IL WEBINAR INIZIA TRA QUALCHE MINUTO
GRAZIE PER AVER SCELTO DI PARTECIPARE

MASSIMO
CHIRIVÌ

IT SECURITY
ETHICAL HACKING

Approfondimento sui controlli CIS

IG1

Un'impresa IG1 è di piccole o medie dimensioni con competenze IT e di sicurezza informatica limitate da dedicare alla protezione delle risorse e del personale. L'obiettivo principale di queste aziende è continuare ad essere operative, in quanto presentano una bassa tolleranza dei tempi di inattività. La sensibilità dei dati che proteggono è bassa e riguarda principalmente le informazioni finanziarie e dei dipendenti.

Le Salvaguardie previste in IG1 dovrebbero essere implementabili con limitate esperienze di sicurezza informatica e mirate a contrastare gli attacchi generici non mirati. Queste Salvaguardie sono in genere progettate per funzionare in combinazione con hardware e software commerciale (COTS) di piccoli uffici aziendali o domestici.

IG2 (Includes IG1)

Un'impresa IG2 impiega personale responsabile della gestione e della protezione dell'infrastruttura IT. Queste aziende supportano vari reparti con diversi profili di rischio in base alla funzione lavorativi e relativi obiettivi. Alcuni piccoli settori aziendali potrebbero avere anche obblighi di rispetto normativo. Le aziende IG2 spesso archiviano ed elaborano informazioni sensibili sui clienti o sull'azienda e possono sopportare brevi interruzioni del servizio. Una delle principali preoccupazioni è la perdita di credibilità in caso di violazione.

Le Salvaguardie previste in IG2 aiutano i team di sicurezza nel fronteggiare una maggiore complessità operativa. L'applicabilità delle Salvaguardie dipenderà dal livello tecnologico dell'azienda e dalle competenze disponibili, necessarie per le corrette installazioni e configurazioni.

IG3 (Includes IG1 and IG2)

Una azienda in IG3 impiega esperti di sicurezza specializzati nei vari aspetti della sicurezza informatica (es. gestione del rischio, test di penetrazione, sicurezza delle applicazioni). Le risorse e i dati in IG3 contengono informazioni sensibili o funzioni soggette a al rispetto normativo e di conformità. Un'impresa IG3 deve garantire la disponibilità dei servizi e la riservatezza ed integrità dei dati sensibili. Gli attacchi riusciti possono causare danni significativi ad un vasto pubblico.

Le Salvaguardie previste in IG3 devono ridurre drasticamente gli attacchi mirati di un avversario sofisticato e contenere l'impatto degli attacchi zero-day.

CONTROLLI 01

Inventario e Controllo delle Risorse Aziendali

SAFEGUARDS TOTAL	IG1	IG2	IG3
5	2/5	4/5	5/5

Panoramica

Gestire attivamente (inventariare, tracciare e correggere) tutte le risorse aziendali (dispositivi dell'utente finale, mobili e portatili inclusi, dispositivi di rete, dispositivi non informatici/ Internet of Things – IoT e server) connessi all'infrastruttura fisicamente, virtualmente, in remoto e quelli in ambienti cloud, per conoscere con precisione la totalità delle risorse che devono essere monitorate e protette in azienda. Ciò aiuterà anche nell'identificare quelle non autorizzate e non gestite, da rimuovere o aggiornare.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
1.1	**Stabilire e Mantenere un Inventario Dettagliato delle Risorse Aziendali** Stabilire e mantenere un inventario accurato, dettagliato e aggiornato di tutte le risorse aziendali con la possibilità di archiviazione o elaborazione dati, includendo: dispositivi dell'utente finale (compresi portatili e mobili), dispositivi di rete, dispositivi non informatici/IoT e server. Assicurare che l'inventario registri l'indirizzo di rete (se statico), l'indirizzo hardware, il nome del computer, il proprietario della risorsa aziendale, il reparto per ogni risorsa e se la risorsa è stata approvata per la connessione alla rete. Per i dispositivi mobili degli utenti finali, gli strumenti di tipo MDM possono supportare questo processo. Questo inventario include le risorse connesse all'infrastruttura fisica, virtuale, remota e quelle all'interno di ambienti cloud. Include inoltre le risorse che sono regolarmente connesse all'infrastruttura di rete dell'impresa, anche se non sono sotto il suo controllo. Rivedere e aggiornare l'inventario di tutte le risorse aziendali semestralmente o più frequentemente.	Dispositivi	Identificare	●	●	●
1.2	**Trattare le Risorse non Autorizzate** Assicurare la presenza di un processo per trattare le risorse non autorizzate su base settimanale. L'azienda può scegliere di rimuovere la risorsa dalla rete, bloccarne la connessione remota o metterla in quarantena.	Dispositivi	Rispondere	●	●	●
1.3	**Utilizzare uno Strumento di Rilevamento Attivo** Utilizzare uno strumento di rilevamento attivo per identificare le risorse connesse alla rete aziendale. Configurarlo per l'esecuzione quotidiana o più frequente.	Dispositivi	Rilevare		●	●
1.4	**Utilizzare i log del Protocollo Dinamico di Configurazione Host (DHCP)** Utilizzare i log su tutti i server DHCP o altri strumenti di gestione degli indirizzi IP (Internet Protocol) per aggiornare l'inventario delle risorse aziendali. Rivedere ed utilizzare i registri per aggiornare l'inventario delle risorse settimanalmente o più frequentemente.	Dispositivi	Identificare		●	●
1.5	**Utilizzare uno Strumento di Rilevazione Passiva** Utilizzare uno strumento di rilevazione passiva per identificare le risorse connesse alla rete aziendale. Rivedere e utilizzare le scansioni per aggiornare l'inventario delle risorse almeno una volta alla settimana o più frequentemente.	Dispositivi	Rilevare			●

