NORMA ITALIANA

Tecnologie informatiche

Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni

Requisiti

UNI CEI ISO/IEC 27001

MARZO 2014

Versione italiana del marzo 2014

Information technology

Security techniques - Information security management systems

Requirements

La norma specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni nel contesto di un'organizzazione. La presente norma internazionale include anche i requisiti per la valutazione e per il trattamento dei rischi relativi alla sicurezza delle informazioni adattati alle necessità dell'organizzazione. I requisiti stabiliti dalla presente norma internazionale sono di carattere generale e predisposti per essere applicabili a tutte le organizzazioni, indipendentemente dalla loro tipologia, dimensione e natura. L'esclusione di qualunque requisito specificato nei punti dal 4 al 10 non è accettabile quando un'organizzazione dichiara la sua conformità alla presente norma internazionale.

TESTO ITALIANO

La presente norma è l'adozione nazionale in lingua italiana della norma internazionale ISO/IEC 27001 (edizione ottobre 2013).

ICS 35.040

PREMESSA NAZIONALE

La presente norma costituisce l'adozione nazionale, in lingua italiana, della norma internazionale ISO/IEC 27001 (edizione ottobre 2013).

La norma internazionale ISO/IEC 27001 è stata elaborata dal Comitato Tecnico ISO/IEC JTC 1 "Tecnologia dell'informazione".

La presente norma è stata elaborata sotto la competenza dell'ente federato all'UNI

UNINFO - Tecnologie informatiche e loro applicazioni

e del

CEI - Comitato Elettrotecnico Italiano

che hanno giudicato la norma ISO/IEC 27001 rispondente, da un punto di vista tecnico, alle esigenze nazionali e ne hanno proposto alla Commissione Centrale Tecnica dell'UNI l'adozione nella presente versione in lingua italiana.

La Commissione Centrale Tecnica ha dato la sua approvazione il 21 febbraio 2014.

La presente norma è stata ratificata dal Presidente del CEI, con delibera del 24 febbraio 2014.

La presente norma è stata ratificata dal Presidente dell'UNI ed è entrata a far parte del corpo normativo nazionale il 6 marzo 2014.

INDICE

0 INTRODUZIONE

0.1 Generalità

La presente norma internazionale è stata elaborata allo scopo di fornire i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni. L'adozione di un sistema di gestione per la sicurezza delle informazioni è una decisione strategica per un'organizzazione. Stabilire e attuare un sistema di gestione per la sicurezza delle informazioni di un'organizzazione sono influenzati dalle sue necessità e obiettivi, dai suoi requisiti di sicurezza, dai suoi processi organizzativi e dalla sua dimensione e struttura. È previsto che tutti questi fattori cambino nel tempo.

Il sistema di gestione per la sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità dalle informazioni mediante l'applicazione di un processo di gestione del rischio e dà fiducia alle parti interessate sull'adeguatezza della gestione dei rischi.

È importante che il sistema di gestione per la sicurezza delle informazioni sia parte integrante dei processi e della struttura gestionale complessiva dell'organizzazione e che la sicurezza delle informazioni sia considerata nella progettazione dei processi, dei sistemi informativi e dei controlli. Ci si attende che un sistema di gestione per la sicurezza delle informazioni sia commisurato alle necessità dell'organizzazione.

La presente norma internazionale può essere utilizzata da parti interne ed esterne al fine di valutare la capacità di un'organizzazione di soddisfare i propri requisiti relativi alla sicurezza delle informazioni.

L'ordine con cui sono presentati i requisiti nella presente norma internazionale non riflette il loro livello di importanza, né implica un ordine con cui devono essere attuati. Gli elementi delle liste sono numerati solo per finalità di referenziazione.

La ISO/IEC 27000 presenta una visione d'insieme e il vocabolario dei sistemi di gestione per la sicurezza delle informazioni, citando la famiglia di norme relative ai sistemi di gestione per la sicurezza delle informazioni (tra cui la ISO/IEC 27003 [2], la ISO/IEC 27004 [3] e la ISO/IEC 27005 [4]), con i termini e le definizioni correlati.

0.2 Compatibilità con altre norme relative a sistemi di gestione

La presente norma internazionale utilizza la struttura ad alto livello, gli stessi titoli per i punti, il testo identico, i termini comuni e le definizioni fondamentali definite nell'Annex SL delle ISO/IEC Directives, Part 1, Consolidated ISO Supplement, e mantiene quindi la compatibilità con le altre norme relative ai sistemi di gestione che hanno adottato l'Annex SL.

L'approccio comune definito dall'Annex SL è utile a quelle organizzazioni che scelgono di realizzare un unico sistema di gestione che soddisfi i requisiti di due o più norme relative ai sistemi di gestione.

1 SCOPO E CAMPO DI APPLICAZIONE

La presente norma internazionale specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni nel contesto di un'organizzazione. La presente norma internazionale include anche i requisiti per la valutazione e il trattamento dei rischi relativi alla sicurezza delle informazioni adattati alle necessità dell'organizzazione. I requisiti stabiliti dalla presente norma internazionale sono di carattere generale e predisposti per essere applicabili a tutte le organizzazioni, indipendentemente dalla loro tipologia, dimensione e natura. L'esclusione di qualunque requisito specificato nei punti dal 4 al 10 non è accettabile quando un'organizzazione dichiara la sua conformità alla presente norma internazionale.

2 RIFERIMENTI NORMATIVI

I documenti richiamati di seguito, in tutto o in parte, sono richiamati con carattere normativo nel presente documento e sono indispensabili per la sua applicazione. Per quanto riguarda i riferimenti con data, si applica esclusivamente l'edizione citata. Per i riferimenti non datati, vale l'ultima edizione del documento a cui si fa riferimento (compresi gli aggiornamenti).

ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary

3 TERMINI E DEFINIZIONI

Ai fini del presente documento si applicano i termini e le definizioni specificati dalla ISO/IEC 27000.

4 CONTESTO DELL'ORGANIZZAZIONE

4.1 Comprendere l'organizzazione e il suo contesto

L'organizzazione deve determinare i fattori esterni ed interni pertinenti alle sue finalità e che influenzano la sua capacità di conseguire gli esiti previsti per il proprio sistema di gestione per la sicurezza delle informazioni.

Nota La determinazione di questi fattori fa riferimento alla definizione del contesto esterno ed interno dell'organizzazione considerato al punto 5.3 della ISO 31000:2009 [5].

4.2 Comprendere le necessità e le aspettative delle parti interessate

L'organizzazione deve determinare:

a) le parti interessate pertinenti al sistema di gestione per la sicurezza delle informazioni; e

b) i requisiti di tali parti interessate attinenti la sicurezza delle informazioni.

Nota I requisiti delle parti interessate possono includere requisiti cogenti*) e obblighi contrattuali.

4.3 Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni

L'organizzazione deve determinare i confini e l'applicabilità del sistema di gestione per la sicurezza delle informazioni per stabilirne il campo di applicazione.

