IL NUOVO STANDARD ISO/IEC 27002 E IL SUO IMPATTO SULLE ORGANIZZAZIONI

La trasformazione digitale accelerata che le organizzazioni hanno subito negli ultimi anni ha avuto un impatto estremamente significativo sullo scenario di rischio che devono gestire, con una crescita significativa del cyber risk con sempre nuovi vettori di attacco volti sia a compromettere il patrimonio informativo, sia ad avere un vantaggio economico (es. attacchi ransomware).
Questo contesto ha fatto sì che, ai fini della protezione del patrimonio informativo, sia le misure di sicurezza informatica sia quelle di tipo tecnico organizzativo, abbiano assunto un peso significativamente maggiore.

ISO/IEC 27001, è lo standard di riferimento mondiale per la gestione della sicurezza di organizzazioni di tutti i tipi, indipendentemente dalle dimensioni o dal settore, a cui è strettamente legato lo standard ISO/IEC 27002 che è la linea guida su supporta le organizzazioni nell'implementare i controlli raccomandati a mitigazione dei rischi, facendo riferimento ai controlli nell'allegato A della ISO/IEC 27001.

ISO/IEC 27002 è una base di riferimento dettagliata per l'implementazione di questi controlli, ma non ha dei requisiti mandatori per la certificazione del Sistema di Gestione per la Sicurezza delle Informazioni.

Entrambi i principi attuali proposti dalle norme hanno l'ultima data di pubblicazione nel 2013, sebbene abbiano continuato ad essere rivisti periodicamente, mantenendo invariato il principio iniziale.
Tuttavia, la ISO/IEC 27002 è stata a lungo percepita come stagnante e molto spesso ridondante nei suoi controlli e non adattata al nuovo scenario affrontato dalle organizzazioni. Per tale ragione all'interno dei gruppi ISO sono state sviluppate una serie di norme che integravano per specifici settori i controlli previsti all'interno del citato standard (es. ISO/IEC 27017 per il cloud, ISO/IEC 2019 per le energy industries, ecc..)
Al fine di rendere maggiormente aderenti i controlli al mutato panorama internazionale di cybersecurity, una nuova versione della ISO/IEC 27002 è prevista all'inizio del 2022.

Nel corso degli anni, molte organizzazioni hanno ampliato per anni il proprio framework di controllo od aggiunto altri standard (es. Cobit, ITIL, CSF, NIST …) per migliorare gli aspetti della sicurezza delle informazioni che l'allegato A della ISO/IEC 27001 e ISO/IEC 27002 non ha affrontato in modo chiaro o diretto. Questo è un elemento importante della ISO/IEC 27001, che ha sempre consentito di ampliare la base dei controlli stabilita dall'allegato A, **che è un elenco di base da considerare**, ma sempre espandibile alla realtà e al contesto di ciascuna organizzazione *(cfr ISO/IEC 27001 - La lista di obiettivi di controllo e di controlli riportati nell'Allegato A non è esaustiva, e ulteriori obiettivi di controllo e controlli potrebbero essere necessari.)* .

Pertanto, questa nuova versione della ISO/IEC 27002 è pertinente e benvenuta, porterà naturalmente in un primo momento ad una revisione "minore" della ISO/IEC 27001 con la modifica dei soli controlli dell'allegato A senza modificare le clausole normative e verrà denominata - *"ISO/IEC 27001:2013/DAMD 1 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS — AMENDMENT 1". Anche questo aggiornamento è atteso per i primi mesi del 2022.*

Poiché ISO/IEC 27002 e ISO/IEC 27001 sono stati gli standard di riferimento per numerose normative e standard a livello internazionale, è naturale aspettarsi che nei prossimi anni verranno avviati diversi aggiornamenti al riguardo.

Un aspetto importante è evidenziato dal nuovo titolo della ISO/IEC 27002 che da "Tecnologie Informatiche - Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni" diventa

“Sicurezza delle informazioni, sicurezza informatica e protezione della privacy — Controlli sulla sicurezza delle informazioni” ampliando così a nuovi aspetti (cybersecurity, sicurezza del cloud e data protection …).

COSA CAMBIA NELLA NUOVA ISO/IEC 27002?

La principale differenza della nuova versione della norma e la versione 2013 è la struttura dell'insieme dei controlli. La maggior parte dei controlli ISO 27002 rimangono invariati, in alcuni casi compattati viste alcune ridondanze presenti nella precedente versione. I controlli sono stati raggruppati dai 14 domini precedenti a 4 "Argomenti" principali, a seconda di ciò a cui si riferisce il controllo.

La ISO/IEC 27002 nella nuova versione 2022 riassume l'insieme aggiornato di 93 misure di controllo della sicurezza (rispetto alle 114 previste nella versione precedente).

Non tutte le misure di controllo dettagliate nella nuova ISO/IEC 27002 sono rilevanti per ogni organizzazione, ma quando lo sono (quali misure di mitigazione del rischio), devono essere messe in atto affinché un’organizzazione sia conforme alla ISO/IEC 27001.

STRUTTURA DELLA NORMA

La nuova ISO/IEC 27002, mantenendo la storica numerazione, riporta i controlli in quattro capitoli (dal cap 5 al capitolo 8.

I nuovi quattro capitoli sono:

Controlli organizzativi	con 37 misure di controllo
Controlli delle Persone	con 8 misure di controllo
Controlli Fisici	con 14 misure di controllo
Controlli tecnologici	con 34 misure di controllo

Ogni misura di controllo nella ISO/IEC 27002: 2022 contiene indicazioni e suggerimenti di implementazione.

A loro volta, a ciascuna misura di controllo sono stati associati quattro attributi, che possono essere utilizzati per applicare diversi criteri di raggruppamento o filtraggio e generare diverse "viste" dei controlli.

Questa è davvero la novità maggiore dello standard che aiuta in maniera più puntuale a capire il significato del controllo e le modalità con cui lo stesso può essere utilizzato come misura di mitigazione del rischio.

Gli attributi definiti sono:

a) **Tipi di controllo** (#Preventivo, #Rilevazione #Correttivo) d

b) **Proprietà di sicurezza delle informazioni** (#Riservatezza, #Integrità, #Disponibilità)

c) **Concetti di sicurezza informatica** (#Identifica, #Proteggi, #Rileva, #Rispondi, #Recupera)

d) **Capacità operative** I valori degli attributi consistono #Governance, #Asset_Management, #Information_Protection, #Human_Resource_Security, #Physical_Security, #System_and_Network_Security, #Application_Security, #Secure_Configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity,

#Security_of_supplier_relationships, #Legal_compliance, #Information_security_event_management e #Information_security_assurance.

e) **Domini di sicurezza** (#Governance_ed_Ecosistema, #Protezione, #Difesa, #Resilienza).

Questi nuovi criteri di classificazione e filtraggio tornano alle tradizionali categorie di raggruppamento dei controlli di sicurezza che abbiamo visto nel corso dei decenni.
Anche il numero dei controlli è stato ridotto a 93, con l'introduzione di 11 nuovi controlli, la cancellazione di 1 controllo esistente, il consolidamento di 57 controlli precedenti in 24 attuali ed il mantenimento di 58 con la stessa denominazione.
La ISO/IEC 27002 includerà nuovi controlli relativi all'intelligence sulle minacce, ai servizi cloud ed allo sviluppo sicuro per riflettere la rapida evoluzione della tecnologia.
A un livello più ampio, ci sono modifiche alle normative relative alla protezione dei dati, in particolare alle informazioni di identificazione personale a livello internazionale.

Le principali differenze sono riassunte nella tabella seguente:

NUOVI CONTROLLI
5.7 Threat intelligence
5.23 Information security for use of cloud services
5.30 ICT readness for Business Continuity
7.4 Physical security monitoring
8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.16 Monitoring services
8.22 Web filtering
8.28 Secure coding
CONTROLLI RIMOSSI
11.2.5 – Removal of asset

Ora passiamo ad una breve analisi dei 93 controlli.

CONTROLLI ORGANIZZATIVI

Politiche per la sicurezza delle informazioni (5.1)
È necessario creare un documenti che contengano come l'organizzazione gestisce gli obiettivi di sicurezza delle informazioni. Nella passata edizione trovavamo questo controllo distribuito nelle varie aree dello standard. Questi documenti devono essere approvati dalla direzione e devono contenere politiche di alto e basso livello. Una volta che le politiche sono in atto, devono essere riviste regolarmente. L'approccio migliore a questo è quello di fissare almeno un incontro almeno annuale o meglio pianificare incontri extra nel periodo se la situazione lo richiede. Se vengono apportate modifiche, la direzione deve dare la propria approvazione. Le politiche dovrebbero essere condivise con gli stakeholder interni ed esterni.