CONTROLLI 02

Inventario e Controllo delle Risorse Software

SAFEGUARDS TOTAL	IG1	IG2	IG3
7	3/7	6/7	7/7

Panoramica

Gestire attivamente (inventariare, tracciare e correggere) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito e che il software non autorizzato e non gestito venga trovato impedendone l'installazione o l'esecuzione.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
2.1	**Stabilire e Mantenere un Inventario Software** Stabilire e mantenere un inventario dettagliato di tutto il software con licenza installato sulle risorse aziendali. L'inventario del software deve documentare il titolo, l'editore, la data di installazione/utilizzo iniziale e la sua finalità; se opportuno, includere URL, app store, versione(i), distribuzione e data di disattivazione. Rivedere e aggiornare l'inventario del software semestralmente o più frequentemente.	Applicazioni	Identificare	●	●	●
2.2	**Accertare il Supporto del Software Autorizzato** Assicurare che solo il software attualmente supportato sia individuato come autorizzato nell'inventario software delle risorse aziendali. Se il software non è supportato, ma è necessario per gli scopi aziendali, documentare un'eccezione che riporti la mitigazione dei controlli l'accettabilità del rischio residuo. Qualsiasi software non supportato privo di documentazione di eccezione, deve essere indicato come non autorizzato. Rivedere l'elenco del software per verificarne il supporto almeno mensilmente o più frequentemente.	Applicazioni	Identificare	●	●	●
2.3	**Trattare il Software non Autorizzato** Assicurare che il software non autorizzato venga rimosso dalle risorse aziendali o riceva un'eccezione documentata. Rivedere mensilmente o più frequentemente.	Applicazioni	Rispondere	●	●	●
2.4	**Utilizzare Strumenti Automatici per l'Inventario del Software** Utilizzare strumenti di inventario del software, quando possibile, in tutta l'azienda per automatizzare l'individuazione e la documentazione del software installato.	Applicazioni	Rilevare		●	●
2.5	**Elenco del Software Consentito** Utilizzare i controlli tecnici, come l'elenco delle applicazioni autorizzate, per garantire che solo il software consentito possa essere accessibile o eseguibile Aggiornare semestralmente o più frequentemente.	Applicazioni	Proteggere		●	●
2.6	**Elenco delle Librerie Consentite** Utilizzare controlli tecnici per garantire che solo le specifiche librerie software autorizzate, come file .dll, .ocx, .so, ecc., possano essere caricate in un processo di sistema. Impedire il caricamento delle librerie non autorizzate in un processo di sistema. Rivalutare semestralmente o più frequentemente.	Applicazioni	Proteggere		●	●
2.7	**Elenco degli Script Consentiti** Utilizzare controlli tecnici, come le firme digitali e controllo di versione, per garantire che solo gli script autorizzati, come file .ps1, .py, ecc., possano essere eseguiti. Impedire l'esecuzione di script non autorizzati. Rivalutare semestralmente o più frequentemente.	Applicazioni	Proteggere			●

CONTROLLI 03

Protezione dei Dati

SAFEGUARDS TOTAL	IG1	IG2	IG3
14	6/14	12/14	14/14

Panoramica

Sviluppare processi e controlli tecnici per identificare, classificare, elaborare in sicurezza, conservare ed eliminare i dati.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
3.1	**Stabilire e Mantenere una Procedura di Gestione dei Dati** Stabilire e mantenere una procedura di gestione dei dati. Considerarne la sensibilità, il proprietario, la gestione, i limiti di conservazione e i requisiti di rimozione, in base agli standard aziendali di riservatezza e conservazione. Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Identificare	●	●	●
3.2	**Stabilire e Mantenere un Inventario dei Dati** Stabilire e mantenere un inventario dei dati, basato sulla procedura di gestione aziendale dei dati. Inventariare come minimo i dati sensibili. Rivedere e aggiornare l'inventario almeno una volta all'anno, dando priorità a quest'ultimi.	Dati	Identificare	●	●	●
3.3	**Configurare le Liste di Controllo degli Accessi** Configurare le liste di controllo degli accessi ai dati in base alle esigenze di conoscenza di un utente. Utilizzare queste liste, note anche come permessi di accesso, a file system locali e remoti, database e applicazioni	Dati	Proteggere	●	●	●
3.4	**Determinare la Conservazione dei Dati** Conservare i dati secondo la procedura aziendale di gestione dei dati. La conservazione dei dati deve includere tempi minimi e massimi.	Dati	Proteggere	●	●	●
3.5	**Rimozione Sicura dei Dati** Eliminare i dati in modo sicuro secondo la procedura aziendale di gestione dei dati Assicurare che il processo ed il metodo di eliminazione siano commisurati alla loro sensibilità.	Dati	Proteggere	●	●	●
3.6	**Crittografare i Dati sui Dispositivi degli Utenti Finali** Crittografare i dati sui dispositivi degli utenti finali contenenti dati sensibili. Le implementazioni possono includere ad esempio: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Dispositivi	Proteggere	●	●	●
3.7	**Stabilire e Mantenere un Sistema di Classificazione dei Dati** Stabilire e mantenere uno schema generale di classificazione dei dati aziendali. Le aziende possono utilizzare etichette, come "Sensibile", "Riservato" e "Pubblico" per classificare i propri dati in base a tali elementi. Rivedere e aggiornare lo schema di classificazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Identificare		●	●
3.8	**Documentare il Flusso dei Dati** Documentare il flusso dei dati. La documentazione include i flussi di dati dei fornitori di servizi e dovrebbe essere basata sulla procedura gestionale dei dati aziendali Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Identificare		●	●
3.9	**Crittografare i Dati sui Media Rimovibili** Crittografare i dati sui media rimovibili.	Dati	Proteggere		●	●
3.10	**Crittografare i Dati Sensibili in Transito** Crittografare i dati in transito. Esempi di implementazione includono: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH).	Dati	Proteggere		●	●
3.11	**Crittografare i Dati Sensibili a Riposo** Crittografare i dati sensibili a riposo su server, applicazioni e database. La crittografia a livello di archiviazione, nota anche come crittografia lato server, soddisfa i requisiti minimi di questa Salvaguardia. Ulteriori metodi di crittografia possono includere quella a livello di applicazione, nota anche come crittografia lato client, in cui l'accesso ai dispositivi di archiviazione non permette l'accesso ai dati in chiaro	Dati	Proteggere		●	●
3.12	**Segmentare Elaborazione ed Archiviazione dei Dati secondo la Sensibilità** Segmentare elaborazione ed archiviazione dei dati in base alla sensibilità. Non elaborare dati sensibili utilizzando risorse aziendali predisposte per livelli inferiori di sensibilità.	Rete	Proteggere		●	●
3.13	**Adottare una Soluzione per la Prevenzione della Perdita dei Dati** Implementare uno strumento automatizzato, di prevenzione della perdita di dati (DLP) basato su host, per identificare tutti i dati sensibili archiviati, elaborati o trasmessi attraverso le risorse aziendali, compresi quelli in locale o presso un fornitore di servizi remoto, aggiornando l'inventario dei dati sensibili.	Dati	Proteggere			●
3.14	**Mantenere un Log di Accesso ai Dati Sensibili** Mantenere un log che registri l'accesso ai dati sensibili, inclusa la loro modifica e l'eliminazione.	Dati	Rilevare			●

CONTROLLI 04

Configurazione Sicura delle Risorse Aziendali e del Software

SAFEGUARDS TOTAL	IG1	IG2	IG3
12	7/12	11/12	12/12

Panoramica

Stabilire e mantenere la configurazione sicura delle risorse aziendali (dispositivi dell'utente finale, inclusi portatili e mobili, dispositivi di rete, dispositivi non informatici / IoT, server) e software (sistemi operativi e applicazioni).