Nel determinare il campo di applicazione, l'organizzazione deve considerare:

a) i fattori esterni ed interni di cui al punto 4.1;

b) i requisiti di cui al punto 4.2; e

c) le interfacce e le interdipendenze tra le attività svolte dall'organizzazione, e quelle svolte da altre organizzazioni.

Il campo di applicazione deve essere disponibile come insieme di informazioni documentate.

4.4 Sistema di gestione per la sicurezza delle informazioni

L'organizzazione deve stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni, in conformità ai requisiti della presente norma internazionale.

*) Nota nazionale - Per "requisiti cogenti" si intendono, nel seguito, quelli stabiliti da leggi, regolamenti, direttive (requisiti legali) e prescrizioni obbligatorie in genere.

5 LEADERSHIP

5.1 Leadership e impegno

L'alta direzione deve dimostrare leadership e impegno nei riguardi del sistema di gestione per la sicurezza delle informazioni:

a) assicurando che la politica e gli obiettivi per la sicurezza delle informazioni siano stabiliti e siano compatibili con gli indirizzi strategici dell'organizzazione;

b) assicurando l'integrazione dei requisiti del sistema di gestione per la sicurezza delle informazioni nei processi dell'organizzazione;

c) assicurando la disponibilità delle risorse necessarie al sistema di gestione per la sicurezza delle informazioni;

d) comunicando l'importanza di un'efficace gestione della sicurezza delle informazioni e dell'essere conforme ai requisiti del sistema di gestione per la sicurezza delle informazioni;

e) assicurando che il sistema di gestione per la sicurezza delle informazioni consegua gli esiti previsti;

f) fornendo guida e sostegno alle persone per contribuire all'efficacia del sistema di gestione per la sicurezza delle informazioni;

g) promuovendo il miglioramento continuo; e

h) fornendo sostegno ad altri pertinenti ruoli gestionali nel dimostrare la propria leadership come opportuno nelle rispettive aree di responsabilità.

5.2 Politica

L'alta direzione deve stabilire una politica per la sicurezza delle informazioni che:

a) sia appropriata alle finalità dell'organizzazione;

b) comprenda gli obiettivi per la sicurezza delle informazioni (vedere punto 6.2) o fornisca un quadro di riferimento per fissare gli obiettivi per la sicurezza delle informazioni;

c) comprenda un impegno a soddisfare i requisiti applicabili e attinenti la sicurezza delle informazioni; e

d) comprenda un impegno per il miglioramento continuo del sistema di gestione per la sicurezza delle informazioni.

La politica per la sicurezza delle informazioni deve:

e) essere disponibile come insieme di informazioni documentate;

f) essere comunicata all'interno dell'organizzazione; e

g) essere disponibile per le parti interessate, per quanto appropriato.

5.3 Ruoli, responsabilità e autorità nell'organizzazione

L'alta direzione deve assicurare che le responsabilità e le autorità per i ruoli pertinenti la sicurezza delle informazioni siano assegnati e comunicati.

L'alta direzione deve assegnare le responsabilità e autorità per:

a) assicurare che il sistema di gestione per la sicurezza delle informazioni sia conforme ai requisiti della presente norma internazionale; e

b) riferire all'alta direzione sulle prestazioni del sistema di gestione per la sicurezza delle informazioni.

Nota L'alta direzione può anche assegnare responsabilità e autorità per riferire all'interno dell'organizzazione sulle prestazioni del sistema di gestione per la sicurezza delle informazioni.

6 PIANIFICAZIONE

6.1 Azioni per affrontare rischi e opportunità

6.1.1 Generalità

Nel pianificare il sistema di gestione per la sicurezza delle informazioni, l'organizzazione deve considerare i fattori di cui al punto 4.1 e i requisiti di cui al punto 4.2 e determinare i rischi e le opportunità che è necessario affrontare per:

a) assicurare che il sistema di gestione per la sicurezza delle informazioni possa conseguire gli esiti previsti;

b) prevenire, o ridurre, gli effetti indesiderati; e

c) realizzare il miglioramento continuo.

L'organizzazione deve pianificare:

d) le azioni per affrontare questi rischi e opportunità; e

e) le modalità per

   1) integrare e attuare le azioni nei processi del proprio sistema di gestione per la sicurezza delle informazioni; e

   2) valutare l'efficacia di tali azioni.

6.1.2 Valutazione del rischio relativo alla sicurezza delle informazioni

L'organizzazione deve definire e applicare un processo di valutazione del rischio relativo alla sicurezza delle informazioni che:

a) stabilisca e mantenga i criteri di rischio relativo alla sicurezza delle informazioni, che includano:

   1) i criteri per l'accettazione del rischio; e

   2) i criteri per effettuare valutazioni del rischio relativo alla sicurezza delle informazioni;

b) assicuri che ripetute valutazioni del rischio relativo alla sicurezza delle informazioni producano risultati coerenti, validi e confrontabili tra loro;

c) identifichi i rischi relativi alla sicurezza delle informazioni:

   1) applicando il processo di valutazione del rischio relativo alla sicurezza delle informazioni per identificare i rischi associati alla perdita di riservatezza, di integrità e di disponibilità delle informazioni incluse nel campo di applicazione del sistema di gestione per la sicurezza delle informazioni; e

   2) identificando i responsabili dei rischi;

d) analizzi i rischi relativi alla sicurezza delle informazioni:

   1) valutando le possibili conseguenze che risulterebbero se i rischi identificati al punto 6.1.2 c) 1) si concretizzassero;

   2) valutando la verosimiglianza realistica del concretizzarsi dei rischi identificati al punto 6.1.2 c) 1); e

   3) determinando i livelli di rischio;

e) ponderi i rischi relativi alla sicurezza delle informazioni:

   1) comparando i risultati dell'analisi del rischio con i criteri di rischio stabiliti al punto 6.1.2 a); e

   2) stabilendo le priorità dei rischi analizzati per il trattamento del rischio.

L'organizzazione deve conservare informazioni documentate sul processo di valutazione del rischio relativo alla sicurezza delle informazioni.

6.1.3 Trattamento del rischio relativo alla sicurezza delle informazioni

L'organizzazione deve definire e applicare un processo di trattamento del rischio relativo alla sicurezza delle informazioni per:

a) selezionare le adeguate opzioni per il trattamento del rischio relativo alla sicurezza delle informazioni, tenendo in considerazione i risultati della valutazione del rischio;

b) determinare tutti i controlli necessari per attuare le opzioni selezionate per il trattamento del rischio relativo alla sicurezza delle informazioni;

Nota Le organizzazioni possono progettare i controlli come richiesto o identificarli da qualsiasi fonte.

c) confrontare i controlli determinati al punto 6.1.3.b) con quelli nell'appendice A e verificare che non siano stati omessi controlli necessari;

Nota 1 L'appendice A riporta un'ampia lista di obiettivi di controllo e di controlli. Gli utilizzatori di questa norma internazionale sono indirizzati all'appendice A per assicurare che non siano trascurati controlli necessari.

