Per conto di AICQ CN[1] - *Autore dr. Giovanni Mattana Presidente AICQ CentroNord*

PECULIARITÀ DELLA NORMA

Scopo della presente scheda è quello di attirare l'attenzione sull'importanza di questa norma e sintetizzarne i contenuti in modo molto schematico (la Norma si estende per 80 pagine).
La norma sarà presto pubblicata da UNI in lingua italiana.
Lo standard fornisce le 'best practices' per l'attuazione dei 'controls' (contromisure) descritti nell'Annex A della norma **ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements.**
L'insieme dei 'controls-contromisure' è riportato in questa norma nell'ordine in cui si trovano nella 27001-Annex A, ma sono strutturandoli secondo il seguente schema:

- **liv.1 Aree di controllo- (**Clauses**). Le Aree di controllo sono ripartite in Categorie di controllo**
- **liv.2 Categorie di controllo (obiettivi). Ogni Categorie di controllo è suddivisa in contromisure**
- **liv. 3 Contromisure- (**controls**).**

Il numero delle Aree di controllo è di 14, quello delle categorie è di 35, le contromisure sono 114.
Questa vastissima materia è raggruppata nei capitoli sotto indicati.
Di seguito si riportano le aree di controllo, le categorie ed le relative contromisure con la descrizione breve data dalla 27001-Annex A.
La *practice* riporta, per tutte le contromisure, come realizzarle: non si è riportato il testo per quelli più autoesplicativi. Dove si è ritenuto che la practice fosse particolarmente significativa, cioè chiarisse alcuni concetti non facilmente desumibili dall'Annex A-27001, si sono riportate alcune indicazioni dalla practice.

Contenuti

INDICAZIONI SINTETICHE

I capitoli 0 e 1 riprendono quanto anticipato sopra nel paragrafo 'peculiarità'.
I capitoli 2 e 3 rimandano esclusivamente alla ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary.
Il capitolo 4 tratta della struttura della norma, come sopra anticipato, definendo

- **4.1 Aree di controllo: Ogni area che definisce controlli di sicurezza contiene una o più categorie principali di sicurezza.**
- **4.2 Categorie di controlli**

Ogni categoria principale di controlli di sicurezza contiene:

a) **un obiettivo di controllo che dichiara cosa si vuole raggiungere;**
b) **uno o più controlli che possono essere applicati per raggiungere l'obiettivo di controllo.**

Le descrizioni dei controlli sono strutturate come segue:

Controllo-Definisce nello specifico il controllo, funzionale alla soddisfazione dell'obiettivo di controllo.

Guida attuativa-Fornisce informazioni più dettagliate per supportare l'attuazione del controllo e il raggiungimento degli obiettivi di controllo. La guida può non risultare completamente attinente o sufficiente in tutte le situazioni e potrebbe non soddisfare i requisiti specifici di controllo dell'organizzazione.

5 POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

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.
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.

Guida attuativa
Viene chiarito che esistono 2 livelli di policy

Al livello più alto, le organizzazioni dovrebbero definire una "politica per la sicurezza delle informazioni", approvata dalla direzione e che definisca l'approccio dell'organizzazione per la gestione dei propri obiettivi relativi alla sicurezza delle informazioni.

Ad un livello inferiore, la politica per la sicurezza delle informazioni dovrebbe essere sostenuta da politiche specifiche per argomento, che impongano ulteriormente l'attuazione degli obiettivi di controllo della sicurezza delle informazioni e che siano, in genere, realizzate per rispondere alle esigenze di determinati gruppi all'interno di un'organizzazione o per trattare argomenti specifici.

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.

6 ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

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.

6.1.1 Ruoli e responsabilità per la sicurezza delle informazioni

Controllo

Tutte le responsabilità relative alla sicurezza delle informazioni dovrebbero essere definite e assegnate.

Guida attuativa

Tutte le responsabilità relative alla sicurezza delle informazioni devono essere definite e assegnate.

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.

6.1.3 Contatti con le autorità: Controllo

Devono essere mantenuti appropriati contatti con le autorità pertinenti.

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.

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.

6.2 Dispositivi portatili e telelavoro

Obiettivo: Assicurare la sicurezza del telelavoro e nell'uso di dispositivi portatili.