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
4.1	**Stabilire e Mantenere una Procedura di Configurazione Sicura** Stabilire e mantenere una procedura di configurazione sicura per le risorse aziendali (dispositivi dell'utente finale inclusi portatili e mobili, dispositivi non informatici / IoT) e per il software (sistemi operativi ed applicazioni). Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Applicazioni	Proteggere	●	●	●
4.2	**Stabilire e Mantenere una Procedura di Configurazione Sicura per l'Infrastruttura di Rete** Stabilire e mantenere una procedura di configurazione sicura per i dispositivi di rete. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Rete	Proteggere	●	●	●
4.3	**Configurare il Blocco Automatico della Sessione sulle Risorse Aziendali** Configurare il blocco automatico della sessione sulle risorse aziendali dopo un periodo di inattività definito. Per i sistemi operativi generici, il periodo non deve superare i 15 minuti. Per i dispositivi mobili dell'utente finale, il periodo non deve superare i 2 minuti.	Utenti	Proteggere	●	●	●
4.4	**Implementare e Gestire un Firewall sui Server** Implementare e gestire un firewall sui server, quando supportato. Esempi di implementazione includono un firewall virtuale, un firewall del sistema operativo o un agent firewall di terze parti.	Dispositivi	Proteggere	●	●	●
4.5	**Implementare e Gestire un Firewall sui Dispositivi dell'Utente Finale** Implementare e gestire un firewall basato su host o uno strumento di filtraggio delle porte sui dispositivi degli utenti finali, con una regola predefinita di negazione che elimina tutto il traffico ad eccezione di porte e servizi esplicitamente consentiti.	Dispositivi	Proteggere	●	●	●
4.6	**Gestire in modo Sicuro Risorse e Software Aziendali** Gestire in modo sicuro risorse e software aziendali. Esempi di implementazione includono la gestione della configurazione tramite il controllo di versione dell'infrastruttura tramite codice e l'accesso alle interfacce amministrative utilizzando protocolli di rete sicuri, come Secure Shell (SSH) e Protocollo di trasferimento Ipertestuale Sicuro (HTTPS). Non utilizzare protocolli di gestione non sicuri, come Telnet (Teletype Network) e HTTP, a meno che non siano essenziali dal punto di vista operativo.	Rete	Proteggere	●	●	●
4.7	**Gestire gli Account Predefiniti di Risorse e Software Aziendali** Gestire gli account predefiniti di risorse e software aziendali, come root, amministratore e altri account preconfigurati rilasciati dal fornitore. Esempi di implementazione includono: disabilitare o rendere inutilizzabili gli account predefiniti.	Utenti	Proteggere	●	●	●
4.8	**Disinstallare o Disabilitare Servizi e Software non Necessari sulle Risorse Aziendali** Disinstallare o disabilitare servizi e software non necessari sulle risorse aziendali, come un servizio di condivisione file inutilizzato, un modulo di applicazione Web o una funzione di servizio.	Dispositivi	Proteggere		●	●
4.9	**Configurare Server DNS Sicuri sulle Risorse Aziendali** Configurare server DNS sicuri sulle risorse aziendali. Esempi di implementazione includono: configurazione delle risorse affinché utilizzino server DNS controllati dall'azienda o accesso a server DNS esterni affidabili.	Dispositivi	Proteggere		●	●
4.10	**Abilitare il Blocco Automatico sui Dispositivi Portatili dell'Utente Finale** Abilitare il blocco automatico del dispositivo portatile dell'utente finale dopo una soglia stabilita di tentativi di autenticazione non riusciti, ove supportato. Per i laptop, non consentire più di 20 tentativi di autenticazione falliti; per tablet e smartphone, non più di 10. Esempi di implementazione includono: Microsoft® InTune Device Lock e Apple® Configuration Profile maxFailedAttempts.	Dispositivi	Rispondere		●	●
4.11	**Abilitare la Cancellazione da Remoto sui Dispositivi Portatili dell'Utente Finale** Cancellare da remoto i dati aziendali dai dispositivi portatili di proprietà dell'utente finale quando è necessario, ad esempio dispositivi smarriti o rubati, o quando una persona lascia l'azienda.	Dispositivi	Proteggere		●	●
4.12	**Separare gli Spazi di Lavoro Aziendali sui Dispositivi Portatili dell'Utente Finale** Assicurare che gli spazi di lavoro aziendali sui dispositivi mobili degli utenti finali siano separati, ove supportato. Esempi di implementazione includono: l'utilizzo di Apple® Configuration Profile, Android™ Work Profile per separare applicazioni e dati aziendali da quelli personali.	Dispositivi	Proteggere			●

CONTROLLI 05

Gestione degli Account

SAFEGUARDS TOTAL	IG1	IG2	IG3
6	4/6	6/6	6/6

Panoramica

Utilizzare procedure e strumenti per assegnare e gestire l'autorizzazione delle credenziali a risorse e software aziendali, per gli account utente, inclusi quelli amministrativi e di servizio.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
5.1	**Stabilire e Mantenere un Inventario degli Account** Stabilire e mantenere un inventario di tutti gli account aziendali. L'inventario deve includere account utenti e amministrativi. L'inventario, dovrebbe contenere almeno il nome della persona, il nome utente, le date di inizio/fine e l'area lavorativa. Assicurare che tutti gli account attivi siano autorizzati, con una pianificazione almeno trimestrale o più frequentemente.	Utenti	Identificare	●	●	●
5.2	**Utilizzare Password Univoche** Utilizzare password univoche per tutte le risorse aziendali. L'implementazione delle "best practice" prevede, come minimo, una password di 8 caratteri per gli account che utilizzano l'autenticazione multi fattore e una password di 14 caratteri per gli account che non la prevedono.	Utenti	Proteggere	●	●	●
5.3	**Disabilitare gli Account Dormienti** Cancellare o disabilitare tutti gli account dormienti dopo un periodo di 45 giorni di inattività, quando supportato.	Utenti	Rispondere	●	●	●
5.4	**Limitare i Privilegi Amministrativi agli Account dell'Amministratore** Limitare i privilegi amministrativi agli account di amministratore riservati alle risorse aziendali. Effettuare attività informatiche generali, navigazione in Internet, posta elettronica ed uso delle suite di produttività, da un account utente non privilegiato.	Utenti	Proteggere	●	●	●
5.5	**Stabilire e Mantenere un Inventario degli Account di Servizio** Stabilire e mantenere un inventario degli account di servizio. L'inventario, deve contenere almeno il referente dell'area lavorativa, data di revisione e scopo. Eseguire revisioni degli account di servizio per verificare che tutti quelli attivi siano autorizzati, con una pianificazione ricorrente almeno trimestrale o più frequentemente.	Utenti	Identificare		●	●
5.6	**Centralizzare la Gestione degli Account** Centralizzare la gestione degli account con un servizio di directory o identità.	Utenti	Proteggere		●	●

