentino in modo accurato la configurazione dei sistemi di produzione target prima della distribuzione del patch sui sistemi di produzione e che il funzionamento del servizio con patch venga verificato a seguito di tutte le attività di patching.
- Monitoraggio di tutti i vendor applicabili e di altre fonti di informazioni rilevanti per indicazioni di allerta legate alle vulnerabilità.
- Qualora sia impossibile applicare un patch a un sistema, sarà necessario prendere le contromisure necessarie.

19.5. La Terza parte deve garantire che, almeno a cadenza annuale, verrà richiesta l'esecuzione di una valutazione della sicurezza IT o un *penetration test* sulle applicazioni e le infrastrutture IT del Terzo usate per prestare i servizi, compresi i siti di Disaster Recovery, per identificare le vulnerabilità che potrebbero essere sfruttate per violare i dati/servizi e per impedire che la sicurezza venga violata mediante attacchi informatici. Su ragionevole richiesta, la Terza parte deve consentire a BT di accedere ai report dei *penetration test* relativi ai servizi prestati.

19.6. La Terza parte deve garantire che l'accesso alle porte di gestione e diagnostica, oltre che agli strumenti di diagnostica, sia controllato in modo sicuro.

19.7. La Terza parte deve garantire che l'accesso agli strumenti di audit sia limitato al personale del relativo fornitore e che l'uso di tali strumenti sia monitorato.

19.8. La Terza parte deve garantire che i server utilizzati per prestare il sevizio non vengano distribuiti su reti non affidabili (la rete non è compresa nel proprio perimetro di sicurezza, è al di là del controllo amministrativo, ad es. interazione con Internet) senza adeguati controlli di sicurezza.

20.Integrità di Rete.

20.1. La Terza parte deve garantire che l'integrità di rete venga stabilita e mantenuta assicurandosi che i seguenti elementi siano opportunamente controllati:

- Le connessioni esterne alla rete sono documentate, passano attraverso un firewall e sono verificate e approvate prima di essere stabilite al fine di evitare violazioni alla sicurezza dei

dati.

- La rete è progettata in modo opportuno sul principio di “defense in depth” per ridurre al minimo le violazioni alla sicurezza informatica mediante l’implementazione di appropriati controlli volti a prevenire eventuali attacchi intenzionali, come la “segmentazione di rete”.
- La progettazione e l’implementazione della rete vengono revisionate almeno una volta all’anno.
- Tutti gli accessi in modalità wireless alla rete sono soggetti a protocolli di autorizzazione, autenticazione, segmentazione e crittografia per prevenire violazioni alla sicurezza.
- Uso di comunicazioni sicure tra dispositivi e stazioni di gestione;
- Uso di comunicazioni sicure tra dispositivi come appropriato, compresa la crittografia di tutti gli accessi di amministratore non tramite console;
- Uso di una potente architettura, suddivisa in livelli e zone e dotata di un’efficace sistema di gestione delle identità e di una configurazione del sistema operativo che deve essere adeguatamente protetta e documentata;
- Mediante la disattivazione (ove applicabile) dei servizi, delle applicazioni e delle porte che non verranno utilizzati.
- Mediante la disattivazione o la rimozione degli account guest.
- Non autorizzando relazioni di trust tra i server;
- Uso del principio di sicurezza dei “privilegi minimi” delle *best practice* per svolgere una funzione;
- Garantendo l’applicazione di misure idonee al rilevamento di intrusioni e/o alla protezione contro di esse;
- Ove appropriato, monitorando l’integrità dei file in modo da rilevare eventuali aggiunte, modifiche o eliminazioni di dati o file di sistema critici.
- Modifica di tutte le password predefinite o fornite dai vendor prima dell’attivazione dei componenti di rete.

20.2. La Rete della Terza parte dovrebbe soddisfare tutti i requisiti normativi e di legge; e

- Evitare, al meglio delle possibilità, che soggetti non autorizzati (ad es. hacker) accedano alla/e Rete/i del Terzo;
- Ridurre, al meglio delle possibilità, il rischio di uso improprio della/e Rete/i del Terzo da parte di soggetti non autorizzati ad accedervi.
- Mettere in atto ogni ragionevole sforzo per rilevare eventuali Violazioni della sicurezza, permettendo una veloce rettifica dei problemi derivanti e l’identificazione dei soggetti che hanno ottenuto l’accesso e di come tale accesso è stato ottenuto.