Nota 2 Gli obiettivi di controllo sono implicitamente inclusi nei controlli scelti. La lista di obiettivi di controllo e di controlli riportati nell'appendice A non è esaustiva, e ulteriori obiettivi di controllo e controlli potrebbero essere necessari.

d) redigere una Dichiarazione di applicabilità che riporti i controlli necessari [vedere i punti 6.1.3 b) e c)] e le giustificazioni per l'inclusione, che siano attuati o meno, e per l'esclusione dei controlli dell'appendice A;

e) formulare un piano di trattamento del rischio relativo alla sicurezza delle informazioni; e

f) ottenere l'approvazione del piano di trattamento del rischio relativo alla sicurezza delle informazioni e l'accettazione dei rischi residui relativi alla sicurezza delle informazioni da parte dei responsabili dei rischi.

L'organizzazione deve conservare informazioni documentate sul processo di trattamento del rischio relativo alla sicurezza delle informazioni.

Nota I processi di valutazione e trattamento del rischio relativo alla sicurezza delle informazioni riportati nella presente norma internazionale sono allineati con i principi e le linee guida generali fornite dalla ISO 31000 Risk management - Principles and guidelines [5].

6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli

L'organizzazione deve stabilire gli obiettivi per la sicurezza delle informazioni per le funzioni e per i livelli pertinenti.

Gli obiettivi per la sicurezza delle informazioni devono:

a) essere coerenti con la politica per la sicurezza delle informazioni;

b) essere misurabili (se possibile);

c) tenere in considerazione i requisiti applicabili alla sicurezza delle informazioni e i risultati della valutazione del rischio e del trattamento del rischio;

d) essere comunicati; e

e) essere aggiornati per quanto appropriato.

L'organizzazione deve conservare informazioni documentate sugli obiettivi per la sicurezza delle informazioni.

Nel pianificare come conseguire i propri obiettivi per la sicurezza delle informazioni, l'organizzazione deve determinare:

f) cosa sarà fatto;

g) quali risorse saranno necessarie;

h) chi ne sarà responsabile;

i) quando sarà completato; e

j) come saranno valutati i risultati.

7 SUPPORTO

7.1 Risorse

L'organizzazione deve determinare e mettere a disposizione le risorse necessarie per stabilire, attuare, mantenere e migliorare in modo continuo il sistema di gestione per la sicurezza delle informazioni.

7.2 Competenza

L'organizzazione deve:

a) determinare le necessarie competenze per le persone che svolgono attività sotto il suo controllo e che influenzano le sue prestazioni relative alla sicurezza delle informazioni;

b) assicurare che queste persone siano competenti sulla base di istruzione, formazione e addestramento o esperienza appropriate;

c) ove applicabile, intraprendere azioni per acquisire la necessaria competenza e valutare l'efficacia delle azioni intraprese; e

d) conservare appropriate informazioni documentate quale evidenza delle competenze.

Nota Le azioni applicabili possono includere, per esempio: il provvedere alla formazione e addestramento, l'affiancamento, o la riallocazione del personale impiegato, oppure l'assunzione o l'incarico a contratto di persone competenti.

7.3 Consapevolezza

Le persone che svolgono attività sotto il controllo dell'organizzazione devono essere consapevoli:

a) della politica per la sicurezza delle informazioni;

b) del proprio contributo all'efficacia del sistema di gestione per la sicurezza delle informazioni, inclusi i benefici derivanti dal miglioramento delle prestazioni relative alla sicurezza delle informazioni; e

c) delle implicazioni del non essere conformi ai requisiti del sistema di gestione per la sicurezza delle informazioni.

7.4 Comunicazione

L'organizzazione deve determinare la necessità per le comunicazioni interne ed esterne in relazione al sistema di gestione per la sicurezza delle informazioni, includendo:

a) ciò su cui comunicare;

b) quando comunicare;

c) con chi comunicare;

d) chi deve comunicare; e

e) i processi attraverso i quali devono essere effettuate le comunicazioni.

7.5 Informazioni documentate

7.5.1 Generalità

Il sistema di gestione per la sicurezza delle informazioni dell'organizzazione deve comprendere:

a) le informazioni documentate richieste dalla presente norma internazionale; e

b) le informazioni documentate che l'organizzazione ritiene necessarie per l'efficacia del sistema di gestione per la sicurezza delle informazioni.

Nota L'estensione delle informazioni documentate del sistema di gestione per la sicurezza delle informazioni può variare da un'organizzazione all'altra in base a:

1) la dimensione dell'organizzazione e il suo tipo di attività, processi, prodotti e servizi;

2) la complessità dei processi e delle loro interazioni; e

3) la competenza delle persone.

7.5.2 Creazione e aggiornamento

Nel creare e aggiornare le informazioni documentate, l'organizzazione deve assicurare appropriati:

a) identificazione e descrizione (per esempio titolo, data, autore o numero di riferimento);

b) formato (per esempio lingua, versione del software, grafica) e supporto (per esempio cartaceo, elettronico); e

c) riesame e approvazione in merito all'idoneità e all'adeguatezza.

7.5.3 Controllo delle informazioni documentate

Le informazioni documentate richieste dal sistema di gestione per la sicurezza delle informazioni e dalla presente norma internazionale devono essere tenute sotto controllo per assicurare che:

a) siano disponibili e idonee all'uso, dove e quando necessario; e

b) siano adeguatamente protette (per esempio da perdita di riservatezza, uso improprio o perdita d'integrità).

Il controllo delle informazioni documentate, da parte dell'organizzazione, deve riguardare le seguenti attività, per quanto applicabile:

c) distribuzione, accesso, reperimento e uso;

d) archiviazione e preservazione, compreso il mantenimento della leggibilità;

e) tenuta sotto controllo delle modifiche (per esempio delle versioni); e

f) conservazione e successive disposizioni.

Le informazioni documentate di origine esterna ritenute necessarie dall'organizzazione per la pianificazione e per il funzionamento del sistema di gestione per la sicurezza delle informazioni, devono essere identificate per quanto appropriato, e tenute sotto controllo.

Nota L'accesso implica una decisione in merito ai permessi per prendere soltanto visione delle informazioni documentate, o ai permessi e autorità per visualizzarle e modificarle, eccetera.

8 ATTIVITÀ OPERATIVE

8.1 Pianificazione e controllo operativi

L'organizzazione deve pianificare, attuare e tenere sotto controllo i processi necessari per soddisfare i requisiti di sicurezza delle informazioni e per mettere in atto le azioni determinate al punto 6.1. L'organizzazione deve anche attuare i piani per conseguire gli obiettivi per la sicurezza delle informazioni determinati al punto 6.2.

L'organizzazione deve le conservare informazioni documentate nella misura necessaria ad avere fiducia che i processi siano stati eseguiti come pianificato.

L'organizzazione deve tenere sotto controllo le modifiche pianificate e riesaminare le conseguenze dei cambiamenti involontari, intraprendendo azioni per mitigare qualunque effetto negativo, per quanto necessario.

L'organizzazione deve assicurare che i processi affidati all'esterno siano determinati e tenuti sotto controllo.