Ruoli e responsabilità della sicurezza delle informazioni (5.2)
La politica deve definire chi è responsabile di quale attività, processo od attività a rischio per la sicurezza delle informazioni. È importante che il compito sia svolto in modo chiaro e per tutti i compiti. E' necessario assicurarsi che i ruoli e le responsabilità siano adatti all' organizzazione come anche previsto dalla clausola 5.3 dello standard ISO/IEC 27001.

Segregazione dei compiti (5.3)
Per prevenire qualsiasi uso improprio dei beni aziendali, il "potere" di controllare pienamente un'attività “critica” non dovrebbe spettare alla stessa persona. Il modo migliore per implementare questo controllo è registrare tutte le attività e dividere le attività importanti nell'esecuzione, nel controllo o nell'approvazione e nell'avvio. Ciò previene frodi ed errori.

Responsabilità di gestione (5.4)
La direzione deve assicurarsi che tutti i dipendenti e gli appaltatori siano a conoscenza e seguano la politica di sicurezza delle informazioni dell'organizzazione. Dovrebbero essere un esempio e dimostrare che la sicurezza delle informazioni è utile e necessaria.

Contatto con le autorità (5.5)
Dovrebbe essere chiaro chi è responsabile di contattare le autorità (ad es. forze dell'ordine, organismi di regolamentazione, autorità di vigilanza), quali autorità devono essere contattate (ad es. quale regione/paese) e in quali casi ciò deve avvenire. Una risposta rapida ed adeguata agli incidenti può ridurre notevolmente l'impatto e può anche essere obbligatoria per legge.

Contatto con gruppi di interesse speciale (5.6)
Per assicurarsi che le ultime tendenze in materia di sicurezza delle informazioni e le migliori pratiche siano mantenute al passo, il personale con compiti nel SGSI dovrebbe mantenere un buon contatto con gruppi di interesse speciale. Tali gruppi possono essere richiesti in alcuni casi per la consulenza di esperti ed essere un'ottima fonte per migliorare le proprie conoscenze. Esempi di tali gruppi sono IAPP, gruppo LinkedIn Information Security NL, Clusit, ISACA, ISC2 …

Intelligence sulle minacce (5.7)
Reagire alle minacce è ben poco per prevenire il loro primo verificarsi. Raccogliendo ed analizzando le informazioni sulle minacce per l’organizzazione, si ha un'idea migliore di quali meccanismi di protezione devono essere messi in atto per proteggere dalle minacce che sono rilevanti per l’organizzazione.

Sicurezza delle informazioni nella gestione dei progetti (5.8)
Per garantire un'implementazione di successo dell'SGSI a livello di organizzazione, la sicurezza delle informazioni dovrebbe essere considerata e documentata in tutti i progetti sotto forma di requisiti. Questi requisiti possono derivare da attività commerciali, legali e dalla conformità con altri standard o regolamenti. Se si dispone di manuali o modelli di gestione dei progetti, è necessario includere un capitolo sulla sicurezza delle informazioni.

Inventario di informazioni e altri beni associati (5.9)
L'organizzazione dovrebbe aver identificato tutte le informazioni e le risorse di elaborazione delle informazioni. Tutti i beni devono essere redatti in un inventario, che dovrebbe essere adeguatamente mantenuto. Conoscere quali risorse ci sono, la loro importanza, dove si trovano e come vengono gestite è essenziale per identificare e prevedere i rischi. Potrebbe anche essere obbligatorio per obblighi di legge o per scopi assicurativi.
Tutte le risorse nell'inventario, quindi l'intera azienda se l'inventario è completo, devono avere un proprietario (ovvero responsabile). Grazie alla proprietà delle risorse, le risorse vengono osservate e gestite durante l'intero ciclo di vita. Attività simili possono essere raggruppate e la supervisione quotidiana di un'attività può essere affidata a un cosiddetto custode, ma il proprietario rimane responsabile. La proprietà delle risorse deve essere approvata dalla direzione.

Uso accettabile delle informazioni e di altre risorse associate (5.10)
Dovrebbero esserci regole ben documentate per l'accesso alle risorse informative. Gli utenti della risorsa devono essere consapevoli dei requisiti di sicurezza delle informazioni relativi all'utilizzo della risorsa e seguirli.
Anche per la gestione dei beni dovrebbero essere in atto procedure. Il personale deve comprendere l'etichettatura delle risorse e sapere come gestire i diversi livelli di classificazione (vedi 5.12). Poiché non esiste uno standard universale per la classificazione, è anche importante conoscere i livelli di classificazione di altre parti, poiché molto probabilmente differiranno da quello dell'organizzazione.

Restituzione dei beni (5.11)
Quando un dipendente o una parte esterna non può più accedere a un bene a causa, ad esempio, della fine del rapporto di lavoro di un contratto, deve restituire il bene all'organizzazione. Ci dovrebbe essere una politica chiara per questo, che deve essere conosciuta da tutti i soggetti coinvolti. Le attività immateriali importanti per le operazioni correnti, come le conoscenze specifiche che non sono ancora documentate, devono essere documentate e restituite come tali.

Classificazione delle informazioni (5.12)
Alcune informazioni sono considerate sensibili a causa ad es empio del valore monetario o legale e deve rimanere confidenziale mentre altre informazioni sono meno cruciali. L'organizzazione dovrebbe disporre di una politica in atto su come gestire le informazioni classificate. La responsabilità di classificare le risorse informative spetta al suo proprietario. Per distinguere tra l'importanza di diverse attività classificate, può essere utile implementare diversi livelli di riservatezza da inesistenti a gravemente impattanti sulla sopravvivenza dell'organizzazione.

Etichettatura delle informazioni (5.13)
Non tutte le informazioni rientrano nella stessa categoria, come discusso nel precedente controllo. È quindi importante etichettare tutte le informazioni in base alla loro classificazione. Quando le informazioni vengono gestite, archiviate o scambiate può essere fondamentale conoscere la classificazione dell'oggetto. Purtroppo, questo può essere utile a persone malintenzionate, nonché una guida per oggetti interessanti. È importante essere consapevoli di questo rischio.

Trasferimento di informazioni (5.14)
Le informazioni sono condivise all'interno e all'esterno dell'organizzazione. Dovrebbe esserci un protocollo per tutti i tipi di condivisione delle informazioni, compresi i documenti digitali, i documenti fisici, i video, ma anche il passaparola. Regole chiare su come le informazioni possono essere condivise in sicurezza aiuta a ridurre il rischio di contaminazione e perdite di informazioni.
Le informazioni condivise tra l'organizzazione e le parti esterne devono essere precedute da un accordo di trasferimento delle informazioni. In questo modo, la fonte, il contenuto, la riservatezza, il mezzo di trasferimento e la destinazione del trasferimento di informazioni sono conosciuti e concordati da entrambe le parti.
La comunicazione aziendale avviene spesso tramite la messaggistica elettronica. Si consiglia alle organizzazioni di avere una panoramica dei tipi approvati di messaggistica elettronica e di documentare come questi sono protetti e possono essere utilizzati.

Controllo accessi (5.15)
Dovrebbe essere posta in atto una politica di controllo dell'accesso per definire come viene gestito l'accesso e chi è autorizzato ad accedere a cosa. Le regole per asset spettano ai proprietari degli asset, che stabiliscono requisiti, restrizioni e diritti per l'accesso al "loro" asset. I termini utilizzati di frequente in una politica di controllo dell'accesso sono necessità di conoscenza e necessità di utilizzo, dove il primo limita i diritti di accesso solo alle informazioni di cui un dipendente ha bisogno per svolgere il proprio compito e il secondo limita i diritti di accesso solo alle strutture di elaborazione delle informazioni necessario per svolgere il compito.

Gestione delle identità (5.16)
Per assegnare i diritti di accesso alle risorse e alle reti e tenere traccia di chi effettua effettivamente l'accesso, gli utenti devono essere registrati con un ID. Quando un dipendente lascia un'organizzazione, l'ID e l'accesso ad essa devono essere rimossi. Quando a un dipendente deve essere solo negato l'accesso, l'accesso dell'ID può essere limitato. Anche se l'utilizzo dell'ID di un altro dipendente potrebbe essere più rapido e facile per accedere a qualcosa, nella maggior parte dei casi ciò non dovrebbe essere consentito dalla direzione. L'ID di condivisione rimuove il collegamento tra una limitazione di accesso e un dipendente e rende quasi impossibile mantenere la persona giusta responsabile delle proprie azioni. L'assegnazione, la modifica e l'eliminazione di un'identità sono spesso chiamate ciclo di vita dell'identità.