21.Mitigazione dei casi di “Denial of Service”.

21.1. La Terza parte deve assicurarsi che i sistemi principali siano protetti da attacchi di tipo “Denial of Service” (DoS) e “Distributed Denial of Service” (DDoS).

22.Monitoraggio e Analisi in continuo della Sicurezza.

22.1. La Terza parte deve garantire di disporre di un quadro coerente e consolidato per la gestione di audit e log che preveda l’analisi degli eventi chiave (compresi gli accessi con privilegi e l’attività del personale) relativi ai sistemi principali, comprese le applicazioni. I log derivanti devono essere conservati per un un periodo minimo di 12 mesi. Come minimo, la Terza parte deve garantire che i log (ove appropriato) contengano i seguenti eventi:

- Punti di inizio e di fine del processo analizzato.
- Modifiche al tipo di evento analizzato, in base a quanto richiesto dall'*audit trail* (ad esempio, i parametri di avvio e le eventuali modifiche ad essi apportate).
- Avvio e arresto dei sistemi.
- Login avvenuti con successo.
- Tentativi di login non andati a buon fine (ad esempio, inserimento di ID utente o password errati).
- Creazione, modifica ed eliminazione di account utente.
- Risorsa a cui i soggetti hanno avuto accesso (ad esempio, dati),
- Dove è avvenuto l'accesso alla risorsa (ad esempio, indirizzo IP),
- Quando (ad esempio, data e ora).

22.2. Il quadro di gestione delle attività di audit e log deve prevedere i seguenti aspetti:

- Garanzia che i log degli eventi principali vengano rivisti da un soggetto indipendente almeno una volta al mese per rilevare eventuali attività non autorizzate, metodi e target degli attacchi
- Le eccezioni vengono annotate e studiate fino alla relativa risoluzione
- I log vengono raccolti da più fonti e sensori, messi in correlazione tra loro, archiviati in una posizione sicura e a prova di manomissione per poter procedere alla ricostruzione degli eventi.
- L'impatto di tali eventi viene determinato in base a delle soglie di allerta prestabilite che prevedono un'azione tempestiva determinata dalla criticità dell'allarme.

23. Sensibilizzazione e Formazione.

23.1. La Terza parte deve garantire che tutti i membri del relativo personale che operano sotto il suo controllo partecipino ai corsi di formazione obbligatori sulla sicurezza delle informazioni, che devono comprendere le *best practice* in tema di sicurezza informatica e la protezione dei dati personali. Detti corsi devono essere frequentati entro un mese dall'inizio del rapporto lavorativo e devono essere aggiornati almeno una volta all'anno includendo, ove appropriato:

- Utenti con privilegi
- Stakeholder di Terzi (ad esempio, subappaltatori, clienti, partner)
- Alta dirigenza
- Personale addetto alla sicurezza fisica e informatica

23.2. La Terza parte deve garantire l'esistenza di un test atto a verificare che l'utente abbia capito le nozioni apprese durante le attività di sensibilizzazione e formazione.

24.Diritto di Ispezione.

24.1. La Terza parte deve consentire a BT di svolgere un'ispezione dell'ambiente di controllo in cui vengono sviluppati, realizzati o prestati i servizi, affinché possa eseguire delle prove e/o valutazioni di conformità ai requisiti di sicurezza almeno a cadenza annuale (o subito dopo un incidente).

24.2. I costi sostenuti per rimediare a eventuali debolezze nel sistema di sicurezza individuate da BT saranno in capo alla Terza parte, che dovrà provvedere nelle tempistiche stabilite dalle Parti.

24.3. In caso si verifichi un incidente grave, la Terza parte dovrà collaborare appieno con BT in eventuali indagini conseguenti svolte da BT, un'autorità normativa e/o un'autorità incaricata dell'applicazione

della legge, garantendo l'accesso e l'assistenza necessari e appropriati a svolgere le dovute indagini. BT potrebbe dover richiedere l'isolamento della Terza parte per valutare eventuali risorse rilevanti appartenenti alla Terza parte e aiutare le indagini; la Terza parte non dovrà negare o ritardare tale richiesta senza giustificazione.