8.2 Valutazione del rischio relativo alla sicurezza delle informazioni

L'organizzazione deve effettuare le valutazioni del rischio relativo alla sicurezza delle informazioni a intervalli pianificati o quando sono proposti o si verificano cambiamenti significativi, considerando i criteri stabiliti al punto 6.1.2 a).

L'organizzazione deve conservare informazioni documentate sui risultati delle valutazioni del rischio relativo alla sicurezza delle informazioni.

8.3 Trattamento del rischio relativo alla sicurezza delle informazioni

L'organizzazione deve attuare il piano di trattamento del rischio relativo alla sicurezza delle informazioni.

L'organizzazione deve conservare informazioni documentate sui risultati del trattamento del rischio relativo alla sicurezza delle informazioni.

9 VALUTAZIONE DELLE PRESTAZIONI

9.1 Monitoraggio, misurazione, analisi e valutazione

L'organizzazione deve valutare le prestazioni della sicurezza delle informazioni e l'efficacia del sistema di gestione per la sicurezza delle informazioni.

L'organizzazione deve determinare:

a) cosa è necessario monitorare e misurare, includendo i processi e i controlli relativi alla sicurezza delle informazioni;

b) i metodi per il monitoraggio, la misurazione, l'analisi e la valutazione, per quanto applicabile, per assicurare risultati validi;

Nota I metodi selezionati dovrebbero produrre risultati comparabili e ripetibili affinché siano considerati validi.

c) quando il monitoraggio e la misurazione devono essere effettuati;

d) chi deve monitorare e misurare;

e) quando i risultati del monitoraggio e della misurazione devono essere analizzati e valutati; e

f) chi deve analizzare e valutare questi risultati.

L'organizzazione deve conservare appropriate informazioni documentate quale evidenza dei risultati dei monitoraggi e delle misurazioni.

9.2 Audit interno

L'organizzazione deve condurre, ad intervalli pianificati, audit interni per fornire informazioni tali da permettere di riconoscere se il sistema di gestione per la sicurezza delle informazioni:

a) è conforme ai

1) requisiti propri dell'organizzazione per il suo sistema di gestione per la sicurezza delle informazioni; e

2) requisiti della presente norma internazionale;

b) è efficacemente attuato e mantenuto.

L'organizzazione deve:

c) pianificare, stabilire, attuare e mantenere uno o più programmi di audit, comprensivi di frequenze, metodi, responsabilità, requisiti di pianificazione e reporting. I programmi di audit devono prendere in considerazione l'importanza dei processi coinvolti e i risultati di audit precedenti;

d) definire i criteri di audit e il campo di applicazione per ciascun audit;

e) selezionare gli auditor e condurre gli audit in modo da assicurare l'obiettività e l'imparzialità del processo di audit;

f) assicurare che i risultati degli audit siano riportati ai pertinenti responsabili; e

g) conservare informazioni documentate quale evidenza dell'attuazione del programma di audit e dei risultati di audit.

9.3 Riesame di direzione

L'alta direzione deve, a intervalli pianificati, riesaminare il sistema di gestione per la sicurezza delle informazioni dell'organizzazione, per assicurarne la continua idoneità, adeguatezza ed efficacia.

Il riesame di direzione deve includere considerazioni su:

a) lo stato delle azioni derivanti dai precedenti riesami di direzione;

b) i cambiamenti dei fattori esterni e interni che hanno attinenza con il sistema di gestione per la sicurezza delle informazioni;

c) le informazioni di ritorno sulle prestazioni relative alla sicurezza delle informazioni, compresi gli andamenti:

   1) delle non conformità e azioni correttive;

   2) dei risultati del monitoraggio e della misurazione;

   3) dei risultati di audit; e

   4) del raggiungimento degli obiettivi per la sicurezza delle informazioni;

d) le informazioni di ritorno dalle parti interessate;

e) i risultati della valutazione del rischio e lo stato del piano di trattamento del rischio; e

f) le opportunità per il miglioramento continuo.

Gli elementi in uscita dal riesame di direzione devono comprendere decisioni relative alle opportunità per il miglioramento continuo e ogni necessità di modifiche al sistema di gestione per la sicurezza delle informazioni.

L'organizzazione deve conservare informazioni documentate quale evidenza dei risultati dei riesami di direzione.

10 MIGLIORAMENTO

10.1 Non conformità e azioni correttive

Quando si verifica una non conformità, l'organizzazione deve:

a) reagire alla non conformità e, per quanto applicabile:

   1) intraprendere azioni per tenerla sotto controllo e correggerla; e

   2) fronteggiarne le conseguenze;

b) valutare la necessità di azioni per eliminare le cause della non conformità, in modo che non si ripeta o non accada altrove:

   1) riesaminando la non conformità;

   2) determinando le cause della non conformità; e

   3) determinando se esistono o potrebbero verificarsi non conformità simili;

c) attuare ogni azione necessaria;

d) riesaminare l'efficacia di ogni azione correttiva intrapresa; e

e) effettuare, se necessario, modifiche al sistema di gestione per la sicurezza delle informazioni.

Le azioni correttive devono essere adeguate agli effetti delle non conformità riscontrate.

L'organizzazione deve tenere informazioni documentate quale evidenza:

f) della natura delle non conformità e ogni successiva azione intrapresa, e

g) dei risultati di ogni azione correttiva.

10.2 Miglioramento continuo

L'organizzazione deve migliorare in modo continuo l'idoneità, l'adeguatezza e l'efficacia del sistema di gestione per la sicurezza delle informazioni.

APPENDICE A (normativa) OBIETTIVI DI CONTROLLO E CONTROLLI DI RIFERIMENTO

Gli obiettivi di controllo e i controlli elencati nel prospetto A.1 sono ripresi direttamente dai punti da 5 a 18 nella ISO/IEC 27002:2013 [1] e allineati ad essi e sono da utilizzare nel contesto del punto 6.1.3.

prospetto A.1 **Obiettivi di controllo e controlli**

A.5 Politiche per la sicurezza delle informazioni		
A.5.1 Indirizzi della direzione per la sicurezza delle informazioni		
Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti.		
A.5.1.1	Politiche per la sicurezza delle informazioni	*Controllo* Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.
A.5.1.2	Riesame delle politiche per la sicurezza delle informazioni	*Controllo* Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.
A.6 Organizzazione della sicurezza delle informazioni		
A.6.1 Organizzazione interna		
Obiettivo: Stabilire un quadro di riferimento gestionale per intraprendere e controllare l'attuazione e l'esercizio della sicurezza delle informazioni all'interno dell'organizzazione.		
A.6.1.1	Ruoli e responsabilità per la sicurezza delle informazioni	*Controllo* Tutte le responsabilità relative alla sicurezza delle informazioni devono essere definite e assegnate.
A.6.1.2	Separazione dei compiti	*Controllo* I compiti e le aree di responsabilità in conflitto tra loro devono essere separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell'organizzazione.
A.6.1.3	Contatti con le autorità	*Controllo* Devono essere mantenuti appropriati contatti con le autorità pertinenti.
A.6.1.4	Contatti con gruppi specialistici	*Controllo* Devono essere mantenuti appropriati contatti con gruppi specialistici o altri contesti ed associazioni professionali frequentate da specialisti della sicurezza delle informazioni.
A.6.1.5	Sicurezza delle informazioni nella gestione dei progetti	*Controllo* La sicurezza delle informazioni deve essere indirizzata nell'ambito della gestione dei progetti, a prescindere dal tipo di progetto.
A.6.2 Dispositivi portatili e telelavoro		
Obiettivo: Assicurare la sicurezza del telelavoro e nell'uso di dispositivi portatili		
A.6.2.1	Politica per i dispositivi portatili	*Controllo* Deve essere adottata una politica e delle misure di sicurezza a suo supporto per la gestione dei rischi introdotti dall'uso di dispositivi portatili.
A.6.2.2	Telelavoro	*Controllo* Devono essere attuate una politica e delle misure di sicurezza a suo supporto per proteggere le informazioni accedute, elaborate o memorizzate presso siti di telelavoro.