CONTROLLI 06

Gestione del Controllo degli Accessi

SAFEGUARDS TOTAL	IG1	IG2	IG3
8	5/8	7/8	8/8

Panoramica

Utilizzare processi e strumenti per creare, assegnare, gestire e revocare credenziali di accesso e privilegi per gli account utenti, amministratori, di servizio per le risorse e i software aziendali.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
6.1	**Stabilire una Procedura di Concessione degli Accessi** Stabilire e seguire una procedura, preferibilmente automatizzata, per concedere l'accesso alle risorse aziendali in caso di nuova assunzione, attribuzione di diritti o cambio di ruolo di un utente.	Utenti	Proteggere	●	●	●
6.2	**Stabilire una Procedura di Revoca degli Accessi** Stabilire e seguire una procedura, preferibilmente automatizzata, per revocare l'accesso alle risorse aziendali, disabilitando gli account immediatamente dopo la cessazione, la revoca dei diritti o il cambio di ruolo di un utente. La disattivazione degli account, piuttosto che la loro eliminazione, potrebbe essere necessaria per consentire gli audit di tracciamento.	Utenti	Proteggere	●	●	●
6.3	**Richiedere MFA per le Applicazioni Esposte Esternamente** Richiedere che tutte le applicazioni aziendali o di terze parti esposte esternamente applichino l'autenticazione multi fattore, ove supportata. Il suo utilizzo tramite un servizio di directory o un provider SSO è un'implementazione	Utenti	Proteggere	●	●	●
6.4	**Richiedere MFA per l'Accesso di Rete Remoto** Richiedere l'autenticazione multi fattore per l'accesso di rete da remoto	Utenti	Proteggere	●	●	●
6.5	**Richiedere MFA per l'Accesso Amministrativo** Richiedere l'autenticazione multi fattore per l'accesso di tutti gli account amministrativi, se supportata, per tutte le risorse aziendali, sia gestite in locale sia utilizzando un fornitore esterno	Utenti	Proteggere	●	●	●
6.6	**Stabilire e Mantenere un Inventario dei Sistemi di Autenticazione ed Autorizzazione** Stabilire e mantenere un inventario dei sistemi di autenticazione ed autorizzazione aziendali, inclusi quelli ospitati in locale o presso un fornitore di servizi remoto. Rivedere e aggiornare l'inventario, come minimo, annualmente o più frequentemente.	Utenti	Identificare		●	●
6.7	**Centralizzare il Controllo degli Accessi** Centralizzare il controllo degli accessi per tutte le risorse aziendali tramite un servizio di directory o un provider SSO, se supportato.	Utenti	Proteggere		●	●
6.8	**Definire e Mantenere un Controllo degli Accessi Basato sui Ruoli** Definire e mantenere il controllo degli accessi basato sui ruoli, determinando e documentando i diritti di accesso necessari per ciascun ruolo aziendale per consentire lo svolgimento dei compiti assegnati. Esegui le revisioni del controllo degli accessi delle risorse aziendali per assicurare che tutti i privilegi siano autorizzati, secondo una pianificazione almeno annuale o più frequentemente.	Dati	Proteggere			●

CONTROLLI 07

Gestione Continua delle Vulnerabilità

SAFEGUARDS TOTAL	IG1	IG2	IG3
7	4/7	7/7	7/7

Panoramica

Sviluppare un piano per valutare e monitorare costantemente le vulnerabilità su tutte le risorse aziendali all'interno dell'infrastruttura, al fine di rimediare e ridurre al minimo la finestra di opportunità per gli aggressori. Monitorare le fonti di informazione del settore pubblico e privato per conoscere le più recenti minacce e vulnerabilità.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
7.1	**Stabilire e Mantenere una Procedura di Gestione delle Vulnerabilità.** Stabilire e mantenere una procedura di gestione delle vulnerabilità documentata. Rivedere ed aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Applicazioni	Proteggere	●	●	●
7.2	**Stabilire e Mantenere una Procedura di Correzione** Stabilire e mantenere una strategia di correzione documentata basata sul rischio nell'ambito di una procedura di correzione, rivedendola mensilmente o più frequentemente.	Applicazioni	Rispondere	●	●	●
7.3	**Gestire l'Aggiornamento Automatico del Sistema Operativo** Eseguire gli aggiornamenti del sistema operativo delle risorse aziendali per mezzo di un sistema automatizzato, mensilmente o più frequentemente.	Applicazioni	Proteggere	●	●	●
7.4	**Gestire l'Aggiornamento Automatico delle Applicazioni** Eseguire gli aggiornamenti delle applicazioni delle risorse aziendali per mezzo di un sistema automatizzato di installazione delle patch, mensilmente o più frequentemente.	Applicazioni	Proteggere	●	●	●
7.5	**Eseguire Scansioni di Vulnerabilità delle Risorse Aziendali Interne** Eseguire scansioni automatizzate delle vulnerabilità delle risorse aziendali interne, trimestralmente o più frequentemente. Effettuare scansioni sia autenticate che non, utilizzando uno strumento di scansione delle vulnerabilità compatibile SCAP.	Applicazioni	Identificare		●	●
7.6	**Eseguire Scansioni di Vulnerabilità delle Risorse Aziendali Esposte Esternamente** Eseguire scansioni automatizzate delle vulnerabilità delle risorse aziendali esposte esternamente utilizzando uno strumento conforme SCAP, mensilmente o più frequentemente.	Applicazioni	Identificare		●	●
7.7	**Correggere le Vulnerabilità Rilevate** Correggere le vulnerabilità rilevate nel software per mezzo di strumenti e procedure, mensilmente o più frequentemente, secondo la procedura di correzione.	Applicazioni	Rispondere		●	●