Informazioni di autenticazione (5.17)
L'autenticazione segreta, come password e badge, deve essere gestita in un processo formale. Altre attività importanti che dovrebbero essere indicate nella politica sono, ad esempio, il divieto agli utenti di condividere informazioni di autenticazione segrete (es. password scritta su un post it sui monitor) , fornire ai nuovi utenti una password che deve essere modificata al primo utilizzo e fare in modo che tutti i sistemi autentichino un utente richiedendo l'autenticazione segreta dell'utente (password su PC, badge di accesso ….).
Se vengono utilizzati sistemi di gestione delle password, devono fornire password valide e seguire rigorosamente la politica delle informazioni di autenticazione segreta dell'organizzazione. Le password stesse devono essere archiviate e trasmesse in modo sicuro dal sistema di gestione delle password.

Diritti di accesso (5.18)
La direzione dovrebbe disporre di un sistema per la fornitura e la revoca dei diritti di accesso. Si consiglia di creare determinati ruoli in base alle attività svolte da determinati tipi di dipendenti e di concedere loro gli stessi diritti di accesso di base. Parte della presenza di un sistema ha ripercussioni sui tentativi di accesso non autorizzato. I dipendenti non hanno bisogno di cercare di accedere a luoghi che non dovrebbero, poiché i diritti di accesso possono essere facilmente richiesti al proprietario e/o alla direzione del bene.
Le organizzazioni e i loro dipendenti non sono statici. I ruoli cambiano o i dipendenti lasciano l'azienda, cambiando continuamente le esigenze di accesso. I proprietari delle risorse dovrebbero verificare regolarmente chi può accedere alla loro risorsa, mentre il cambio di ruolo o l'abbandono dovrebbe attivare una revisione dei diritti di accesso da parte della direzione. Poiché i diritti di accesso privilegiato sono più sensibili, dovrebbero essere riesaminati più spesso. Una volta che un contratto o un accordo è stato risolto, i diritti di accesso della parte ricevente dovrebbero essere rimossi.

Sicurezza delle informazioni nei rapporti con i fornitori (5.19)
Poiché i fornitori hanno accesso a determinate risorse, le organizzazioni devono stabilire una politica che indichi i requisiti per la mitigazione del rischio e misure di governo e controllo. Questa politica e queste misure devono essere comunicate ai fornitori e concordate. Esempi di tali requisiti sono i processi logistici predeterminati, gli obblighi di un processo di incidente per entrambe le parti, gli accordi di non divulgazione e la documentazione del processo di fornitura.

Affrontare la sicurezza delle informazioni negli accordi con i fornitori (5.20)
Ogni fornitore che in qualsiasi modo, direttamente o indirettamente, entra in contatto con le informazioni dell'organizzazione deve seguire i requisiti di sicurezza delle informazioni stabiliti ed accettarli. Esempi sono i requisiti sulla classificazione delle informazioni, sull'uso accettabile e sui diritti di audit. Un aspetto facilmente dimenticato di un accordo è cosa fare quando il fornitore non può o non vuole più fornire. È importante implementare una clausola in tal senso.

Gestire la sicurezza delle informazioni nella filiera ICT (5.21)
Gli accordi con i fornitori dovrebbero inoltre indicare i requisiti di sicurezza delle informazioni e gli accordi sui servizi ICT e la catena di approvvigionamento. Esempi di requisiti inclusi sono la necessità di essere in grado di seguire gli articoli lungo la catena di approvvigionamento e il mantenimento di un certo livello minimo di sicurezza a ogni livello della "catena".

Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori (5.22)
Tutti commettono errori, anche i fornitori. Indipendentemente dal fatto che l'errore sia accaduto per caso o deliberatamente, il risultato è lo stesso: l'organizzazione non riceve esattamente ciò che è stato concordato e la fiducia può diminuire. Per questo motivo, le organizzazioni dovrebbero tenere d'occhio i fornitori e controllarli dove ritenuto necessario. In questo modo, un'organizzazione è consapevole quando un fornitore fa qualcosa fuori dall'ordinario.
Proprio come con le modifiche al sistema, la direzione deve controllare tutte le modifiche ai servizi dei fornitori. Devono assicurarsi che le politiche di sicurezza delle informazioni siano aggiornate e che eventuali modifiche nella fornitura del servizio stesso siano gestite. Un piccolo cambiamento nel servizio fornito combinato con una politica di sicurezza delle informazioni obsoleta potrebbe comportare un nuovo grande rischio. Possono verificarsi facilmente cambiamenti dal lato del fornitore, ad esempio quando il servizio viene migliorato, viene fornita una nuova app o sistema o cambiano le politiche e le procedure del fornitore.

Sicurezza delle informazioni per l'utilizzo dei servizi cloud (5.23)
I fornitori di cloud offrono un servizio che, quando è in uso, è il più delle volte una parte vitale dell'infrastruttura di un'organizzazione. I documenti di Office sono archiviati nel cloud, ma molti provider SaaS offrono il loro prodotto ai propri clienti tramite un provider cloud come Amazon AWS, Microsoft Azure o Google Cloud.
I rischi che circondano questa parte critica dell'organizzazione dovrebbero essere adeguatamente mitigati. Le organizzazioni dovrebbero disporre di processi per l'utilizzo, la gestione e l'abbandono (strategia di uscita) di un cloud utilizzato. La rottura dei legami con un provider cloud spesso significa che un nuovo provider cloud è all'orizzonte, quindi non bisogna nemmeno dimenticare il controllo degli acquisti e l'onboarding su un nuovo cloud. Proprio come qualsiasi altro software di terze parti, un nuovo ambiente cloud dovrebbe consentire di mantenere il livello di sicurezza delle informazioni desiderato, senza comprometterlo.

NOTA – ad integrazione di questo controllo rimangono validi i controlli aggiuntivi previsti all'interno degli standard ISO/IEC 27017 e ISO/IEC 27018

Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni (5.24)
Le organizzazioni devono creare e documentare procedure per gli incidenti di sicurezza delle informazioni e chi è responsabile di cosa. In questo modo, se si verifica un incidente di sicurezza delle informazioni, può essere gestito in modo efficace e rapido. Gli incidenti di sicurezza si verificano inaspettatamente e possono causare un certo caos, che può essere mitigato disponendo di un protocollo seguito da personale esperto e formato.

Valutazione e decisione sugli eventi di sicurezza delle informazioni (5.25)
Le organizzazioni dovrebbero disporre di un metodo di valutazione ben documentato per gli incidenti di sicurezza. Quando si verifica un evento sospetto, la persona responsabile deve testare l'evento rispetto ai requisiti e determinare se si è verificato un incidente di sicurezza delle informazioni effettivo. I risultati di questa valutazione dovrebbero essere documentati, in modo che possano essere utilizzati come riferimento futuro.

Risposta agli incidenti di sicurezza delle informazioni (5.26)
Questo punto sembra semplice, ma è comunque importante da menzionare e talvolta difficile attuare nella pratica. Una volta che si verifica un incidente di sicurezza delle informazioni, è necessario rispondere seguendo le procedure di impostazione da parte del personale incaricato. Le azioni predeterminate dovrebbero essere intraprese e l'intero processo accuratamente documentato. Questo aiuta a prevenire eventi futuri ed eliminare le relative vulnerabilità di sicurezza.

Imparare dagli incidenti di sicurezza delle informazioni (5.27)
Anche se gli incidenti sono indesiderati, hanno comunque un grande valore. Le conoscenze acquisite dalla risoluzione di un incidente dovrebbero essere utilizzate per prevenire incidenti simili in futuro e possono aiutare ad identificare un possibile problema sistematico. Con controlli aggiuntivi, è importante tenere d'occhio i costi; un nuovo controllo non dovrebbe costare all'organizzazione su base annuale più degli incidenti che mitiga.

Raccolta delle prove (5.28)
Una volta che si verifica un incidente, la causa di solito non è immediatamente chiara. Quando la causa è un individuo o un'organizzazione, dovrebbero essere disciplinati in base all'intenzione ed all'effetto. Per collegare un incidente a una causa, è necessario raccogliere prove. In caso di un'azione dannosa, questa prova ed il modo in cui è stata ottenuta potrebbero essere utilizzati in procedimenti legali. Per prevenire la distruzione accidentale o deliberata delle prove, dovrebbe esistere una procedura di identificazione delle prove chiara e sicura.