prospetto A.1 **Obiettivi di controllo e controlli** (Continua)

A.7 Sicurezza delle risorse umane		
A.7.1 Prima dell'impiego		
Obiettivo: Assicurare che il personale e i collaboratori comprendano le proprie responsabilità e siano adatti a ricoprire i ruoli per i quali sono presi in considerazione.		
A.7.1.1	Screening	*Controllo* Devono essere svolti dei controlli per la verifica del background effettuati su tutti i candidati all'impiego in accordo con le leggi, con i regolamenti pertinenti e con l'etica e devono essere proporzionati alle esigenze di business, alla classificazione delle informazioni da accedere e ai rischi percepiti.
A.7.1.2	Termini e condizioni di impiego	*Controllo* Gli accordi contrattuali con il personale e con i collaboratori devono specificare le responsabilità loro e dell'organizzazione relativamente alla sicurezza delle informazioni.
A.7.2 Durante l'impiego		
Obiettivo: Assicurare che il personale e i collaboratori siano a conoscenza delle loro responsabilità per la sicurezza delle informazioni e vi adempiano.		
A.7.2.1	Responsabilità della direzione	*Controllo* La direzione deve richiedere a tutto il personale e ai collaboratori di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite dall'organizzazione.
A.7.2.2	Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni	*Controllo* Tutto il personale dell'organizzazione e, quando pertinente, i collaboratori, devono ricevere un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa.
A.7.2.3	Processo disciplinare	*Controllo* Deve essere istituito un processo disciplinare, formale e comunicato, per intraprendere provvedimenti nei confronti del personale che ha commesso una violazione della sicurezza delle informazioni.
A.7.3 Cessazione e variazione del rapporto di lavoro		
Obiettivo: Tutelare gli interessi dell'organizzazione come parte del processo di variazione o di cessazione del rapporto di lavoro.		
A.7.3.1	Cessazione o variazione delle responsabilità durante il rapporto di lavoro	*Controllo* Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o la variazione del rapporto di lavoro devono essere definiti, comunicati al personale o al collaboratore e resi effettivi.
A.8 Gestione degli asset		
A.8.1 Responsabilità per gli asset		
Obiettivo: Identificare gli asset dell'organizzazione e definire adeguate responsabilità per la loro protezione.		
A.8.1.1	Inventario degli asset	*Controllo* Tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni devono essere identificati; un inventario di questi asset deve essere compilato e mantenuto aggiornato.
A.8.1.2	Responsabilità degli asset	*Controllo* Gli asset censiti nell'inventario devono avere un responsabile.
A.8.1.3	Utilizzo accettabile degli asset	*Controllo* Le regole per l'utilizzo accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni devono essere identificate, documentate e attuate.
A.8.1.4	Restituzione degli asset	*Controllo* Tutto il personale e gli utenti di parti esterne devono restituire tutti gli asset dell'organizzazione in loro possesso al termine del periodo di impiego, del contratto o dell'accordo stipulato.

prospetto A.1 **Obiettivi di controllo e controlli** (Continua)

A.8.2 Classificazione delle informazioni		
Obiettivo: Assicurare che le informazioni ricevano un adeguato livello di protezione in linea con la loro importanza per l'organizzazione.		
A.8.2.1	Classificazione delle informazioni	*Controllo* Le informazioni devono essere classificate in relazione al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzate.
A.8.2.2	Etichettatura delle informazioni	*Controllo* Deve essere sviluppato e attuato un appropriato insieme di procedure per l'etichettatura delle informazioni in base allo schema di classificazione adottato dall'organizzazione.
A.8.2.3	Trattamento degli asset	*Controllo* Deve essere sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione adottato dall'organizzazione.
A.8.3 Trattamento dei supporti		
Obiettivo: Prevenire la divulgazione non autorizzata, la modifica, la rimozione o la distruzione delle informazioni archiviate sui supporti.		
A.8.3.1	Gestione dei supporti rimovibili	*Controllo* Devono essere sviluppate procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adottato dall'organizzazione.
A.8.3.2	Dismissione dei supporti	*Controllo* La dismissione dei supporti non più necessari deve avvenire in modo sicuro, attraverso l'utilizzo di procedure formali.
A.8.3.3	Trasporto dei supporti fisici	*Controllo* I supporti che contengono informazioni devono essere protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto.
A.9 Controllo degli accessi		
A.9.1 Requisiti di business per il controllo degli accessi		
Obiettivo: Limitare l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni.		
A.9.1.1	Politica di controllo degli accessi	*Controllo* Una politica di controllo degli accessi deve essere definita, documentata ed aggiornata sulla base dei requisiti di business e di sicurezza delle informazioni.
A.9.1.2	Accesso alle reti e ai servizi di rete	*Controllo* Agli utenti devono essere forniti solo degli accesi alle reti ed ai servizi di rete per il cui uso sono stati specificatamente autorizzati.
A.9.2 Gestione degli accessi degli utenti		
Obiettivo: Assicurare l'accesso agli utenti autorizzati e prevenire accessi non autorizzati a sistemi e servizi.		
A.9.2.1	Registrazione e de-registrazione degli utenti	*Controllo* Deve essere attuato un processo formale di registrazione e de-registrazione per abilitare l'assegnazione dei diritti di accesso.
A.9.2.2	Provisioning degli accessi degli utenti	*Controllo* Deve essere attuato un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi.
A.9.2.3	Gestione dei diritti di accesso privilegiato	*Controllo* L'assegnazione e l'uso di diritti di accesso privilegiato devono essere limitati e controllati.
A.9.2.4	Gestione delle informazioni segrete di autenticazione degli utenti	*Controllo* L'assegnazione di informazioni segrete di autenticazione deve essere controllata attraverso un processo di gestione formale.
A.9.2.5	Riesame dei diritti di accesso degli utenti	*Controllo* I responsabili degli asset devono riesaminare ad intervalli regolari i diritti di accesso degli utenti.
A.9.2.6	Rimozione o adattamento dei diritti di accesso	*Controllo* I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione.

prospetto A.1 **Obiettivi di controllo e controlli** (Continua)