CONTROLLI 08

Gestione dei Log di Controllo

SAFEGUARDS TOTAL	12	IG1	3/12	IG2	11/12	IG3	12/12

Panoramica

Raccogliere, avvisare, esaminare e conservare i log di controllo degli eventi che potrebbero aiutare a rilevare, comprendere o rimediare in seguito ad un attacco.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
8.1	**Stabilire e Mantenere una Procedura di Gestione dei Log di Controllo** Stabilire e mantenere una procedura di gestione dei log di controllo che soddisfi i requisiti di registrazione. Come minimo, salvare i log delle risorse aziendali, per la loro revisione e conservazione. Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Rete	Proteggere	●	●	●
8.2	**Raccogliere i Log di Controllo** Raccogliere i log di controllo. Assicurare che la procedura aziendale di gestione dei log sia attivata su tutti i dispostivi aziendali .	Rete	Rilevare	●	●	●
8.3	**Assicurare un Spazio Adeguato per l'Archiviazione dei Log** Assicurare che le destinazioni di archiviazione dei log mantengano uno spazio adeguato per adattarsi al processo aziendale di gestione dei log di controllo.	Rete	Proteggere	●	●	●
8.4	**Standardizzare la Sincronizzazione dell'Orario** Standardizzare la sincronizzazione dell'orario. Configurare almeno due sorgenti orarie sulle risorse aziendali, se supportato.	Rete	Proteggere		●	●
8.5	**Raccogliere i Log di Controllo Dettagliati** Configurare il logging dettagliato per le risorse aziendali che contengono dati sensibili. Includere l'origine dell'evento, data, nome utente, marca temporale, indirizzo di origine e di destinazione, ed altri elementi utili che potrebbero aiutare in una indagine forense.	Rete	Rilevare		●	●
8.6	**Raccogliere i Log di Controllo del DNS** Raccogliere i log di controllo delle query DNS sulle risorse aziendali, ove appropriato e supportato..	Rete	Rilevare		●	●
8.7	**Raccogliere i Log di Controllo delle Richieste URL** Raccogliere i log di controllo delle richieste URL, ove appropriato e supportato.	Rete	Rilevare		●	●
8.8	**Raccogliere i Log di Controllo dai Command-Line** Raccogliere i log di controllo delle interfacce command-line. Esempi di implementazione includono la raccolta dei log di PowerShell®, BASH™, e terminali di amministrazione remota.	Dispositivi	Rilevare		●	●
8.9	**Centralizzare i Log di Controllo** Centralizzare, per quanto possibile, raccolta e conservazione dei log di controllo delle risorse aziendali.	Rete	Rilevare		●	●
8.10	**Conservare i Log di Controllo** Conservare i log di controllo delle risorse aziendali per un minimo di 90 giorni.	Rete	Proteggere		●	●
8.11	**Effettuare le Revisioni dei Log di Controllo** Effettuare le revisioni dei log di controllo per rilevare anomalie o eventi inconsueti che potrebbero indicare una potenziale minaccia. Attuare i controlli su base settimanale o più frequentemente.	Rete	Rilevare		●	●
8.12	**Raccogliere i Log dei Fornitori di Servizi** Raccogliere i log dei fornitori di servizi, se supportati. Esempi di implementazione includono la raccolta di eventi di autenticazione e autorizzazione, eventi di creazione ed eliminazione di dati ed eventi di gestione degli utenti.	Dati	Rilevare			●

CONTROLLI 09

Protezione della Posta elettronica e del Browser Web

SAFEGUARDS TOTAL	7	IG1	2/7	IG2	6/7	IG3	7/7

Panoramica

Migliorare le protezioni ed il rilevamento delle minacce provenienti dalle e-mail e da vettori web, che danno l'opportunità agli aggressori di manipolare il comportamento umano sfruttandone il diretto coinvolgimento.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
9.1	**Assicurare l'Utilizzo di Client E-mail e di Browser Pienamente Supportati** Assicurare che venga permessa l'esecuzione solo di client di posta elettronica e di browser pienamente supportati ed aggiornati alla versione più recente rilasciata dal fornitore.	Applicazioni	Proteggere	●	●	●
9.2	**Utilizzare Servizi di Filtro DNS** Utilizzare i servizi di filtro DNS su tutte le risorse aziendali per bloccare l'accesso ai domini riconosciuti come pericolosi.	Rete	Proteggere	●	●	●
9.3	**Mantenere ed Applicare i Filtri URL di Rete** Applicare ed aggiornare i filtri URL di rete per limitare la connessione di una risorsa aziendale a siti Web potenzialmente dannosi o non approvati. Esempi di implementazione includono i filtri basati sulla categoria, i filtri basati sulla reputazione o tramite l'uso di elenchi di blocco. Applicare i filtri su tutte le risorse aziendali.	Rete	Proteggere		●	●
9.4	**Limitare le Estensioni di Browser e Client E-Mail non Necessarie o non Autorizzate** Limitare, disinstallando o disattivando dal browser o dal client di posta elettronica, qualsiasi estensione, plug-in e applicazione add-on, non autorizzata o non necessaria.	Applicazioni	Proteggere		●	●
9.5	**Implementare DMARC** Per ridurre la possibilità di e-mail contraffatte o modificate da domini validi, implementare le policy e le verifiche DMARC, iniziando con l'implementazione del Sender Policy Framework (SPF) e degli standard di Chiave Identificativa Dominio Mail (DKIM).	Rete	Proteggere		●	●
9.6	**Bloccare i Tipi di File non Necessari** Bloccare i tipi di file non necessari in ingresso sul gateway di posta elettronica aziendale.	Rete	Proteggere		●	●
9.7	**Installare e Mantenere le Protezioni Anti-Malware del Server di Posta** Installare e mantenere le protezioni anti-malware del server di posta, esempio scansione degli allegati e/o sandboxing.	Rete	Proteggere			●

CONTROLLI 10

Difesa dal Malware

SAFEGUARDS TOTAL	IG1	IG2	IG3
7	3/7	7/7	7/7

Panoramica

Prevenire o controllare installazione, diffusione ed esecuzione di applicazioni, codici o script dannosi sulle risorse aziendali.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
10.1	**Distribuire e Mantenere il Software Anti-Malware** Distribuire e mantenere il software anti-malware su tutte le risorse aziendali.	Dispositivi	Proteggere	●	●	●
10.2	**Configurare gli Aggiornamenti Automatici delle Firme Anti-Malware** Configurare gli aggiornamenti automatici dei file delle firme anti-malware su tutte le risorse aziendali.	Dispositivi	Proteggere	●	●	●
10.3	**Disabilitare Esecuzione e Riproduzione Automatica per i Supporti Rimovibili** Disabilitare l'esecuzione e la riproduzione automatica per i supporti rimovibili.	Dispositivi	Proteggere	●	●	●
10.4	**Configurare la Scansione Automatica dei Supporti Rimovibili** Configurare il software anti-malware per la scansione automatica dei supporti rimovibili.	Dispositivi	Rilevare		●	●
10.5	**Abilitare le Funzioni Anti-Exploit** Abilitare le funzioni anti-exploit sui software e sui dispositivi aziendali, se possibile, come ad esempio Microsoft® Prevenzione di Esecuzione in area Dati (DEP), Windows® Defender Exploit Guard (WDEG), Apple® Protezione di Integrità del Sistema (SIP), Gatekeeper™.	Dispositivi	Proteggere		●	●
10.6	**Gestire Centralmente il Software Anti-Malware** Gestire in modo centralizzato il software anti-malware.	Dispositivi	Proteggere		●	●
10.7	**Utilizzare un Software Anti-Malware Basato sul Comportamento** Utilizzare un software anti-malware basato sul comportamento.	Dispositivi	Rilevare		●	●