Sicurezza delle informazioni durante l'interruzione (5.29)
Le organizzazioni dovrebbero determinare i propri requisiti per la continuità della sicurezza delle informazioni in caso di crisi. La scelta più semplice è riprendere le attività standard di sicurezza delle informazioni nel miglior modo possibile in una situazione avversa. Una volta che i requisiti sono stati determinati e concordati nella gestione, è necessario mettere in atto procedure, piani e controlli per riprendere con un livello accettabile di sicurezza delle informazioni in caso di crisi.
Man mano che le organizzazioni cambiano, cambia anche il modo migliore per rispondere a una crisi. Un'organizzazione che, ad esempio, ha raddoppiato le sue dimensioni entro un anno molto probabilmente beneficerà di una risposta diversa rispetto all'anno precedente. Per questo motivo, la continuità della sicurezza delle informazioni va controllata regolarmente.

Prontezza ICT per la continuità aziendale (5.30)
Durante la pianificazione della Business Continuity, è necessario prestare particolare attenzione agli scenari in cui i sistemi IT si possono guastare. Dovrebbe esserci una strategia chiara su come verranno ripristinati i sistemi, chi lo farà e quanto tempo potrebbe impiegare. Dovrebbe anche essere chiaro cosa significa "ripristino" in uno scenario specifico, dal momento che avere solo i sistemi principali in esecuzione è probabile che sia sufficiente per la prima settimana dopo un completo tracollo.

NOTA – Rispetto alla versione precedente, viene meglio chiarito che ai fini della sicurezza delle informazioni è necessario considerare gli aspetti di supporto ICT in caso di eventi che possono compromettere la continuità aziendale. La norma non richiede un modello di Business Continuity di cui allo standard 22301, ma che l'ICT sia a supporto della continuità aziendale

Individuazione dei requisiti legali, statutari, regolamentari e contrattuali (5.31)
I requisiti provengono da tutti i luoghi e devono essere soddisfatti. Le organizzazioni dovrebbero quindi avere una panoramica di tutti i requisiti relativi alla sicurezza delle informazioni che devono rispettare e di come farlo. Poiché i requisiti possono cambiare o essere aggiunti, la panoramica della conformità dei requisiti deve essere aggiornata. Nell'analisi del contesto che l'organizzazione fa (cfr req. 4.1 dello standard ISO/IEC 27010) dovrebbero sempre quindi esse analizzate le normative applicabili.
Un esempio di cambiamento dei requisiti è quando la tua organizzazione si espande in un nuovo paese in un altro continente. È probabile che questo paese abbia leggi diverse sulla privacy, sull'archiviazione delle informazioni e sulla crittografia.

Diritti di proprietà intellettuale (5.32)
I diritti di proprietà intellettuale, anch'essi parte della conformità legale, sono un'area che merita un'attenzione speciale. La Proprietà Intellettuale può essere di grande valore, quindi è importante documentare la propria proprietà intellettuale ed anche l'uso della proprietà intellettuale di altri. Un uso errato (accidentale) della Proprietà Intellettuale di altri può dar luogo a grandi cause legali e dovrebbe essere prevenuto a tutti i costi.

Protezione delle registrazioni (5.33)
Tutte le registrazioni, siano essi registrazioni contabili o di controllo, dovrebbero essere protetti. Le registrazioni sono a rischio di perdita, compromissione o accesso non autorizzato. I requisiti per la protezione della documentazione potrebbero provenire dall'organizzazione stessa o da altre fonti come la legislazione o le compagnie assicurative. Per questo, dovrebbero essere create e seguite linee guida rigorose.

Privacy e protezione delle informazioni di identificazione personale (PII) (5.34)
A seconda del paese o dello spazio economico in cui si trova un'organizzazione, potrebbero essere applicate normative diverse sulla protezione dei dati personali. Alle organizzazioni situate nell'UE e/o che trattano dati personali dei cittadini dell'UE, si applica il Regolamento generale sulla protezione dei dati (GDPR). Le organizzazioni devono assicurarsi di essere a conoscenza dei requisiti stabiliti da tale legislazione e seguirla religiosamente. Il GDPR, ad esempio, impone la conduzione di accordi sul trattamento dei dati, la tenuta di un registro delle attività di trattamento e la trasparenza del trattamento dei dati. (NdR in Cina è operativo dallo scorso anno il PIPL).

NOTA – ad integrazione di questo controllo rimangono validi i controlli aggiuntivi previsti all'interno degli standard ISO/IEC 27018 e ISO/IEC 27701.

Revisione indipendente della sicurezza delle informazioni (5.35)
È impossibile per le organizzazioni rivedere obiettivamente il proprio sistema di sicurezza delle informazioni. Per questo motivo, le organizzazioni dovrebbero far controllare la sicurezza delle informazioni da una parte indipendente su base regolare o quando si verificano grandi cambiamenti. Ciò mantiene la visione di un'organizzazione della sicurezza delle informazioni corretta e trasparente. Una parte indipendente può essere anche un auditor interno a tempo pieno, che ha il solo compito di svolgere le verifiche interne e non ha altri compiti e responsabilità contrastanti.

Conformità alle politiche e agli standard per la sicurezza delle informazioni (5.36)
Con tutte queste politiche, standard e procedure di sicurezza, è importante che i manager esaminino regolarmente se le attività e/o i processi di cui sono responsabili sono completamente conformi. Affinché ciò avvenga correttamente, dovrebbero essere a conoscenza esattamente di quali regole e requisiti devono rispettare e verificarli manualmente o con uno strumento di reporting automatico.
Anche i sistemi informativi devono essere regolarmente rivisti per verificarne la conformità. Il modo più semplice e generalmente più conveniente per farlo è per mezzo di strumenti automatizzati. Questo strumento può controllare rapidamente tutte le sfacettaure di un sistema e segnalare esattamente cosa è andato / potrebbe andare storto. I test di vulnerabilità come i test di penetrazione possono mostrare in modo efficace eventuali punti deboli, ma potrebbero effettivamente danneggiare il sistema se eseguiti senza cautela.

Procedure operative documentate (5.37)
Le procedure per l'utilizzo delle apparecchiature devono essere documentate e messe a disposizione di coloro che utilizzano le apparecchiature. Dalla semplice procedura di utilizzo del computer (dall'avvio allo spegnimento) all'utilizzo di apparecchiature più complicate dovrebbe esserci una guida su come utilizzarle in modo sicuro e corretto. Data la loro importanza, le procedure dovrebbero essere trattate come documenti formali, il che significa che qualsiasi modifica dovrebbe essere approvata dalla direzione.

CONTROLLI DELLE PERSONE

Selezione del personale - Screening (6.1)
Un sistema di gestione della sicurezza delle informazioni necessita di una politica per lo screening di tutti i dipendenti nuovi o promossi, compresi i consulenti e il personale temporaneo. Questo per garantire che i dipendenti siano competenti e affidabili. La politica deve tenere conto sia della legislazione e dei regolamenti locali sia del ruolo del nuovo dipendente per garantire che lo screening sia sufficiente ma non sproporzionato. Alcuni ruoli all'interno di un'organizzazione possono richiedere un livello di screening più elevato, ad esempio se i dipendenti gestiranno informazioni riservate. In particolare per i ruoli di sicurezza delle informazioni, lo screening dovrebbe includere anche le competenze e l'affidabilità necessarie, e ciò dovrebbe essere documentato di conseguenza.

Termini e condizioni di lavoro (6.2)
Prima di iniziare il lavoro, il dipendente deve essere a conoscenza della politica di sicurezza delle informazioni dell'organizzazione, inclusi i ruoli e le responsabilità di sicurezza delle informazioni. Questo potrebbe essere comunicato tramite un codice di condotta firmato o un metodo simile. I contratti dei dipendenti dovrebbero includere anche la politica di sicurezza delle informazioni pertinente dell'organizzazione, incluso un accordo di riservatezza se il dipendente avrà accesso a informazioni riservate.

Consapevolezza, istruzione e formazione in materia di sicurezza delle informazioni (6.3)
I dipendenti hanno bisogno di una formazione sulla sicurezza delle informazioni quando entrano a far parte nei ruoli dell'organizzazione. Anche il personale in servizio da più tempo deve mantenere la propria consapevolezza con una formazione e una comunicazione regolari. La formazione deve essere pertinente al ruolo. Per molti dipendenti, ciò includerà nozioni di base come promemoria sulla sicurezza delle password ed attacchi di ingegneria sociale. Per il personale tecnico o per coloro che gestiscono materiale riservato sarà richiesta una formazione più approfondita per il proprio ruolo specifico.