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.

6.2.2 Telelavoro: Controllo

Devono essere attuate una politica e delle misure di sicurezza a suo supporto per proteggere le informazioni consultate, elaborate o memorizzate presso siti di telelavoro.

Guida attuativa

Le organizzazioni che permettono attività di telelavoro dovrebbero emettere una politica che definisca le condizioni e le limitazioni al telelavoro. Dove ritenuto applicabile e quando permesso dalla legge, i seguenti temi dovrebbero essere considerati:

- *a) il livello di sicurezza fisica del sito di telelavoro, considerando gli edifici e l'ambiente circostante;*
- *b) l'ambiente di telelavoro proposto;*
- *c) i requisiti per la sicurezza delle comunicazioni, tenendo in considerazione la necessità di accesso remoto ai sistemi interni dell'organizzazione, la criticità delle informazioni che dovranno essere accedute e che verranno trasmesse attraverso il canale di comunicazione, nonché la criticità del sistema interno;*
- *d) la fornitura di accesso in modalità desktop virtuale che prevenga l'elaborazione e la memorizzazione di informazioni su dispositivi privati;*
- *e) le minacce di accesso non autorizzato alle informazioni o alle risorse da parte di altri soggetti che frequentano il luogo, ad es. i famigliari e gli amici;*
- *f) l'uso di reti casalinghe e i requisiti o le limitazioni alla configurazione di servizi wireless di rete;*
- *g) le politiche e le procedure per prevenire discussioni riguardo i diritti per la proprietà intellettuale sviluppatisi su dispositivi privati;*

h) l'accesso a dispositivi privati (per verificare la sicurezza del sistema o durante un'indagine), che potrebbero essere proibiti dalla legge;
i) gli accordi di licenza del software tali per cui le organizzazioni potrebbero diventare responsabili per le licenze di software sulle workstation private di proprietà del personale o di utenti di terze parti;
j) le protezioni dal malware e i requisiti per l'uso di firewall.

7 SICUREZZA DELLE RISORSE UMANE

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.

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.
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.

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.
7.2.1 Responsabilità della direzione: controllo
La direzione deve richiedere a tutto il personale e ai collaborator di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite dall'organizzazione.
7.2.2 Consapevolezza, istruzione, formazione e addestramento della sicurezza delle informazioni: controllo.
Tutto il personale dell'organizzazione e, quando pertinente, il collaborator, devono ricevere un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa.
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.

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.
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.

8 GESTIONE DEGLI ASSET

8.1 **Responsabilità per gli asset**
Obiettivo: Identificare gli asset dell'organizzazione e definire adeguate responsabilità per la loro protezione.

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.
8.1.2 Responsabilità degli asset: Controllo
Gli asset censiti nell'inventario devono avere un responsabile.

Guida attuativa

Hanno la qualifica per essere indicati come responsabili degli asset i singoli individui e le entità per le quali è stata approvata una responsabilità di gestione per il ciclo di vita degli asset.

È attuato normalmente un processo per assicurare la tempestiva assegnazione della responsabilità degli asset. La responsabilità dovrebbe essere assegnata quando gli asset sono creati o quando sono trasferiti all'organizzazione. Il responsabile dell'asset dovrebbe essere responsabile della corretta gestione dello stesso lungo il suo intero ciclo di vita.

Il responsabile dell'asset dovrebbe:

a) assicurare che gli asset siano inventariati;
b) assicurare che gli asset siano appropriatamente classificati e protetti;
c) definire e riesaminare periodicamente i privilegi di accesso e la classificazione per gli asset più importanti, considerando le politiche di controllo degli accessi applicabili;
d) assicurare un corretto trattamento quando gli asset sono dismessi o distrutti.

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.

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.

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.

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.

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.

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.

8.3 Trattamento dei supporti

Obiettivo: Prevenire la divulgazione non autorizzata, la modifica, la rimozione o la distruzione delle informazioni archiviate sui supporti.

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.

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.

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.

9 CONTROLLO DEGLI ACCESSI

9.1 **Requisiti di business per il controllo degli accessi**

Obiettivo: Limitare l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni.

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.

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.