A.9.3 Responsabilità dell'utente		
Obiettivo: Rendere gli utenti responsabili della salvaguardia delle loro informazioni di autenticazione.		
A.9.3.1	Utilizzo delle informazioni segrete di autenticazione	*Controllo* Gli utenti devono essere tenuti a seguire le prassi dell'organizzazione nell'uso di informazioni segrete di autenticazione.
A.9.4 Controllo degli accessi ai sistemi e alle applicazioni		
Obiettivo: Prevenire l'accesso non autorizzato a sistemi ed applicazioni.		
A.9.4.1	Limitazione dell'accesso alle informazioni	*Controllo* L'accesso a informazioni e funzioni di sistemi applicativi deve essere limitato secondo le politiche di controllo degli accessi.
A.9.4.2	Procedure di log-on sicure	*Controllo* Quando richiesto dalle politiche di controllo degli accessi, l'accesso a sistemi e applicazioni deve essere controllato da procedure di log-on sicure.
A.9.4.3	Sistema di gestione delle password	*Controllo* I sistemi di gestione delle password devono essere interattivi e devono assicurare password di qualità.
A.9.4.4	Uso di programmi di utilità privilegiati	*Controllo* L'uso di programmi di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema deve essere limitato e strettamente controllato.
A.9.4.5	Controllo degli accessi al codice sorgente dei programmi	*Controllo* Gli accessi al codice sorgente dei programmi devono essere limitati.
A.10 Crittografia		
A.10.1 Controlli crittografici		
Obiettivo: Assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni.		
A.10.1.1	Politica sull'uso dei controlli crittografici	*Controllo* Deve essere sviluppata e attuata una politica sull'uso dei controlli crittografici per la protezione delle informazioni.
A.10.1.2	Gestione delle chiavi	*Controllo* Deve essere sviluppata e attuata una politica sull'uso, sulla protezione e sulla durata delle chiavi crittografiche attraverso il loro intero ciclo di vita.
A.11 Sicurezza fisica e ambientale		
A.11.1 Aree sicure		
Obiettivo: Prevenire l'accesso fisico non autorizzato, danni e disturbi alle informazioni dell'organizzazione e alle strutture di elaborazione delle informazioni.		
A.11.1.1	Perimetro di sicurezza fisica	*Controllo* Si devono definire e usare dei perimetri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni.
A.11.1.2	Controlli di accesso fisico	*Controllo* Le aree di sicurezza devono essere protette da appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi.
A.11.1.3	Rendere sicuri uffici, locali e strutture	*Controllo* Deve essere progettata e applicata la sicurezza fisica agli uffici, ai locali ed agli impianti.
A.11.1.4	Protezione contro minacce esterne ed ambientali	*Controllo* Deve essere progettata e applicata un'adeguata protezione fisica da calamità naturali, attacchi malevoli o accidenti.
A.11.1.5	Lavoro in aree sicure	*Controllo* Devono essere progettate e attuate procedure per lavorare nelle aree sicure.
A.11.1.6	Aree di carico e scarico	*Controllo* I punti di accesso, come le aree di carico e scarico e altri punti attraverso i quali persone non autorizzate potrebbero accedere ai locali, devono essere controllati e, se possibile, isolati dalle strutture di elaborazione delle informazioni per evitare accessi non autorizzati.

prospetto A.1 **Obiettivi di controllo e controlli** (Continua)

A.11.2 Apparecchiature		
Obiettivo: Prevenire la perdita, il danneggiamento, il furto o la compromissione di asset e l'interruzione delle attività operative dell'organizzazione.		
A.11.2.1	Disposizione delle apparecchiature e loro protezione	*Controllo* Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato.
A.11.2.2	Infrastrutture di supporto	*Controllo* Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari.
A.11.2.3	Sicurezza dei cablaggi	*Controllo* I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi devono essere protetti da intercettazioni, interferenze o danneggiamenti.
A.11.2.4	Manutenzione delle apparecchiature	*Controllo* Le apparecchiature devono essere correttamente mantenute per assicurare la loro continua disponibilità e integrità.
A.11.2.5	Trasferimento degli asset	*Controllo* Apparecchiature, informazioni o software non devono essere portati all'esterno del sito senza preventiva autorizzazione.
A.11.2.6	Sicurezza delle apparecchiature e degli asset all'esterno delle sedi	*Controllo* Devono essere previste misure di sicurezza per gli asset all'esterno delle sedi dell'organizzazione, considerando i diversi rischi derivanti dall'operare all'esterno dei locali dell'organizzazione stessa.
A.11.2.7	Dismissione sicura o riutilizzo delle apparecchiature	*Controllo* Tutte le apparecchiature contenenti supporti di memorizzazione devono essere controllate per assicurare che ogni dato critico od il software concesso in licenza sia rimosso o sovrascritto in modo sicuro prima della dismissione o del riutilizzo.
A.11.2.8	Apparecchiature incustodite degli utenti	*Controllo* Gli utenti devono assicurare che le apparecchiature incustodite siano appropriatamente protette.
A.11.2.9	Politica di schermo e scrivania puliti	*Controllo* Devono essere adottate sia una politica di "scrivania pulita" per i documenti ed i supporti di memorizzazione rimovibili, sia una politica di "schermo pulito" per i servizi di elaborazione delle informazioni.
A.12 Sicurezza delle attività operative		
A.12.1 Procedure operative e responsabilità		
Obiettivo: Assicurare che le attività operative delle strutture di elaborazione delle informazioni siano corrette e sicure.		
A.12.1.1	Procedure operative documentate	*Controllo* Devono essere documentate e rese disponibili delle procedure operative a tutti gli utenti che le necessitano.
A.12.1.2	Gestione dei cambiamenti	*Controllo* I cambiamenti all'organizzazione, ai processi di business, alle strutture di elaborazione delle informazioni e ai sistemi che potrebbero influenzare la sicurezza delle informazioni devono essere controllati.
A.12.1.3	Gestione della capacità	*Controllo* L'uso delle risorse deve essere monitorato e messo a punto. Si devono fare proiezioni sui futuri requisiti di capacità per assicurare le prestazioni di sistema richieste.
A.12.1.4	Separazione degli ambienti di sviluppo, test e produzione	*Controllo* Gli ambienti di sviluppo, test e produzione devono essere separati per ridurre il rischio di accesso o cambiamenti non autorizzati all'ambiente di produzione.
A.12.2 Protezione dal malware		
Obiettivo: Assicurare che le informazioni e le strutture preposte alla loro elaborazione siano protette contro il malware.		
A.12.2.1	Controlli contro il malware	*Controllo* Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti.

prospetto A.1 **Obiettivi di controllo e controlli** (Continua)