Processo disciplinare (6.4)
Dovrebbe essere in atto una politica per il processo disciplinare a seguito di una violazione confermata della politica di sicurezza delle informazioni. Il procedimento disciplinare deve essere proporzionato e graduato, con azioni che dipendono dalla gravità dell'incidente, dall'intenzione, dalla recidiva e, soprattutto, dall'adeguata formazione del dipendente. Molti incidenti di sicurezza registrati saranno il risultato di una violazione delle norme e dovrebbero portare ad un'azione disciplinare. Questo è importante da ricordare perché il personale dovrebbe evitare di segnalare incidenti di sicurezza per paura di azioni disciplinari.

Responsabilità dopo la cessazione o il cambio di rapporto di lavoro (6.5)
Le responsabilità in materia di sicurezza delle informazioni non cessano quando il rapporto di lavoro viene modificato o terminato. I termini e le condizioni di lavoro del dipendente devono contenere accordi di riservatezza, che richiedono al dipendente di rispettare la riservatezza delle informazioni dopo aver lasciato l'organizzazione. Quando un dipendente lascia, può anche lasciare vacanti i ruoli di sicurezza delle informazioni. Per mantenere la continuità della sicurezza, la direzione deve identificare questi ruoli in modo che possano essere trasferiti.

Riservatezza o accordi di riservatezza (6.6)
Se la riservatezza delle informazioni è sufficientemente elevata, potrebbe essere necessario proteggerla da termini legalmente applicabili. In questo caso possono essere utilizzati accordi di riservatezza, stabilendo le informazioni coperte, le responsabilità di tutte le parti, la durata dell'accordo e le sanzioni in caso di violazione dell'accordo. Questi proteggono le informazioni dalla divulgazione dopo che il dipendente ha lasciato l'organizzazione per un determinato periodo di tempo.

Lavoro a distanza (6.7)
Il lavoro a distanza è diventato uno standard in molte organizzazioni, offrendo maggiore flessibilità sia alle organizzazioni che ai dipendenti. Vi sono tuttavia implicazioni sulla sicurezza delle informazioni per il lavoro a distanza, che dovrebbero essere considerate e documentate. La politica di lavoro a distanza dovrebbe delineare dove e quando il lavoro a distanza è consentito, la fornitura di dispositivi e attrezzature, l'accesso autorizzato e quali informazioni possono essere raggiunte da remoto. Di particolare importanza sono le politiche che regolano l'uso di reti sconosciute e il rischio che amici, familiari o estranei possano sentire o vedere informazioni riservate.

Segnalazione di eventi di sicurezza delle informazioni (6.8)
I dipendenti a volte incappano in incidenti di sicurezza delle informazioni durante il loro lavoro quotidiano. Gli incidenti possono includere errori umani, violazioni della riservatezza, malfunzionamenti, sospette infezioni da malware e non conformità con la politica di sicurezza delle informazioni o la legge. Il primo passo per identificare, correggere e prevenire il ripetersi degli incidenti è la segnalazione. I dipendenti hanno quindi bisogno di un canale di rendicontazione e di essere consapevoli della sua esistenza.

CONTROLLI FISICI

Perimetro di sicurezza fisica (7.1)
Il primo passo per proteggere uno spazio fisico è definirne il perimetro. Si possono quindi individuare aree sensibili o critiche all'interno del perimetro. Il perimetro deve essere sufficientemente sicuro fisicamente per proteggere il contenuto, con allarmi e sistemi di rilevamento degli intrusi.

Controlli fisici all'ingresso (7.2)
Solo le persone autorizzate dovrebbero poter accedere a beni ed informazioni. Il livello delle restrizioni dipende dai requisiti organizzativi. Le cose da considerare includono l'identificazione personale e la registrazione di chi accede ai locali. Dovrebbe essere in atto una procedura per ricevere i visitatori per stabilire la loro identità, dove possono andare e se devono essere accompagnati. Anche le consegne presentano un rischio, sia perché le aree di consegna devono essere protette sia per impedire al personale di consegna di entrare in aree riservate.

Messa in sicurezza di uffici, locali e strutture (7.3)
Gli uffici devono essere protetti con chiavi digitali o fisiche. In generale, directory e mappe dettagliate non dovrebbero essere apertamente accessibili in quanto possono evidenziare la posizione di risorse sensibili.

Monitoraggio della sicurezza fisica (7.4)
Questo nuovo controllo incoraggia il monitoraggio dei locali fisici al fine di scoraggiare gli intrusi e rilevare eventuali intrusioni. Guardie, telecamere ed allarmi controllano tutti contro l'accesso non autorizzato. La progettazione di qualsiasi sistema di monitoraggio dovrebbe essere considerata confidenziale. Sono necessari test regolari per garantire che il sistema funzioni. I sistemi di sorveglianza con telecamera ed altri sistemi di monitoraggio che raccolgono informazioni personali o possono essere utilizzati per tracciare le persone possono richiedere un'attenzione speciale ai sensi delle leggi sulla protezione dei dati. Ad esempio, la sorveglianza delle telecamere potrebbe richiedere una valutazione dell'impatto sulla protezione dei dati ai sensi della legislazione GDPR.

Protezione contro le minacce fisiche e ambientali (7.5)
I disastri naturali o causati dall'uomo e gli attacchi fisici minacciano la sicurezza delle informazioni e la continuità aziendale. Il livello di questi rischi dipende fortemente dalla posizione. Inondazioni, incendi e grandi tempeste sono i rischi più probabili, ma nelle valutazioni del rischio possono essere presi in considerazione anche i rischi derivanti da terremoti, disordini civili e attacchi terroristici.

Lavorare in aree sicure (7.6)
L'esistenza e lo scopo di ambienti sicuri dovrebbero essere condivisi solo in base alla necessità di conoscenza. Pertanto gli ambienti sicuri dovrebbero essere tenuti chiusi, con accesso limitato alle persone autorizzate. In generale, il lavoro solitario dovrebbe essere scoraggiato, sia per motivi di sicurezza che per motivi di protezione.

Scrivania e schermo puliti (7.7) Politica di schermo e scrivania puliti
Chiunque può accedere alle informazioni riservate lasciate su scrivanie, schermi, stampanti e lavagne. una chiara politica della scrivania e dello schermo definisce come e dove è possibile accedere alle informazioni. Una politica di base non include documenti stampati lasciati incustoditi, né nelle aree di lavoro né nelle stampanti e sugli schermi dei dispositivi bloccati. Potrebbero essere necessarie politiche più dettagliate per le informazioni riservate, ad esempio che le informazioni non possono essere visualizzate su uno schermo in un ambiente aperto.

Localizzazione e protezione delle apparecchiature (7.8)
Un'attenta citazione delle apparecchiature può ridurre al minimo una serie di rischi: non solo l'accesso non autorizzato, ma anche i rischi dovuti a fattori ambientali, cibo e bevande versati, atti vandalici e degrado dovuto alla luce o all'umidità. La protezione richiesta dipenderà dalla sensibilità dell'apparecchiatura.

Sicurezza degli asset fuori sede (7.9)
I dispositivi, inclusi i dispositivi privati (bring-your-own-devices), necessitano ancora di protezione quando lasciano i locali. Le basi includono un'adeguata protezione fisica come coperture assicurative e prevenzione dei furti non lasciando i dispositivi incustoditi. L'organizzazione deve essere a conoscenza di quali dispositivi vengono utilizzati fuori sede, da chi e quali informazioni vengono consultate o utilizzate fuori sede.

Supporti di memorizzazione (7.10)
Le informazioni archiviate in qualsiasi formato multimediale comportano il rischio di accesso non autorizzato e di perdita dell'integrità delle informazioni a causa di modifiche o degrado, perdita, distruzione o rimozione. I supporti dovrebbero quindi essere conservati in modo sicuro e infine distrutti in modo sicuro. Le politiche che disciplinano la gestione dei supporti rimovibili dovrebbero riguardare quali informazioni possono essere archiviate su supporti rimovibili, la registrazione e il tracciamento di tali supporti, come dovrebbero essere archiviati in modo sicuro per prevenire l'accesso o il degrado non autorizzati e come dovrebbero essere trasportati. Quando l'archiviazione non è più necessaria, è necessaria la distruzione sicura. Questo può essere eseguito da una parte esterna.