9.2 Gestione degli accessi degli utenti
Obiettivo: Assicurare l'accesso agli utenti autorizzati e prevenire accessi non autorizzati a sistemi e servizi.
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.
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.
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.
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.
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.
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.

9.3 Responsabilità dell'utente
Obiettivo: Rendere gli utenti responsabili della salvaguardia delle loro informazioni di autenticazione.
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.
Guida attuativa
Tutti gli utenti devono essere avvisati di:

a) *mantenere riservate le informazioni segrete di autenticazione, assicurandosi che non vengano divulgate a nessun'altra terza parte, incluso personale con autorità;*
b) *evitare di tenere una registrazione (ad esempio su carta, documenti software o dispositivi portatili) delle informazioni segrete di autenticazione, a meno che questa possa essere memorizzata in modo sicuro e il metodo di memorizzazione sia stato approvato (ad esempio una cassaforte software per le password);*
c) *modificare le informazioni segrete di autenticazione ogni qualvolta vi sia un'indicazione della loro possibile compromissione;etc.*

9.4 Controllo degli accessi ai sistemi e alle applicazioni
Obiettivo: Prevenire l'accesso non autorizzato a sistemi ed applicazioni.
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.
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.
9.4.3 Sistema di gestione delle password: Controllo
I sistemi di gestione delle password devono essere interattivi e devono assicurare password di qualità.
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.
9.4.5 Controllo degli accessi al codice sorgente dei programmi: Controllo
Gli accessi al codice sorgente dei programmi devono essere limitati.

10 CRITTOGRAFIA

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.
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.
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.

11 SICUREZZA FISICA E AMBIENTALE

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.
11.1.1 Perimetro di sicurezza fisica: Controllo
Si devono definire e usare dei perimetri di sicurezza per proteggere le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni.
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.
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.
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.
11.1.5 Lavoro in aree sicure: Controllo
Devono essere progettate e attuate procedure per lavorare nelle aree sicure.
Guida attuativa
Si dovrebbero prendere in considerazione le seguenti linee guida:

- *k) il personale dovrebbe essere a conoscenza dell'esistenza di un'area sicura, o delle attività che vi si svolgono, solo se necessario;*
- *l) il lavoro non supervisionato in aree sicure dovrebbe essere evitato, sia per ragioni di sicurezza che per prevenire opportunità di attività malevole;*
- *m) le aree sicure non presidiate dovrebbero essere fisicamente chiuse a chiave e periodicamente controllate; non dovrebbero essere consentite apparecchiature fotografiche, video, audio o altre apparecchiature di registrazione quali macchine fotografiche portatili, a meno che il loro uso non venga autorizzato.*

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.

11.2 Apparecchiature

Obiettivo: Prevenire la perdita, il danneggiamento, il furto o la compromissione di asset e l'interruzione delle attività operative dell'organizzazione.

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.
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.
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.
11.2.4 Manutenzione delle apparecchiature: Controllo
Le apparecchiature devono essere correttamente mantenute per assicurare la loro continua disponibilità e integrità.
11.2.5 Trasferimento degli asset: Controllo
Apparecchiature, informazioni o software non devono essere portati all'esterno del sito senza preventiva autorizzazione.
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.
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.
11.2.8 Apparecchiature incustodite degli utenti: Controllo
Gli utenti devono assicurare che le apparecchiature incustodite siano appropriatamente protette.

Guida attuativa

Tutti gli utenti dovrebbero essere sensibilizzati sui requisiti e sulle procedure di sicurezza per proteggere le apparecchiature incustodite, così come pure sulle loro responsabilità per l'attuazione di tale protezione. Gli utenti dovrebbero essere avvisati di:

a) chiudere le sessioni attive quando hanno completato l'attività, a meno che non possano essere protette da un appropriato meccanismo di bloccaggio, ad es. screen saver protetto da password;
b) effettuare il log-off da applicazioni o servizi di rete quando non più necessari;
c) proteggere il computer o i dispositivi mobili, quando non in uso, da un utilizzo non autorizzato con una chiusura a chiave o con un controllo equivalente, ad esempio una password di accesso.

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.