CONTROLLI 11

Recupero dei Dati

SAFEGUARDS TOTAL	IG1	IG2	IG3
5	4/5	5/5	5/5

Panoramica

Stabilire e mantenere sufficienti procedure di ripristino dei dati per riportare le risorse aziendali in funzione ad uno stato attendibile di pre-incidente.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
11.1	**Stabilire e Mantenere una Procedura di Recupero dei Dati** Stabilire e mantenere una procedura di recupero dei dati. Definire l'ambito delle attività di ripristino dei dati, la priorità del ripristino e la sicurezza dei dati di backup. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Recuperare	●	●	●
11.2	**Eseguire Backup Automatizzati** Eseguire backup automatizzati delle risorse aziendali in funzione. Eseguire il backup settimanalmente o più frequentemente, in base alla sensibilità dei dati.	Dati	Recuperare	●	●	●
11.3	**Proteggere i Dati di Ripristino** Proteggere i dati di ripristino con controlli equivalenti ai dati originali. Applicare la crittografia necessaria o separare i dati in funzione dei requisiti.	Dati	Proteggere	●	●	●
11.4	**Stabilire e Mantenere una Istanza Isolata dei Dati di Ripristino** Stabilire e mantenere un'istanza isolata dei dati di ripristino. Le implementazioni di esempio includono il controllo della versione delle destinazioni di backup tramite sistemi o servizi offline, cloud e off-site.	Dati	Recuperare	●	●	●
11.5	**Recupero Dati di Prova** Testare il ripristino del backup trimestralmente, o con maggiore frequenza, per un campione di risorse aziendali in funzione.	Dati	Recuperare		●	●

CONTROLLI 12

Gestione dell'Infrastruttura di Rete

SAFEGUARDS TOTAL	8	IG1	1/8	IG2	7/8	IG3	8/8

Panoramica

Stabilire, implementare e gestire attivamente (tracciando, segnalando, correggendo) i dispositivi di rete, al fine di impedire agli aggressori di sfruttarne servizi e punti di accesso vulnerabili.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
12.1	**Assicurare l'Aggiornamento dell'Infrastruttura di Rete** Assicurare che l'infrastruttura di rete sia sempre aggiornata. Esempi di implementazione includono l'esecuzione dell'ultima versione stabile del software e / o l'utilizzo delle potenzialità NaaS (network-as-a-service) attualmente disponibili. Rivedere le versioni del software mensilmente o più frequentemente per verificarne il supporto	Rete	Proteggere	●	●	●
12.2	**Stabilire e Mantenere una Architettura di Rete Sicura** Stabilire e mantenere un'architettura di rete sicura. Un'architettura di rete sicura deve prevedere almeno la segmentazione, i privilegi minimi e la disponibilità.	Rete	Proteggere		●	●
12.3	**Gestione Sicura dell'Infrastruttura di Rete** Gestire in sicurezza l'infrastruttura di rete. Esempi di implementazione includono il controllo di versione dell'infrastruttura tramite codice e l'uso di protocolli di rete sicuri, come SSH e HTTPS.	Rete	Proteggere		●	●
12.4	**Stabilire e Mantenere il / i Diagramma / i dell'Architettura** Stabilire e mantenere i diagrammi dell'architettura e / o altra documentazione del sistema di rete. Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Rete	Identificare		●	●
12.5	**Centralizzare Autenticazione, Autorizzazione e Auditing di Rete** Centralizzare AAA di rete.	Rete	Proteggere		●	●
12.6	**Utilizzare Protocolli Sicuri di Gestione e Comunicazione della Rete** Utilizzare protocolli sicuri di gestione e comunicazione della rete (esempio 802.1X, Protocollo di Accesso Wi-Fi 2–WPA2 versione Enterprise o superiore)	Rete	Proteggere		●	●
12.7	**Assicurare l'Utilizzo di VPN per i Dispositivi Remoti e Connessione AAA all'Infrastruttura Aziendale** Richiedere agli utenti l'autenticazione alla VPN aziendale e ai servizi di autenticazione prima dell'accesso alle risorse aziendali dai dispositivi degli utenti finali.	Dispositivi	Proteggere		●	●
12.8	**Stabilire e Mantenere Risorse Informatiche Dedicate per tutto il Lavoro Amministrativo** Stabilire e mantenere risorse informatiche dedicate, fisicamente o logicamente separate, per tutte le attività amministrative o che richiedano l'accesso amministrativo. Le risorse informatiche dovrebbero essere segmentate dalla rete primaria dell'azienda e non avere accesso a Internet.	Dispositivi	Proteggere			●

CONTROLLI 13

Monitoraggio e Difesa della Rete

SAFEGUARDS TOTAL	IG1	IG2	IG3
11	0/11	6/11	11/11

Panoramica

Adottare processi e strumenti per stabilire e mantenere un monitoraggio completo della rete e una difesa contro le minacce alla sicurezza dell'infrastruttura di rete aziendale e agli utenti.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
13.1	**Centralizzare gli Avvisi degli Eventi di Sicurezza** Centralizzare gli avvisi degli eventi di sicurezza delle risorse aziendali per la correlazione ed analisi dei log. L'implementazione delle best practice prevede l'uso di un SIEM, che includa gli avvisi di correlazione degli eventi definiti dal fornitore. Anche una piattaforma di analisi dei log configurata con avvisi di sicurezza correlati e rilevanti soddisfa questa salvaguardia.	Rete	Rilevare		●	●
13.2	**Adottare una Soluzione di Rilevamento Intrusioni Basata su Host** Adottare una soluzione di rilevamento delle Intrusioni basata su host sulle risorse aziendali, ove appropriato e/o supportato	Dispositivi	Rilevare		●	●
13.3	**Adottare una Soluzione di Rilevamento Intrusioni Basata sulla Rete** Adottare una soluzione di rilevamento delle intrusioni basata sulla rete sulle risorse aziendali, ove appropriato. Esempi di implementazione includono l'utilizzo di un Sistema di Rete per il Rilevamento delle Intrusioni (NIDS) o un servizio fornito in cloud equivalente (CSP)	Rete	Rilevare		●	●
13.4	**Filtrare il Traffico tra i Segmenti di Rete** Filtrare il traffico tra i segmenti di rete ove appropriato	Rete	Proteggere		●	●
13.5	**Gestire il Controllo degli Accessi per le Risorse Remote** Gestire il controllo degli accessi per le risorse che si connettono da remoto alle dotazioni aziendali. Determinare il numero di accessi in base a: software anti-malware aggiornato installato, conformità della configurazione sicura relativamente al processo definito dall'azienda, verifica di aggiornamento del sistema operativo e delle applicazioni.	Dispositivi	Proteggere		●	●
13.6	**Salvare i Log del Flusso di Traffico di Rete** Salvare i log del flusso di traffico di rete e / o il traffico di rete per esaminare e inviare avvisi dai dispositivi di rete.	Rete	Rilevare		●	●
13.7	**Adottare una Soluzione di Prevenzione delle Intrusioni Basata su Host** Adottare una soluzione di prevenzione delle intrusioni basata su host sulle risorse aziendali, ove appropriato e / o supportato. Esempi di implementazione includono l'uso di un client Endpoint di Rilevamento e Risposta (EDR) o di un agent IPS basato su host.	Dispositivi	Proteggere			●
13.8	**Adottare una Soluzione di Prevenzione delle Intrusioni Basata sulla Rete** Adottare una soluzione di prevenzione delle intrusioni di rete, ove appropriato. Esempi di implementazione includono l'uso di un sistema di prevenzione delle intrusioni di rete (NIPS) o di un servizio CSP equivalente.	Rete	Proteggere			●
13.9	**Implementare il Controllo degli Accessi a Livello di Porta** Adottare il controllo degli accessi a livello di porta che utilizzi 802.1x o protocolli di controllo di accesso alla rete simili, come i certificati, includendo l'autenticazione dell'utente e / o del dispositivo.	Dispositivi	Proteggere			●
13.10	**Eseguire il Filtraggio a Livello di Applicazione** Eseguire il filtraggio a livello di applicazione. Esempi di implementazione includono un proxy di filtraggio, un firewall a livello di applicazione o un gateway.	Rete	Proteggere			●
13.11	**Perfezionare le Soglie di Avviso degli Eventi di Sicurezza** Ottimizzare le soglie di avviso degli eventi di sicurezza mensilmente o più.	Rete	Rilevare			●