Utilità di supporto (7.11)
Le interruzioni di corrente possono compromettere immediatamente le attività di un'azienda. Meno ovviamente, le telecomunicazioni e l'aria condizionata interromperanno tutte le attività digitali e i guasti alle forniture di gas, fognature o acqua impediranno ai dipendenti di lavorare in loco. I sistemi di ispezione e di allarme possono identificare guasti effettivi o potenziali. I piani di continuità dovrebbero identificare le opzioni di backup e i dettagli di contatto di emergenza per i fornitori di servizi.

Sicurezza del cablaggio (7.12)
Le informazioni ed i dati vengono trasferiti tramite cavi, mentre i computer, i sistemi di sicurezza e i controlli ambientali richiedono tutti alimentazione, fornita tramite cablaggio. I primi possono essere intercettati e le interruzioni di entrambi possono compromettere la sicurezza delle informazioni e la continuità aziendale. Il grado di sicurezza richiesto dipende dall'organizzazione e in molti casi sarà gestito da fornitori di strutture edilizie o società di telecomunicazioni e servizi pubblici. Le protezioni di base includono l'uso di condotti di cablaggio o coperture del pavimento dei cavi per evitare danni e l'accesso bloccato all'accesso ai servizi di pubblica utilità e ai punti di ingresso.

Manutenzione attrezzature (7.13)
La manutenzione delle apparecchiature introduce due considerazioni sulla sicurezza delle informazioni: apparecchiature in condizioni di scarsa manutenzione rischiano la perdita di informazioni; mentre l'assistenza o la manutenzione delle apparecchiature può esporre le informazioni a parti esterne o non autorizzate. È meno probabile che le apparecchiature sottoposte a manutenzione ed\\\\\ aggiornamento regolari richiedano riparazioni più rischiose o provochino interruzioni. Quando sono necessarie riparazioni, è necessario prestare attenzione nella scelta dei fornitori di servizi e nel controllo del loro lavoro.

Smaltimento o riutilizzo sicuro delle apparecchiature (7.14)
Le apparecchiati che non sono più in uso possono ancora avere installato software con licenza o avere archiviati dati sensibili. Questo vale anche per le apparecchiature che richiedono riparazione e dovrebbe essere preso in considerazione quando si decide se utilizzare servizi di riparazione esterni. Le funzioni di eliminazione standard potrebbero non essere adeguate per rimuovere le informazioni riservate. Invece, metodi specializzati di distruzione, cancellazione o sovrascrittura riducono il rischio che informazioni residue rimangano sul supporto di memorizzazione. Ricordarsi di rimuovere anche etichette o contrassegni fisici!

CONTROLLI TECNOLOGICI

Dispositivi utente endpoint (8.1)
I dispositivi utente endpoint sono tutti i dispositivi da cui è possibile accedere, elaborare o salvare informazioni. Includono laptop, smartphone e PC. Una policy per i dispositivi endpoint degli utenti dovrebbe includere la registrazione, la protezione fisica, password e crittografia e l'uso responsabile. L'uso responsabile include il controllo di chi ha accesso al dispositivo, l'installazione del software, l'aggiornamento regolare del sistema operativo e il backup del dispositivo. Un'organizzazione può richiedere una politica specifica per portare il proprio dispositivo al fine di prevenire controversie e rischi per la sicurezza delle informazioni associati.

Diritti di accesso privilegiati (8.2)
L'assegnazione di diritti di accesso privilegiati o di amministratore a utenti, componenti software e sistemi dovrebbe essere effettuata caso per caso e solo se necessario. Ciò significa che è necessaria una politica in atto che determini quando i diritti di accesso possono essere concessi e quando devono scadere o essere revocati. Quando vengono concessi diritti di accesso privilegiato, l'utente dovrebbe capire a cosa servono e quando dovrebbero essere utilizzati. Il primo passaggio è che gli utenti privilegiati dovrebbero sempre essere consapevoli di disporre dei diritti di accesso di amministratore. Questi diritti non dovrebbero essere utilizzati per le attività quotidiane, che dovrebbero essere sempre eseguite con account di accesso standard. L'accesso con privilegi deve essere utilizzato solo durante l'esecuzione di attività di amministrazione.

Limitazione dell'accesso alle informazioni (8.3)
L'accesso alle informazioni ed ad altre risorse dovrebbe essere basato sulle esigenze aziendali, con accesso limitato a utenti particolari. Le informazioni non dovrebbero essere accessibili agli utenti anonimi per impedire accessi non rintracciabili e non autorizzati. Ciò è importante per preservare la riservatezza delle informazioni, per monitorarne l'utilizzo e per prevenirne la modifica e la distribuzione.

Accesso al codice sorgente (8.4)
Il codice sorgente deve essere protetto per prevenire modifiche indesiderate e mantenere il codice riservato. Il ruolo e l'azienda dei dipendenti devono determinare se dispongono dell'accesso in lettura e scrittura. Limitare l'accesso in sola lettura per la maggior parte del personale aiuta a proteggere l'integrità del codice. Per lo stesso motivo, gli sviluppatori dovrebbero utilizzare strumenti di sviluppo che controllano le attività, anziché avere accesso diretto al repository del codice sorgente.

Autenticazione sicura (8.5)
L'autenticazione sicura aiuta a garantire che un utente sia chi dice di essere. La modalità di autenticazione richiesta dipende dalla classificazione delle informazioni. I nomi utente e le password forniscono un livello di autenticazione di base, che può essere rafforzato utilizzando controlli crittografici o biometrici, smart card o token o altra autenticazione a più fattori. Le schermate di accesso dovrebbero mostrare la quantità minima di informazioni possibile per evitare di fornire aiuto a persone non autorizzate. Tutti i tentativi di accesso devono essere registrati, riusciti o meno, in modo da poter identificare attacchi o utilizzi non autorizzati.

Gestione della capacità (8.6)
La gestione della capacità copre tutte le risorse umane, gli uffici e altre strutture, non solo l'elaborazione e l'archiviazione delle informazioni. I requisiti futuri dovrebbero essere presi in considerazione nella pianificazione aziendale e della sicurezza, in particolare se l'acquisizione di asset ha tempi lunghi. Il cloud computing spesso consente una gestione flessibile della capacità. Al contrario, le strutture fisiche e il personale possono richiedere una pianificazione più strategica. L'ottimizzazione dell'archiviazione delle informazioni fisiche e digitali, l'eliminazione dei vecchi dati e l'elaborazione batch e le applicazioni ottimizzate significheranno un utilizzo più efficiente della capacità esistente.

Protezione contro il malware (8.7)
Il software di rilevamento del malware (ad es. scanner antivirus) fornisce una certa protezione, ma non è l'unico a proteggere dal malware. La protezione include anche la consapevolezza della sicurezza delle informazioni, i controlli di accesso e i controlli di gestione delle modifiche per impedire l'installazione di malware o causare problemi. Come prima linea di difesa, il software di rilevamento del malware deve essere installato e aggiornato regolarmente. Tuttavia, una politica per prevenire l'installazione non autorizzata di software, l'uso di siti Web sospetti, il download di file da fonti remote e il rilevamento delle vulnerabilità sono altrettanto importanti. Infine, i rischi per la sicurezza possono essere ridotti pianificando attivamente un attacco malware. Tenere il passo con i nuovi malware, isolare gli ambienti critici e creare piani di continuità aziendale in caso di attacco contribuirà a mantenere la continuità aziendale in caso di attacco.

Gestione delle vulnerabilità tecniche (8.8)
La gestione delle vulnerabilità tecniche può essere suddivisa in tre categorie: identificazione, valutazione ed azione. Per identificare le vulnerabilità, le risorse devono essere inventariate con i dettagli del fornitore, della versione, dello stato di implementazione e del proprietario responsabile. Il fornitore può fornire informazioni sulle vulnerabilità, ma il proprietario deve identificare risorse aggiuntive che monitorano e rilasciano informazioni sulle vulnerabilità e metodi per identificare le vulnerabilità, come il pen test. Quando è stata identificata una vulnerabilità, è necessario valutare il rischio e l'urgenza, nonché i potenziali rischi dell'applicazione di un aggiornamento o di una patch. Gli aggiornamenti possono essere spesso utilizzati per agire contro le vulnerabilità, ma potrebbero non risolvere adeguatamente il problema e introdurre nuovi problemi. Se non è disponibile alcun aggiornamento o se l'aggiornamento è considerato inadeguato, misure come soluzioni alternative, isolamento dalla rete e maggiore monitoraggio possono essere sufficienti per mitigare il rischio.