25.Sicurezza fisica - Sede di BT.

25.1 Tutto il personale della Terza parte che lavora presso le sedi BT dovrà essere in possesso di, e mostrare chiaramente, una tessera identificativa fornita da BT o dal Terzo, la quale deve essere corredata di una fotografia chiara e che raffiguri in modo veritiero il suo proprietario. BT potrebbe anche fornire al personale della Terza parte una tessera di accesso elettronica e/o una tessera per visitatori a durata limitata da utilizzare secondo le istruzioni di emissione locali.

25.2 Qualora BT abbia fornito al personale della Terza parte una tessera di accesso, la Terza parte dovrà tempestivamente comunicare a BT, entro e non oltre 5 giorni lavorativi, quando un membro del suo personale non avrà più necessità di accedere alle sedi BT.

25.3 Solo i server con configurazione approvata di BT (approved "BT build servers"), i Webtop PC di BT e gli End Device fidati possono essere connessi direttamente (tramite spina a una porta LAN o con connessione Wireless) ai domini BT. Senza autorizzazione scritta di BT, la Terza parte non potrà collegare nessuna apparecchiatura non approvata da BT ai Domini BT.

25.4 I criteri di protezione fisica e le linee guida per lavorare presso le sedi di BT dovranno essere rispettate e dovranno includere, a titolo esemplificativo ma non esaustivo, l'accompagnamento del Personale della Terza parte e l'adozione di pratiche di lavoro appropriate all'interno delle aree protette.

25.5 Qualora la Terza parte sia autorizzata a fornire al suo personale un accesso senza accompagnamento a determinate aree della proprietà di BT, il firmatario autorizzato della Terza parte e il Personale della Terza parte dovranno attenersi alle indicazioni contenute nel documento Accesso ai siti di BT da parte dei Fornitori - Guida obbligatoria alla sicurezza

Inoltre, il firmatario autorizzato della Terza parte e il Personale della Terza parte dovranno essere sottoposti almeno ai controlli preliminari all'assunzione L2

26. Sicurezza di rete – Rete propria di BT.

26.1 La Terza parte dovrà mettere a disposizione del Referente di BT Security i nomi, gli indirizzi (e tutti gli altri dettagli che BT riterrà necessari) di ogni singolo membro del personale del terzo che, periodicamente, sarà direttamente coinvolto nell'implementazione, manutenzione e/o gestione del servizio prima che questi siano rispettivamente impiegati in tali attività di implementazione, manutenzione e/o gestione.

26.2 In relazione alle sue attività di supporto con base in Regno Unito, la Terza parte dovrà avere un team di addetti alla sicurezza qualificati composto da almeno un cittadino britannico che dovrà essere disponibile per mantenere i rapporti con il Referente di BT Security (o soggetti da lui nominati) e partecipare alle riunioni che il Referente di BT Security deciderà ragionevolmente di richiedere periodicamente.

26.3 La Terza parte dovrà fornire al Referente di BT Security un programma (opportunamente aggiornato quando necessario) di tutti i componenti attivi compresi nel Servizio e/o nei Servizi e le loro rispettive fonti.

26.4 La Terza parte dovrà fornire i dettagli dei singoli membri del personale che faranno da collegamento con la squadra addetta alla gestione delle vulnerabilità di BT (CERT) per quanto riguarda la discussione sulle vulnerabilità identificate dalla terza parte relativamente a BT nel o nei Servizi. La Terza parte dovrà fornire a BT informazioni puntuali sulle vulnerabilità e conformarsi (a spese della terza parte) a ragionevoli requisiti in relazione alle vulnerabilità periodicamente comunicati dal Referente di BT Security. La Terza parte informerà BT in merito a qualsivoglia vulnerabilità in tempi sufficienti a

consentire l'applicazione o l'installazione di controlli di mitigazione, prima che la terza parte renda pubbliche tali vulnerabilità.