12 SICUREZZA DELLE ATTIVITÀ OPERATIVE

12.1 Procedure operative e responsabilità
Obiettivo: Assicurare che le attività operative delle strutture di elaborazione delle informazioni siano corrette e sicure.
12.1.1 Procedure operative documentate: Controllo
Devono essere documentate e rese disponibili delle procedure operative a tutti gli utenti che le necessitano.
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 influenzano la sicurezza delle informazioni devono essere controllati.
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.

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.

12.2 Protezione dal malware

Obiettivo: Assicurare che le informazioni e le strutture preposte alla loro elaborazione siano protette contro il malware.
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.

12.3 Backup

Obiettivo: Proteggere dalla perdita di dati**.**
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.

12.4 Raccolta di log e monitoraggio

Obiettivo: Registrare eventi e generare evidenze.
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.
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.
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.
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.

12.5 Controllo del software di produzione

Obiettivo: Assicurare l'integrità dei sistemi di produzione.
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.
Guida attuativa
Le seguenti linee guida dovrebbero essere considerate per controllare i cambiamenti del software sui sistemi di produzione:

a) *l'aggiornamento del software di produzione, delle applicazioni e delle librerie dovrebbe essere effettuato solo da amministratori formati ed addestrati, previa adeguata autorizzazione della direzione (vedere controllo 9.4.5);*
b) *sui sistemi di produzione dovrebbe essere presente solo codice eseguibile approvato e non codice di sviluppo o compilatori;*
c) *le applicazioni e i sistemi operativi dovrebbero essere installati solo dopo test estensivi e completati con successo; i test dovrebbero includere verifiche di usabilità, di sicurezza, sugli effetti su altri sistemi e di facilità d'uso e dovrebbero essere effettuati su sistemi separati (vedere controllo 12.1.4); dovrebbe essere inoltre assicurato che tutte le corrispondenti librerie di programmazione siano state aggiornate;*
d) *si dovrebbe utilizzare un sistema di controllo delle configurazioni per mantenere il controllo su tutto il software installato così come sulla documentazione di sistema;*
e) *dovrebbe essere presente una strategia di rollback preventiva all'implementazione dei cambiamenti;*
f) *dovrebbe essere mantenuto un log di audit di tutti gli aggiornamenti alle librerie di produzione;*
g) *le versioni precedenti dei software dovrebbero essere conservate come misura di contingenza;*

h) *le versioni obsolete del software dovrebbero essere archiviate assieme a tutte le informazioni richieste e ai parametri, alle procedure, alle configurazioni e ai software di supporto per tutto il tempo in cui i dati sono mantenuti archiviati.*

12.6 Gestione delle vulnerabilità tecniche
Obiettivo: Prevenire lo sfruttamento di vulnerabilità tecniche.
12.6.1 Gestione delle vulnerabilità tecniche: Control
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.
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.
12.7 Considerazioni sull'audit dei sistemi informativi Obiettivo: Minimizzare l'impatto delle attività di audit sui sistemi di produzione.
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.

13 SICUREZZA DELLE COMUNICAZIONI

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.
13.1.1 Controlli di rete: Controllo
Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
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.
13.1.3 Segregazione nelle reti: Controllo
Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi.

13.2 Trasferimento delle informazioni
Obiettivo: Mantenere la sicurezza delle informazioni trasferite sia all'interno di un'organizzazione sia con qualsiasi entità esterna.
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.
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
13.2.3 Messaggistica elettronica: Controllo
Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato.
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.

14 ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI

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.

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.
Guida attuativa
I requisiti per la sicurezza delle informazioni dovrebbero essere identificati utilizzando vari metodi, come la derivazione dei requisiti di conformità da regolamenti e politiche, dalla modellazione delle minacce e dai riesami degli incidenti, oppure tramite l'uso delle soglie di vulnerabilità. I risultati ottenuti dall'identificazione dei requisiti dovrebbero essere documentati e riesaminati da tutti gli stakeholder.
I requisiti ed i controlli per la sicurezza delle informazioni dovrebbero riflettere il valore per il business delle informazioni coinvolte (vedere categoria 8.2) e il potenziale impatto negativo sul business che potrebbe provenire dalla mancanza di un'adeguata sicurezza.
L'identificazione e la gestione di requisiti per la sicurezza delle informazioni e dei processi relativi dovrebbero essere integrati nelle fasi iniziali dei progetti relativi ai sistemi informativi. Le considerazioni preliminari per i requisiti relativi alla sicurezza delle informazioni, ad esempio nella fase di progettazione, possono condurre a soluzioni più economiche ed efficaci.
I requisiti per la sicurezza delle informazioni dovrebbero anche prendere in considerazione i seguenti punti:

a) *il livello di fiducia richiesto in ogni dichiarazione di identità degli utenti, al fine di dedurre i requisiti per la loro autenticazione;*
b) *il provisioning degli accessi e i processi di autorizzazione per utenti di business e per utenti privilegiati o tecnici;*
c) *la comunicazione, a utenti e operatori, dei loro compiti e delle loro responsabilità;*
d) *le necessità di protezione degli asset coinvolti, con particolare riguardo per la disponibilità, per la riservatezza e per l'integrità;*
e) *i requisiti derivanti da processi di business quali il monitoraggio e la raccolta di log delle transazioni nonché i requisiti per il non ripudio;*
f) *i requisiti richiesti da altri controlli di sicurezza, ad es. interfacce per la raccolta di log e il monitoraggio o sistemi di individuazione di fughe di informazioni.*

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.
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".

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.
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.
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.
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.
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.
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.
Guida attuativa
Le procedure per l'ingegnerizzazione sicura dei sistemi informativi basate sui principi di ingegneria della sicurezza dovrebbero essere stabilite, documentate ed applicate alle attività interne di progettazione dei sistemi informativi. La sicurezza dovrebbe essere progettata in tutti i livelli dell'architettura (funzionale, dati, applicazioni e tecnologia), bilanciando le necessità di sicurezza delle informazioni con le necessità di accessibilità. Le nuove tecnologie dovrebbero essere analizzate per valutarne i rischi di sicurezza e la progettazione dovrebbe essere riesaminata in relazione agli attacchi conosciuti.

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.
14.2.7 Sviluppo affidato all'esterno: Controllo
L'organizzazione deve supervisionare e monitorare l'attività di sviluppo dei sistemi affidata all'esterno
14.2.8 Test di sicurezza dei sistemi Controllo
I test relativi alle funzionalità di sicurezza devono essere effettuati durante lo sviluppo
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.

14.3 Dati di test
Obiettivo: Assicurare la protezione dei dati usati per il test.
14.3.1 Protezione dei dati di test : Controllo
I dati di test devono essere scelti con attenzione, protetti e tenuti sotto controllo.

15 RELAZIONI CON I FORNITORI
15.1 Sicurezza delle informazioni nelle relazioni con i fornitori
Obiettivo: Assicurare la protezione degli asset dell'organizzazione accessibili da parte dei fornitori.

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.
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.
15.1.3 Filiera di fornitura per l'ICT (Information and communication 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.

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.
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.
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.

16 GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI

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.

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.

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.

Guida attuativa

Il personale e i collaboratori dovrebbero essere resi consapevoli della propria responsabilità di segnalare il più velocemente possibile ogni evento relativo alla sicurezza delle informazioni. Essi dovrebbero anche essere consapevoli delle procedure per segnalare gli eventi relativi alla sicurezza delle informazioni e del punto di contatto al quale gli eventi dovrebbero essere segnalati.

Le situazioni da considerare per la segnalazione di eventi relativi alla sicurezza delle informazioni includono:

a) *i controlli di sicurezza inefficaci;*
b) *le violazioni delle aspettative di integrità, riservatezza o disponibilità delle informazioni;*
c) *gli errori umani;*
d) *le non conformità rispetto a politiche e linee guida;*
e) *le violazioni delle soluzioni di sicurezza fisica;*
f) *i cambiamenti non controllati dei sistemi;*
g) *i malfunzionamenti di software o hardware;*
h) *le violazioni di accesso.*

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.

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.

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.

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.

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.

17 ASPETTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI NELLA GESTIONE DELLA CONTINUITÀ OPERATIVA

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.

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.

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.
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.

17.2 Ridondanze

Obiettivo: Assicurare la disponibilità delle strutture per l'elaborazione delle informazioni.
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.

18 CONFORMITÀ

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.
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.
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.
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.
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.

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.

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.
18.2.1 Riesame indipendente della sicurezza delle informazioni: Controllo
L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e la sua attuazione (ovvero, 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.
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.
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.