Gestione della configurazione (8.9)
Software, hardware, servizi e reti devono essere configurati per funzionare correttamente con le impostazioni di sicurezza ritenute necessarie per proteggere l'organizzazione. La configurazione deve essere basata sulle esigenze aziendali e sulle minacce note. Come con tutti i sistemi sicuri, l'accesso privilegiato dovrebbe essere limitato e le funzioni non necessarie disabilitate. Le modifiche alla configurazione devono seguire la procedura di gestione delle modifiche ed essere completamente approvate e documentate.

Cancellazione delle informazioni (8.10)
Le informazioni non dovrebbero essere conservate più a lungo del necessario al fine di ridurre il rischio di esposizione alla sicurezza delle informazioni, ottimizzare l'uso delle risorse e rispettare leggi come il GDPR. È necessario utilizzare software di eliminazione sicura approvato per garantire l'eliminazione permanente e fornitori di smaltimento certificati dovrebbero essere utilizzati per i supporti fisici. Il metodo di eliminazione utilizzato dai fornitori di servizi cloud deve essere verificato dall'organizzazione per assicurarsi che sia adeguato. Mantenere un record di eliminazione è utile in caso di fuga di dati.

Mascheramento dei dati (8.11)
Solo la quantità minima di dati richiesta per un'attività dovrebbe essere disponibile nei risultati di ricerca. A tal fine, i dati personali dovrebbero essere mascherati (o anonimizzati o pseudonimizzati) per nascondere l'identità dei soggetti. Ciò può essere richiesto da leggi come il GPDR.

Prevenzione della fuga di dati (8.12)
Il monitoraggio ed il rilevamento dei tentativi non autorizzati di divulgazione od estrazione di dati sono fondamentali per la prevenzione. Quando viene rilevato un tentativo, è possibile attivare misure come la quarantena e-mail o i blocchi di accesso. Altri metodi, come le politiche e la formazione sul caricamento, la condivisione o l'accesso ai dati dovrebbero essere utilizzati per affrontare i rischi di perdita di dati da parte del personale.

Backup delle informazioni (8.13)
L'organizzazione ha bisogno di una politica specifica sui backup, che copra metodo, frequenza e test. Durante lo sviluppo della politica, l'organizzazione dovrebbe considerare punti come garantire la completezza dei backup e dei ripristini, le esigenze aziendali dei backup, dove e come vengono archiviati e come viene testato il sistema di backup. Il sistema di backup dovrebbe essere considerato parte dei piani di continuità operativa ed essere adeguato a soddisfare i requisiti di continuità.

Ridondanza delle strutture di elaborazione delle informazioni (8.14)
Qualsiasi organizzazione necessita di un'architettura di sistema sufficiente a soddisfare i requisiti di disponibilità aziendale. La ridondanza garantisce la disponibilità disponendo di capacità di riserva in caso di guasto del sistema e spesso richiede sistemi duplicati come gli alimentatori. Un'adeguata ridondanza che può essere attivata quando necessario costituisce una parte importante della pianificazione della continuità operativa e dovrebbe essere verificata regolarmente.

Registrazione / Logging (8.15)
La registrazione dei log degli eventi, genera prove, garantisce l'integrità delle informazioni di registro, può aiutare a prevenire l'accesso non autorizzato, identifica eventi di sicurezza delle informazioni e supporta le indagini. Un piano di registrazione deve identificare quali informazioni devono essere registrate (ad es. ID utente) e può coprire eventi come tentativi di accesso al sistema, modifiche, transazioni o accesso a file, tra le altre cose. I log devono essere protetti anche da utenti privilegiati in modo che non possano essere cancellati o modificati. I registri devono essere monitorati ed analizzati per rilevare modelli o eventi che potrebbero essere incidenti di sicurezza delle informazioni.

Attività di monitoraggio (8.16)
Lo scopo del monitoraggio è rilevare comportamenti anomali ed identificare potenziali incidenti di sicurezza delle informazioni. Il sistema di monitoraggio potrebbe coprire il traffico di rete, l'accesso al sistema, i registri e l'uso delle risorse. Il monitoraggio può aiutare ad identificare guasti o colli di bottiglia del sistema, attività associate a malware, accessi non autorizzati, comportamenti insoliti e attacchi come attacchi Denial of Service.

Sincronizzazione orologio (8.17)
La sincronizzazione dell'orologio è importante per garantire che i tempi di un incidente di sicurezza delle informazioni siano registrati in modo affidabile. I sistemi locali devono utilizzare un protocollo NTP (Network Time Protocol) per garantire la sincronizzazione. I fornitori di servizi cloud generalmente gestiscono i tempi per la registrazione. Tuttavia, gli orologi locali potrebbero non essere perfettamente sincronizzati con l'orologio del provider di servizi cloud. In questo caso, la differenza deve essere registrata e monitorata.

Utilizzo di programmi di utilità privilegiati (8.18)
Un programma di utilità può essere in grado di ignorare i controlli del sistema e dell'applicazione. L'utilizzo e l'accesso ai programmi di utilità dovrebbe pertanto essere strettamente limitato, con l'identificazione univoca dell'utente e la registrazione dell'utilizzo.

Installazione di software su sistemi operativi (8.19)
L'installazione del software può introdurre vulnerabilità nei sistemi operativi. Per ridurre al minimo questo rischio, il software deve essere installato solo da persone autorizzate. Il software dovrebbe provenire da fonti affidabili e ben mantenute o completamente testato se sviluppato internamente. Le versioni precedenti devono essere conservate e tutte le modifiche registrate in modo che sia possibile il rollback, se necessario.

Controlli di rete (8.20)
Le reti devono essere sufficientemente sicure da proteggere le informazioni che passano su di esse. Per mantenerle al sicuro, devono essere mantenuti aggiornati e monitorati, con la possibilità di limitare sia le connessioni ai dispositivi autenticati che il traffico che può passare sulla rete. Un metodo per isolare la rete può essere utile se la rete viene attaccata.

Sicurezza dei servizi di rete (8.21)
I servizi di sicurezza della rete coprono tutto, dalla fornitura di una semplice connessione e larghezza di banda, a servizi complessi come firewall e sistemi di rilevamento delle intrusioni. Il livello di sicurezza richiesto dipenderà dalle esigenze aziendali. Quando la sicurezza richiesta viene identificata, deve essere implementata e monitorata. Questo è spesso fatto da fornitori di servizi di rete di terze parti. Le procedure di autorizzazione all'accesso ed i mezzi di accesso come le VPN dovrebbero essere presi in considerazione durante l'impostazione dei servizi di sicurezza della rete.

Filtraggio Web (8.22)
Non tutti i siti web su Internet sono sicuri. Alcuni contengono informazioni illegali ed altri distribuiscono malware. Il blocco degli indirizzi IP di siti Web sospetti può ridurre i rischi. Tuttavia, non tutti i siti Web dannosi possono essere bloccati, quindi il filtraggio deve essere accompagnato da regole e formazione di sensibilizzazione sull'uso appropriato e responsabile di Internet.

Segregazione nelle reti (8.23)
Le reti di grandi dimensioni possono essere suddivise in più domini. Ciò significa che a ciascun dominio possono essere applicati diversi livelli di sicurezza, con accesso limitato a diverse parti della rete aziendale. Le reti possono essere completamente separate fisicamente o digitalmente utilizzando reti logiche. Le reti wireless non hanno confini fisici e dovrebbero quindi essere considerate come connessioni esterne fino a quando non viene superato un gateway come una VPN durante l'accesso a dati sensibili.

Uso della crittografia (8.24)
L'uso della crittografia deve essere gestito con attenzione, tenendo in considerazione il livello di protezione richiesto, la gestione delle chiavi, la crittografia dei dispositivi endpoint ed il modo in cui la crittografia potrebbe influire sull'ispezione dei contenuti (ad es. scansione di malware). La gestione delle chiavi richiede un processo di generazione, archiviazione, storicizzazione, recupero, distribuzione, ritiro e distruzione di chiavi crittografiche.

Ciclo di vita di sviluppo sicuro (8.25)
Lo sviluppo sicuro copre la costruzione di servizi, architetture, software e sistemi. Un aspetto chiave è la separazione degli ambienti di sviluppo, test (approvazione) e produzione con repository sicuri per il codice sorgente. La sicurezza dovrebbe essere una considerazione fin dalla fase delle specifiche e progettazione, con punti di controllo integrati nel piano di progetto e test pianificati. Gli sviluppatori devono anche essere consapevoli delle linee guida per la codifica sicura ed essere in grado di prevenire, trovare e correggere le vulnerabilità.