26.5 La Terza parte dovrà garantire che tutti i componenti collegati alla sicurezza compresi nel Servizio come identificati da o per BT vengano, periodicamente e a spese della terza parte, valutati esternamente a ragionevole soddisfazione di BT.

26.6 La Terza parte dovrà fornire prontamente, in ogni caso entro 7 giorni lavorativi, al Referente di BT Security tutti i dettagli relativi a qualsivoglia caratteristica e/o funzionalità di ciascuno dei Servizi (o che sono state pianificate nella Roadmap di ciascuno dei Servizi) che, periodicamente:

- la Terza parte conoscerà; o
- il Referente di BT Security ritiene ragionevolmente siano progettate, o possano essere utilizzate per intercettazioni illegali o altro tipo di intercettazione o traffico delle telecomunicazioni, e informi di conseguenza la terza parte. Tali dettagli dovranno includere tutte le Informazioni ragionevolmente necessarie per consentire al Referente di BT Security di comprendere appieno la natura, la composizione e l'ambito di applicazione di tali caratteristiche e/o funzionalità.

26.7 Per mantenere l'accesso alle Reti e/o ai sistemi di BT, la Terza parte dovrà comunicare immediatamente a BT qualsivoglia modifica apportata al suo metodo di accesso tramite firewall, tra cui la fornitura della conversione di indirizzi di rete.

26.8 Alla Terza parte non è consentito utilizzare strumenti di monitoraggio di rete in grado di vedere informazioni sulle applicazioni.

26.9 La Terza parte dovrà garantire che la funzionalità IPv6 inclusa nei sistemi operativi sia disabilitata sugli host (ad esempio, server o dispositivi di utenti finali) che si collegano alla Rete BT e i domini dovrebbero essere disabilitati se non necessari.

26.10 Il personale della Terza parte che si occupa della compilazione, dello sviluppo o delle attività di supporto delle Reti BT o delle Risorse di rete dovranno garantire che tutti i membri del Personale della terza parte abbiano superato come minimo i controlli preliminari all'assunzione L2. I controlli preliminari all'assunzione L3 saranno richiesti per i ruoli identificati dal Referente di BT Security. Se la Terza parte non può dare direttamente il nulla osta di sicurezza al Personale della parte come parte dei controlli L3, BT fornirà la sua assistenza in tale procedura, a spese della terza parte.

26.11 La Terza parte dovrà occuparsi della manutenzione di hardware e software secondo quanto indicato nelle specifiche del produttore.

26.12 La Terza parte non dovrà utilizzare supporti amovibili (dischi, unità USB, ecc.) destinati ad attività di supporto e manutenzione per nessun altro scopo.

27. Glossario.

Termine	Definizione
Autenticazione a due fattori	A volte denominata verifica in due passaggi o autenticazione a doppio fattore, è un processo di sicurezza in cui l'utente fornisce due diversi fattori di autenticazione per la verifica della sua identità, al fine di proteggere al meglio le credenziali dell'utente e le risorse a cui l'utente può accedere.
Terza parte/Terzo	Soggetto che lavora per noi ma che non è un dipendente BT
AES	L'Advanced Encryption Standard (AES) è una specifica relativa alla crittografia dei dati elettronici elaborata dal National Institute of Standards and Technology (NIST) americano nel 2001.
ASG	Application Support Group