CONTROLLI 14

Sensibilizzazione e Formazione sulle Competenze di Sicurezza

SAFEGUARDS TOTAL	IG1	IG2	IG3
9	8/9	9/9	9/9

Panoramica

Stabilire e mantenere un programma di sensibilizzazione alla sicurezza per istruire il personale affinché sia consapevole ed adeguatamente preparato per ridurre i rischi di sicurezza informatica aziendali.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
14.1	**Stabilire e Mantenere un Programma di Sensibilizzazione alla Sicurezza** Stabilire e mantenere un programma di sensibilizzazione alla sicurezza. Lo scopo è quello di istruire il personale su come interagire con le risorse e i dati aziendali in modo sicuro. Effettuare la formazione al momento dell'assunzione e, come minimo, annualmente. Rivedere e aggiornare i contenuti annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	N/A	Proteggere	●	●	●
14.2	**Formare il Personale nel Riconoscimento degli Attacchi Social Engineering** Formare il personale nel riconoscimento degli attacchi social engineering, come il phishing, pre-texting e tailgating.	N/A	Proteggere	●	●	●
14.3	**Formare il Personale sulle Migliori Tecniche di Autenticazione** Formare il personale sulle migliori tecniche di autenticazione. Alcuni esempi includono MFA, composizione delle password e gestione delle credenziali.	N/A	Proteggere	●	●	●
14.4	**Formare il Personale sulle Migliori Tecniche di Gestione dei Dati** Formare il personale su come identificare, salvare trasferire, archiviare e cancellare in modo appropriato i dati sensibili. È compresa la formazione del personale sulla disattivazione dello schermo quando viene lasciata la postazione, sulla cancellazione di lavagne fisiche o virtuali a fine riunione, sull'archiviazione sicura di dati e risorse	N/A	Proteggere	●	●	●

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
14.5	**Formare il Personale sulle Cause di Esposizione Involontaria di Dati** Formare il personale sulle cause di esposizione involontaria di dati. Alcuni esempi includono l'errato trasferimento di dati sensibili, la perdita di un dispositivo portatile dell'utente finale o la pubblicazione di dati non dovuta.	N/A	Proteggere	●	●	●
14.6	**Formare il Personale sul Riconoscimento e Segnalazione degli Incidenti di Sicurezza** Formare il personale affinché riconosca un potenziale incidente e possa segnalarlo	N/A	Proteggere	●	●	●
14.7	**Formare il Personale su Identificazione e Segnalazione di Mancati Aggiornamenti dei Dispositivi Aziendali** Formare il personale per capire come verificare e segnalare un mancato aggiornamento automatizzato di uno strumento o procedura. Parte di questa formazione dovrebbe prevedere la modalità di segnalazione al personale IT di qualsiasi malfunzionamento di strumenti o procedure automatizzati.	N/A	Proteggere	●	●	●
14.8	**Formare il Personale sui Pericoli di Connessione e Trasmissione di Dati Aziendali su Reti non Sicure** Formare il personale sui pericoli della connessione e della trasmissione di dati su reti non sicure per le attività aziendali. Se l'azienda dispone di lavoratori remoti, la formazione deve includere le indicazioni per garantire che tutti gli utenti configurino in modo sicuro la propria infrastruttura di rete domestica.	N/A	Proteggere	●	●	●
14.9	**Effettuare una Formazione Specifica sulla Competenze e per la Sensibilizzazione sulla Sicurezza** Effettuare una formazione specifica sulle competenze e per la sensibilizzazione sulla sicurezza. Esempi di implementazione includono corsi di amministrazione sicura dei sistemi per il personale IT (OWASP® Top 10 sulla consapevolezza e prevenzione delle vulnerabilità per sviluppatori di applicazioni Web e formazione avanzata sulla sensibilizzazione social engineering per ruoli di alto profilo).	N/A	Proteggere		●	●

CONTROLLI 15

Gestione dei Service Provider

SAFEGUARDS TOTAL	7	IG1	1/7	IG2	4/7	IG3	7/7

Panoramica

Sviluppare una procedura per valutare i Service Provider che detengono dati sensibili o sono responsabili delle piattaforme o dei processi IT aziendali più importanti, per assicurarsi che proteggano tali piattaforme ed i dati in modo appropriato.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
15.1	**Stabilire e Mantenere un Inventario dei Service Providers** Stabilire e mantenere un inventario dei service providers. L'inventario deve riportare tutti i service providers conosciuti, compresa la classificazione e il contatto aziendale designato. Rivedere ed aggiornare l'inventario annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	N/A	Identificare	●	●	●
15.2	**Stabilire e Mantenere un Criterio di Gestione del Service Provider** Stabilire e mantenere un criterio di gestione del service provider. Garantire che i criteri includano la classificazione, l'inventario, la valutazione, il monitoraggio e la disattivazione dei service provider. Rivedere ed aggiornare i criteri annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	N/A	Identificare		●	●
15.3	**Classificare i Service Providers** Classificare i service provider. La classificazione può includere una o più caratteristiche, come la sensibilità dei dati, volume dei dati, requisiti di disponibilità, normative applicabili, rischio intrinseco e rischio mitigato. Rivedere ed aggiornare la classificazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	N/A	Identificare		●	●
15.4	**Garantire che i Contratti dei Service Provider Includano Requisiti di Sicurezza** Garantire che i contratti dei service provider includano i requisiti di sicurezza. Esempi di requisiti possono includere: requisiti minimi del programma di sicurezza, notifica e risposta di incidenti di sicurezza e / o violazione dei dati, requisiti di crittografia dei dati e procedure di dismissione dei dati. Questi requisiti di sicurezza devono essere coerenti con la politica di gestione del service provider aziendale. Rivedere i contratti del service provider annualmente per garantire la presenza di tali requisiti.	N/A	Proteggere		●	●
15.5	**Valutare i Service Provider** Valutare i service provider aziendali in coerenza con i relativi criteri di gestione. La valutazione può variare in base alle classificazioni e può includere la revisione di rapporti di valutazione standardizzati, come il Servizio di Controllo Organizzazione 2 (SOC 2) e l'Attestato di Conformità (AoC) del Settore delle Carte di Pagamento (PCI), questionari personalizzati o altre adeguate e rigorose procedure. Rivalutare i fornitori di servizi annualmente o in occasione nuovo contratto o di suo di rinnovo.	N/A	Identificare			●
15.6	**Controllare i Service Providers** Controllare i service provider aziendali in coerenza con i relativi criteri di gestione. Il monitoraggio può includere una rivalutazione periodica della conformità, il monitoraggio delle note di rilascio e il monitoraggio del dark web.	Dati	Rilevare			●
15.7	**Disattivazione Sicura dei Service Providers** Disattivazione sicura dei service providers. Esempi di considerazioni includono la disattivazione degli account utente e di servizio, l'interruzione dei flussi di dati e la rimozione sicura dei dati aziendali dai sistemi.	Dati	Proteggere			●