Requisiti di sicurezza dell'applicazione (8.26)
Le organizzazioni devono identificare e specificare i requisiti di sicurezza per le applicazioni, quindi determinarli utilizzando una valutazione del rischio. I requisiti sono determinati dal livello di classificazione di sicurezza delle informazioni che passano attraverso l'applicazione. I requisiti possono includere controlli di accesso, livello di protezione, crittografia, controlli di input ed output, registrazione, gestione dei messaggi di errore, resilienza agli attacchi e requisiti legali. La sicurezza richiede una considerazione particolare se l'applicazione esegue transazioni di informazioni, ordini e pagamenti.

Architettura di sistema sicura e principi ingegneristici (8.27)
I principi di architettura ed ingegneria garantiscono che i sistemi siano progettati, implementati e gestiti in modo sicuro durante tutto il loro ciclo di vita di sviluppo. Analisi dei principi del sistema sicuro quali controlli di sicurezza sono necessari e come dovrebbero essere applicati. Dovrebbero essere prese in considerazione anche le buone pratiche, le considerazioni pratiche sui costi e la complessità e su come le nuove funzionalità possono essere integrate nei sistemi esistenti.

Sviluppo sicuro (8.28)
La pratica dello sviluppo sicuro aiuta a garantire che il codice venga scritto per ridurre al minimo le vulnerabilità. I principi di sviluppo sicuro possono essere utilizzati per promuovere le migliori pratiche e stabilire standard minimi nell'organizzazione. Questi dovrebbero prendere in considerazione le attuali minacce del mondo reale, l'uso di ambienti controllati per lo sviluppo e garantire la competenza degli sviluppatori. La codifica sicura dovrebbe includere anche la gestione degli aggiornamenti e della manutenzione, in particolare il controllo di chi è responsabile della manutenzione dei codici da fonti esterne.

Test di sicurezza in fase di sviluppo e accettazione (8.29)
I test di sicurezza dovrebbero essere parte integrante dei test di sviluppo. Ciò include il test della configurazione sicura dei sistemi operativi (ad es. firewall), la codifica sicura e le funzioni di sicurezza (come l'accesso). I test devono essere programmati, documentati ed avere criteri per determinare risultati accettabili.

Sviluppo in outsourcing (8.30)
Quando lo sviluppo viene esternalizzato, i requisiti di sicurezza delle informazioni devono essere comunicati e concordati dallo sviluppatore esternalizzato e monitorati dall'organizzazione di outsourcing. Le licenze e la proprietà intellettuale, i test e le prove dei test ed i diritti contrattuali per l'audit del processo di sviluppo sono esempi di considerazioni sulla sicurezza che dovrebbero essere concordate tra le parti.

Separazione degli ambienti di sviluppo, test e produzione (8.31)
Le attività di test e sviluppo possono causare modifiche indesiderate o guasti del sistema, che potrebbero compromettere l'ambiente di produzione se non adeguatamente protetto. Il grado di separazione tra test e produzione dipenderà dall'organizzazione, ma gli ambienti devono essere separati ed etichettati chiaramente, in modo che il test o azioni come la compilazione non possano aver luogo nell'ambiente di produzione. Le modifiche dovrebbero essere monitorate, con un attento controllo su chi ha accesso a ciascun ambiente. Nessuno dovrebbe avere la possibilità di apportare modifiche sia all'ambiente di test che a quello di produzione senza previa revisione e approvazione.

Gestione del cambiamento (8.32)
La riservatezza, la disponibilità e l'integrità delle informazioni possono essere tutte compromesse quando si introduce un'infrastruttura o un software o si apportano modifiche sostanziali a uno esistente. Un processo formale di documentazione, test, controllo di qualità ed implementazione può ridurre i rischi. La documentazione dei test e la pianificazione delle emergenze sono importanti nel periodo che precede l'implementazione, in particolare per garantire che il nuovo software non influisca negativamente sull'ambiente di produzione. Potrebbe essere necessario modificare le guide e le procedure operative dopo aver apportato le modifiche.

Informazioni sul test (8.33)
Ci sono due considerazioni chiave per le informazioni sui test: dovrebbero essere sufficientemente vicine alle informazioni operative per garantire che i risultati dei test siano affidabili, ma non dovrebbero contenere informazioni operative riservate. Se le informazioni sensibili devono essere utilizzate per il test, dovrebbero essere protette, modificate o rese anonime prima di essere utilizzate e dovrebbero essere cancellate immediatamente dopo il test.

Protezione dei sistemi informativi durante audit e test (8.34)
I sistemi operativi non dovrebbero essere indebitamente influenzati da audit o revisioni tecniche. Per evitare scompigli eccessivi, gli audit dovrebbero essere pianificati con tempi e portata concordati. L'accesso in sola lettura preverrà modifiche accidentali ai sistemi durante un controllo e tutti gli accessi dovrebbero essere monitorati.

IN CHE MODO LA NUOVA REVISIONE DELLA ISO/IEC 27002 INFLUISCE SULLA ISO/IEC 27001?
La ISO/IEC 27002 ha la sua origine nella ISO/IEC 17799, essendo il primo standard ISO di riferimento delle buone pratiche per la gestione della sicurezza delle informazioni.
La ISO/IEC 27002 è stata presa come riferimento per l'allegato A della ISO/IEC 27001.
Naturalmente, in questo contesto, un aggiornamento alla ISO/IEC 27002 influirà inevitabilmente sull'insieme dei controlli nella ISO/IEC 27001. Si prevede pertanto che tali modifiche si riflettano nell'allegato A della ISO 27001 dopo la pubblicazione ufficiale della ISO/IEC 27002 aggiornata, per mantenere coerenza tra i due standard.

IN CHE MODO INFLUISCE LA NUOVA ISO/IEC 27002 SULLE ORGANIZZAZIONI CHE HANNO GIÀ LA CERTIFICAZIONE ISO/IEC 27001?
Attualmente non vi è alcun impatto sulle organizzazioni che già mantengono un Sistema di Gestione per la Sicurezza delle Informazioni certificato fino all'approvazione della nuova ISO/IEC 27002 ed all'aggiornamento dell'allegato A, in una nuova versione della ISO/IEC 27001.
In generale, le organizzazioni avranno un periodo di transizione nel quale sono tenuti ad adottare lo standard ISO/IEC 27001 una volta che lo standard rivisto sarà pubblicato (es. revisione dell'annex A).
Per le organizzazioni che cercano e stanno per certificare il proprio Sistema per la Gestione della Sicurezza delle Informazioni, questo non dovrebbe essere un ostacolo. Le organizzazioni dovrebbero familiarizzare con la nuova serie di controlli e, con l'aiuto della mappatura alla versione 2013 presente all'interno della tabella B2 presente all'interno della nuova 27002, prepararsi ad aggiornare il proprio sistema di gestione.

Altro importante impatto riguarderà quelle organizzazioni che hanno adottato ed ottenuto attestazioni di conformità delle norme definite 270XX in particolare ISO/IEC 27017 e ISO/IEC 27018 che si basano sulla ISO/IEC 27002:2013 ed oltretutto richieste, almeno in Italia, per poter adempiere a specifiche richieste di AgID.

Si precisa che il presente documento è stato predisposto utilizzando prevalentemente le informazioni tratte dalla versione FDIS della ISO/IEC 27002 non essendo, alla data di stesura, ancora disponibile la pubblicazione ufficiale della nuova norma

Attilio Rampazzo CISA, CRISC, CDPSE
Information Systems Consultant, Trainer & Auditor
European Data Protection Expert
Auditor RGVI QMS ISMS ITSMS BCMS (Registri AICQ SICEV)
Data Protection Officer - Data Protection Auditor (Registri AICQ SICEV)
Referente Registri AICQ SICEV Auditor Sicurezza delle Informazioni & IT Service Management
Referente Registro AICQ SICEV Professionisti ICT (UNI 11506)
Referente Registro AICQ SICEV Professionisti Trattamento e Protezione Dati Personali (UNI 11697)

attilio.rampazzo@gmail.com

Paolo Sferlazza
Advisor, Auditor and Trainer

PCI QSA, CISM,CISA,CRISC,LA27001, LA 22301, CBCI, MBCI, CDPSE, OPST, COBIT 5, ITIL, LA20000, LA9001, ISFS, CMMI, Scrum Master

paolo.sferlazza@gerico-sec.it