Gruppo BT	Per Gruppo BT si intendono tutte le CFU e le CU del Gruppo BT comprese, a titolo esemplificativo ma non esaustivo, Openreach, EE e Plusnet. Ai fini del presente documento, se non specificato diversamente, verranno tutte indicate con 'BT'
Stakeholder BT	Dipendente BT responsabile del lavoro affidato alla Terza parte.
TVCC	Televisione a circuito chiuso.
DBA	Amministratore di database
DC	Data Centre
Defence in Depth	Si tratta di un approccio alla sicurezza informatica in cui diversi meccanismi di difesa vengono organizzati su più livelli al fine di proteggere i dati e le informazioni di valore. Se un meccanismo fallisce, ne subentra un altro per sventare l'attacco.
DR	Disaster Recovery
GCM	Galois/Counter Mode è una modalità di funzionamento dei cifrari a blocchi crittografici a chiave simmetrica ampiamente adottato in virtù delle sue performance
HDD	Disco rigido
HMG	Governo del Regno Unito, comprensivo di tutti gli organi di governo del Regno Unito
ISMS	Sistema di gestione della sicurezza delle informazioni. Si tratta di un quadro di politiche e procedure comprensivo di tutti i controlli legali, fisici e tecnici coinvolti nei processi di gestione dei rischi informatici di un'azienda.
ISO 27001	Si tratta di uno standard di settore relativo ai sistemi di gestione della sicurezza delle informazioni (ISMS).
ISO 27017	Standard relativo ai controlli per la sicurezza delle informazioni basato sulla norma ISO/IEC 27002 per i servizi Cloud
ISO 7816	Standard internazionale relativo alle schede di identificazione elettroniche con contatti, nello specifico le smart card, gestito congiuntamente dall'Organizzazione internazionale per la normazione (ISO) e dalla Commissione Elettrotecnica Internazionale (IEC).
NAS	Dispositivo di archiviazione singolo che opera sui file di dati.
NIST	Il National Institute of Standards and Technology è un laboratorio di fisica e un'agenzia non governativa del Dipartimento del Commercio degli Stati Uniti.
PCI DSS	Il Payment Card Industry Data Security Standard (PCI DSS) è uno standard di sicurezza delle informazioni per le aziende che gestiscono carte di credito emesse dai principali sistemi di carte.
Account con privilegi	Un utente con privilegi è un soggetto a cui è concesso l'accesso amministrativo ai sistemi più importanti
RSA	(Rivest–Shamir–Adleman) è uno dei primi sistemi di crittografia a chiave pubblica e viene ampiamente utilizzato per proteggere la trasmissione dei dati.
SAN	Rete locale costituita da più dispositivi che operano su blocchi di disco
SSD	Unità allo stato solido

28.Cronologia delle modifiche.

N. versione	Data	Modifica apportata da	Breve descrizione della modifica
0.1	30/10/2017	Mark Tilston	Bozza iniziale per mappatura e aggiornamento contenuto
0.2	10/04/2019	Tim Hunt	Trasferito su nuovo formato

N. versione	Data	Modifica apportata da	Breve descrizione della modifica
1.0	01/05/2019	Ian Morton	Versione approvata
1.1	01/10/2019	Karen Tanner	Ulteriori controlli aggiunti per aumento dei requisiti di sicurezza di BT

29.Approvazione documento

Ruolo	Data
Mark Tilston	06/11/2019

30.Conformità

Siamo lieti del fatto che gran parte dei dipendenti BT agiscano in modo professionale e in linea con i valori di BT. Nei confronti di chi si comporta in modo non conforme al presente standard, BT potrebbe prendere misure disciplinari che variano in base alle norme e alle leggi locali.

Nei confronti di altri soggetti che si comportano in modo non conforme al presente standard, BT potrebbe decidere di risolvere gli accordi presi per la prestazione dei servizi.

31.Link e Informazioni utili

Per il personale di BT:

Questo è il link da cui è possibile accedere a tutte le Politiche e Standard BT.

I nostri standard e le politiche vengono sottoposti a revisione almeno una volta all'anno. Per consultare il nostro programma di revisione, fare clic qui.

Per segnalare un "Indicente di sicurezza", inviare un'e-mail a: Centro di controllo sicurezza

Per maggiori informazioni o linee guida sul presente standard o su qualsiasi altra politica o standard relativi alla sicurezza, contattare security.policy@bt.com

Per le Terze parti:

A questo link è possibile prendere visione di tutti gli Standard e altre condizioni di sicurezza.

32. Proprietà e Riservatezza

Il presente documento non dovrebbe essere condiviso con nessun'altra Terza parte senza l'autorizzazione scritta di BT. Il presente standard e tutti i documenti associati sono di proprietà di BT e, se richiesto, dovrebbero essere restituiti.

Il presente documento è classificato come "Internal"; tuttavia, se viene scaricato da una Terza parte dovrebbe essere trattato come "Confidential"