A.12.3 Backup		
Obiettivo: Proteggere dalla perdita di dati.		
A.12.3.1	Backup delle informazioni	*Controllo* Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata.
A.12.4 Raccolta di log e monitoraggio		
Obiettivo: Registrare eventi e generare evidenze.		
A.12.4.1	Raccolta di log degli eventi	*Controllo* La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni deve essere effettuata, mantenuta e riesaminata periodicamente.
A.12.4.2	Protezione delle informazioni di log	*Controllo* Le strutture per la raccolta dei log e le informazioni di log devono essere protette da manomissioni e accessi non autorizzati.
A.12.4.3	Log di amministratori e operatori	*Controllo* Le attività degli amministratori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti e riesaminati periodicamente.
A.12.4.4	Sincronizzazione degli orologi	*Controllo* Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza devono essere sincronizzati rispetto a una singola sorgente temporale di riferimento.
A.12.5 Controllo del software di produzione		
Obiettivo: Assicurare l'integrità dei sistemi di produzione.		
A.12.5.1	Installazione del software sui sistemi di produzione	*Controllo* Devono essere attuate procedure per controllare l'installazione del software sui sistemi di produzione.
A.12.6 Gestione delle vulnerabilità tecniche		
Obiettivo: Prevenire lo sfruttamento di vulnerabilità tecniche.		
A.12.6.1	Gestione delle vulnerabilità tecniche	*Controllo* Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata e appropriate misure devono essere intraprese per affrontare i rischi relativi.
A.12.6.2	Limitazioni all'installazione del software	*Controllo* Devono essere stabilite e attuate regole per il governo dell'installazione del software da parte degli utenti.
A.12.7 Considerazioni sull'audit dei sistemi informativi		
Obiettivo: Minimizzare l'impatto delle attività di audit sui sistemi di produzione.		
A.12.7.1	Controlli per l'audit dei sistemi informativi	*Controllo* I requisiti e le attività di audit che prevedono una verifica dei sistemi di produzione devono essere attentamente pianificati e concordati per minimizzare le interferenze con i processi di business.
A.13 Sicurezza delle comunicazioni		
A.13.1 Gestione della sicurezza della rete		
Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.		
A.13.1.1	Controlli di rete	*Controllo* Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
A.13.1.2	Sicurezza dei servizi di rete	*Controllo* I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno.
A.13.1.3	Segregazione nelle reti	*Controllo* Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi.

prospetto A.1 **Obiettivi di controllo e controlli** (Continua)

A.13.2 Trasferimento delle informazioni		
Obiettivo: Mantenere la sicurezza delle informazioni trasferite sia all'interno di un'organizzazione sia con qualsiasi entità esterna.		
A.13.2.1	Politiche e procedure per il trasferimento delle informazioni	*Controllo* Devono esistere politiche, procedure e controlli formali a protezione del trasferimento delle informazioni attraverso l'uso di tutte le tipologie di strutture di comunicazione.
A.13.2.2	Accordi per il trasferimento delle informazioni	*Controllo* I trasferimenti sicuri di informazioni di business tra l'organizzazione e le parti esterne devono essere indirizzati in appositi accordi.
A.13.2.3	Messaggistica elettronica	*Controllo* Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato.
A.13.2.4	Accordi di riservatezza o di non divulgazione	*Controllo* I requisiti per gli accordi di riservatezza o di non divulgazione che riflettono le necessità dell'organizzazione per la protezione delle informazioni devono essere identificati, riesaminati periodicamente e documentati.
A.14 Acquisizione, sviluppo e manutenzione dei sistemi		
A.14.1 Requisiti di sicurezza dei sistemi informativi		
Obiettivo: Assicurare che la sicurezza delle informazioni sia parte integrante di tutto il ciclo di vita dei sistemi informativi. Questo include anche i requisiti specifici per i sistemi informativi che forniscono servizi attraverso reti pubbliche.		
A.14.1.1	Analisi e specifica dei requisiti per la sicurezza delle informazioni	*Controllo* I requisiti relativi alla sicurezza delle informazioni devono essere inclusi all'interno dei requisiti per i nuovi sistemi informativi o per l'aggiornamento di quelli esistenti.
A.14.1.2	Sicurezza dei servizi applicativi su reti pubbliche	*Controllo* Le informazioni coinvolte nei servizi applicativi che transitano su reti pubbliche devono essere protette da attività fraudolente, da dispute contrattuali, da divulgazioni e da modifiche non autorizzate.
A.14.1.3	Protezione delle transazioni dei servizi applicativi	*Controllo* Le informazioni coinvolte nelle transazioni dei servizi applicativi devono essere protette al fine di prevenire trasmissioni incomplete, errori di instradamento, alterazione non autorizzata di messaggi, divulgazione non autorizzata, duplicazione non autorizzata di messaggi o attacchi di tipo "replay".
A.14.2 Sicurezza nei processi di sviluppo e supporto		
Obiettivo: Assicurare che la sicurezza delle informazioni sia progettata ed attuata all'interno del ciclo di sviluppo dei sistemi informativi.		
A.14.2.1	Politica per lo sviluppo sicuro	*Controllo* Le regole per lo sviluppo del software e dei sistemi devono essere stabilite ed applicate agli sviluppi all'interno dell'organizzazione.
A.14.2.2	Procedure per il controllo dei cambiamenti di sistema	*Controllo* 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.
A.14.2.3	Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative	*Controllo* 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.
A.14.2.4	Limitazioni ai cambiamenti dei pacchetti software	*Controllo* La modifica dei pacchetti software deve essere disincentivata e limitata ai cambiamenti necessari; inoltre, tutti i cambiamenti devono essere strettamente controllati.
A.14.2.5	Principi per l'ingegnerizzazione sicura dei sistemi	*Controllo* I principi per l'ingegnerizzazione di sistemi sicuri devono essere stabiliti, documentati, manutenuti e applicati ad ogni iniziativa di implementazione di un sistema informativo.
A.14.2.6	Ambiente di sviluppo sicuro	*Controllo* Le organizzazioni devono definire e proteggere in modo appropriato ambienti di sviluppo sicuro per lo sviluppo dei sistemi e per le iniziative di integrazione che coprono l'intero ciclo di sviluppo dei sistemi.

prospetto A.1 **Obiettivi di controllo e controlli** (Continua)

A.14.2.7	Sviluppo affidato all'esterno	*Controllo* L'organizzazione deve supervisionare e monitorare l'attività di sviluppo dei sistemi affidata all'esterno.
A.14.2.8	Test di sicurezza dei sistemi	*Controllo* I test relativi alle funzionalità di sicurezza devono essere effettuati durante lo sviluppo.
A.14.2.9	Test di accettazione dei sistemi	*Controllo* Devono essere stabiliti dei programmi di test e di accettazione ed i criteri ad essi relativi per i nuovi sistemi informativi, per gli aggiornamenti e per le nuove versioni.
A.14.3 Dati di test		
Obiettivo: Assicurare la protezione dei dati usati per il test.		
A.14.3.1	Protezione dei dati di test	*Controllo* I dati di test devono essere scelti con attenzione, protetti e tenuti sotto controllo.
A.15 Relazioni con i fornitori		
A.15.1 Sicurezza delle informazioni nelle relazioni con i fornitori		
Obiettivo: Assicurare la protezione degli asset dell'organizzazione accessibili da parte dei fornitori.		
A.15.1.1	Politica per la sicurezza delle informazioni nei rapporti con i fornitori	*Controllo* I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset dell'organizzazione da parte dei fornitori devono essere concordati con i fornitori stessi e documentati.
A.15.1.2	Indirizzare la sicurezza all'interno degli accordi con i fornitori	*Controllo* Tutti i requisiti relativi alla sicurezza delle informazioni devono essere stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire componenti dell'infrastruttura IT per le informazioni dell'organizzazione.
A.15.1.3	Filiera di fornitura per l'ICT (Information and Comunication Technology)	*Controllo* Gli accordi con i fornitori devono includere i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni associati ai servizi e ai prodotti della filiera di fornitura per l'ICT.
A.15.2 Gestione dell'erogazione dei servizi dei fornitori		
Obiettivo: Mantenere un livello concordato di sicurezza delle informazioni ed erogazione dei servizi in linea con gli accordi con i fornitori.		
A.15.2.1	Monitoraggio e riesame dei servizi dei fornitori	*Controllo* Le organizzazioni devono regolarmente monitorare, riesaminare e sottoporre a audit l'erogazione dei servizi da parte dei fornitori.
A.15.2.2	Gestione dei cambiamenti ai servizi dei fornitori	*Controllo* I cambiamenti alla fornitura dei servizi da parte dei fornitori, incluso il mantenimento e il miglioramento delle attuali politiche, procedure e controlli per la sicurezza delle informazioni, devono essere gestiti, tenendo conto della criticità delle informazioni di business, dei sistemi e processi coinvolti e della rivalutazione dei rischi.
A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni		
A.16.1 Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti		
Obiettivo: Assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza.		
A.16.1.1	Responsabilità e procedure	*Controllo* Devono essere stabilite le responsabilità e le procedure di gestione per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni.
A.16.1.2	Segnalazione degli eventi relativi alla sicurezza delle informazioni	*Controllo* Gli eventi relativi alla sicurezza delle informazioni devono essere segnalati il più velocemente possibile attraverso appropriati canali gestionali.
A.16.1.3	Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni	*Controllo* Deve essere richiesto a tutto il personale ed ai collaboratori che utilizzano i sistemi informativi ed i servizi dell'organizzazione di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi.
A.16.1.4	Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni	*Controllo* Gli eventi relativi alla sicurezza devono essere valutati e deve essere deciso se classificarli come incidenti relativi alla sicurezza delle informazioni.

prospetto A.1 **Obiettivi di controllo e controlli** (Continua)

A.16.1.5	Risposta agli incidenti relativi alla sicurezza delle informazioni	*Controllo* Si deve rispondere agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate.
A.16.1.6	Apprendimento dagli incidenti relativi alla sicurezza delle informazioni	*Controllo* La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni deve essere utilizzata per ridurre la verosimiglianza o l'impatto degli incidenti futuri.
A.16.1.7	Raccolta di evidenze	*Controllo* L'organizzazione deve definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze.
A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa		
A.17.1 Continuità della sicurezza delle informazioni		
Obiettivo: La continuità della sicurezza delle informazioni deve essere integrata nei sistemi per la gestione della continuità operativa dell'organizzazione.		
A.17.1.1	Pianificazione della continuità della sicurezza delle informazioni	*Controllo* L'organizzazione deve determinare i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri.
A.17.1.2	Attuazione della continuità della sicurezza delle informazioni	*Controllo* L'organizzazione deve stabilire, documentare, attuare e mantenere processi, procedure e controlli per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa.
A.17.1.3	Verifica, riesame e valutazione della continuità della sicurezza delle informazioni	*Controllo* L'organizzazione deve verificare ad intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse.
A.17.2 Ridondanze		
Obiettivo: Assicurare la disponibilità delle strutture per l'elaborazione delle informazioni.		
A.17.2.1	Disponibilità delle strutture per l'elaborazione delle informazioni	*Controllo* Le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità.
A.18 Conformità		
A.18.1 Conformità ai requisiti cogenti e contrattuali		
Obiettivo: Evitare violazioni a obblighi cogenti o contrattuali relativi alla sicurezza delle informazioni e di qualsiasi requisito di sicurezza.		
A.18.1.1	Identificazione della legislazione applicabile e dei requisiti contrattuali	*Controllo* Per ogni sistema informativo e per l'organizzazione in generale si devono esplicitamente definire, documentare e mantenere aggiornati tutti i requisiti cogenti e contrattuali pertinenti, oltre all'approccio stesso dell'organizzazione per soddisfarli.
A.18.1.2	Diritti di proprietà intellettuale	*Controllo* Devono essere attuate delle procedure adeguate a garantire la conformità ai requisiti cogenti e contrattuali per l'uso del materiale sul quale potrebbero insistere diritti di proprietà intellettuale e per l'uso di prodotti software proprietari.
A.18.1.3	Protezione delle registrazioni	*Controllo* Le registrazioni devono essere protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato in conformità ai requisiti cogenti, contrattuali e di business.
A.18.1.4	Privacy e protezione dei dati personali	*Controllo* Si devono assicurare la privacy e la protezione dei dati personali, come richiesto dalla legislazione e dai regolamenti pertinenti, per quanto applicabile.
A.18.1.5	Regolamentazione sui controlli crittografici	*Controllo* I controlli crittografici devono essere utilizzati in conformità a tutti gli accordi, la legislazione e i regolamenti pertinenti.

prospetto A.1 **Obiettivi di controllo e controlli** (Continua)

A.18.2 Riesami della sicurezza delle informazioni		
Obiettivo: Assicurare che la sicurezza delle informazioni sia attuata e gestita in conformità alle politiche e alle procedure dell'organizzazione.		
A.18.2.1	Riesame indipendente della sicurezza delle informazioni	*Controllo* L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e la sua attuazione (ossia, gli obiettivi di controllo, i controlli, le politiche, i processi e le procedure per la sicurezza delle informazioni) devono essere riesaminati in modo indipendente ad intervalli pianificati oppure quando si verificano cambiamenti significativi.
A.18.2.2	Conformità alle politiche e alle norme per la sicurezza	*Controllo* I responsabili devono riesaminare regolarmente la conformità dei processi di elaborazione delle informazioni rispetto alle politiche, alle norme e a ogni altro requisito appropriato per la sicurezza.
A.18.2.3	Verifica tecnica della conformità	*Controllo* I sistemi informativi devono essere regolarmente riesaminati per conformità con le politiche e con le norme per la sicurezza dell'organizzazione.

BIBLIOGRAFIA

[1] ISO/IEC 27002:2013 Information Technology - Security Techniques - Code of practice for information security controls

[2] ISO/IEC 27003 Information technology - Security techniques - Information security management system implementation guidance

[3] ISO/IEC 27004 Information technology - Security techniques - Information security management - Measurement

[4] ISO/IEC 27005 Information technology - Security techniques - Information security risk management

[5] ISO 31000:2009 Risk management - Principles and guidelines

[6] ISO/IEC Directives, Part 1, Consolidated ISO Supplement - Procedures specific to ISO, 2012