CONTROLLI **16**

Sicurezza degli Applicativi

SAFEGUARDS TOTAL	14	IG1	0/14	IG2	11/14	IG3	14/14

Panoramica

Gestire la sicurezza del ciclo di vita del software sviluppato in proprio, ospitato o acquistato per prevenire, rilevare e rimediare ai punti deboli di sicurezza prima che possano impattare sull'azienda.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
16.1	**Stabilire e Mantenere una Procedura di Sviluppo Sicuro delle Applicazioni** Stabilire e mantenere una procedura di sviluppo sicuro delle applicazioni. In questo procedimento si considerino elementi quali: standard di progettazione di applicazioni sicure, pratiche di codifica sicura, formazione per gli sviluppatori, gestione delle vulnerabilità, sicurezza del codice di terze parti e procedure di test di sicurezza delle applicazioni. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	Applicazioni	Proteggere		●	●
16.2	**Stabilire e Mantenere una Procedura di Accettazione e Risoluzione delle Vulnerabilità** Stabilire e mantenere una procedura di accettazione e risoluzione delle segnalazioni di vulnerabilità del software, inclusa quella dedicata per la segnalazione da parte di entità esterne. Il procedimento deve includere elementi quali: un criterio di gestione delle vulnerabilità che identifichi il processo di segnalazione, il responsabile della gestione delle segnalazioni di vulnerabilità e un sistema per la presa in carico, l'assegnazione, la risoluzione e la relativa verifica. Come parte del processo, utilizzare un sistema di rilevamento delle vulnerabilità che includa livelli di gravità e metriche per misurarne i tempi di identificazione, analisi e correzione. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa salvaguardia. Gli sviluppatori di applicazioni di terze parti devono rendere pubblici questi criteri al fine di soddisfare le aspettative delle parti interessate	Applicazioni	Proteggere		●	●
16.3	**Eseguire l'Analisi della Causa Principale sulle Vulnerabilità della Sicurezza** Eseguire l'analisi della causa principale sulle vulnerabilità della sicurezza. Quando si esaminano le vulnerabilità, l'analisi della causa principale è il lavoro di valutazione dell'origine sottostante che crea il punto debole nel codice permettendo ai team di sviluppo di andare oltre la semplice correzione dei singoli problemi quando si presentano.	Applicazioni	Proteggere		●	●
16.4	**Stabilire e Gestire un Inventario di Componenti Software di Terze Parti** Stabilire e gestire un inventario aggiornato dei componenti di terze parti utilizzati nello sviluppo, spesso indicato come "distinta del materiale", nonché dei componenti previsti per un uso futuro. Questo inventario deve includere i rischi che ogni componente di terzi potrebbe comportare. Valutare l'elenco almeno mensilmente per identificare eventuali modifiche o aggiornamenti a questi componenti e verificarne il corrente supporto.	Applicazioni	Proteggere		●	●
16.5	**Utilizzare Componenti Software di Terze Parti Aggiornati** Utilizzare componenti software di terze parti aggiornati e affidabili. Quando possibile, scegliere framework e librerie consolidati e comprovati che forniscano una sicurezza adeguata. Acquisire questi componenti da fonti attendibili o valutare le vulnerabilità del software prima dell'uso.	Applicazioni	Proteggere		●	●
16.6	**Stabilire e Mantenere un Sistema di Valutazione della Gravità e una Procedura per le Vulnerabilità delle Applicazioni** Stabilire e mantenere un sistema di valutazione della gravità e una procedura per le vulnerabilità delle applicazioni che faciliti la priorità dell'ordine in cui vengono scoperte e risolte. Questo processo include la definizione di un livello minimo di accettabilità di sicurezza per il rilascio di codice o applicazioni. I livelli di gravità offrono un modo sistematico di valutazione delle vulnerabilità che migliorano la gestione del rischio e aiutano a garantire che i bug più gravi vengano corretti per primi. Rivedere e aggiornare il sistema e la procedura annualmente.	Applicazioni	Proteggere		●	●
16.7	**Utilizzare Modelli di Hardening Standard per la Configurazione dell'Infrastruttura Applicativa** Utilizzare modelli di hardening standard di tipo industriale per la configurazione dei componenti dell'infrastruttura applicativa. Ciò include i relativi server, i database, i server web e si applica ai contenitori cloud, ai componenti Platform as a Service (PaaS) e ai componenti SaaS. Non consentire al software sviluppato internamente di indebolire l'hardening della configurazione.	Applicazioni	Proteggere		●	●
16.8	**Separare i Sistemi in Produzione e da quelli non in Produzione** Mantenere ambienti separati tra i sistemi in produzione e quelli non in produzione	Applicazioni	Proteggere		●	●
16.9	**Formare gli Sviluppatori sui Concetti di Sicurezza delle Applicazioni e sulla Codifica Sicura** Garantire che tutto il personale di sviluppo software riceva formazione sulla scrittura di codice sicuro per il proprio ambiente di sviluppo e le proprie responsabilità. La formazione può includere principi generali di sicurezza e pratiche standard di sicurezza delle applicazioni. Predisporre la formazione almeno annualmente e progettandola in modo da promuovere la sicurezza all'interno del team di sviluppo e favorire la cultura della sicurezza tra gli sviluppatori.	Applicazioni	Proteggere		●	●
16.10	**Applicare Principi di Progettazione Sicura nelle Architetture Applicative** Applicare principi di progettazione sicura nelle architetture applicative. I principi di progettazione sicura includono il concetto di privilegio minimo e l'applicazione della mediazione per validare ogni operazione eseguita dall'utente, applicando il concetto di "non fidarsi mai dell'input dell'utente". Gli esempi includono la garanzia che il controllo degli errori espliciti venga eseguito e documentato per tutti gli input, inclusi dimensioni, tipi di dati, intervalli o formati accettabili. Progettazione sicura significa anche ridurre al minimo la superficie di attacco dell'infrastruttura dell'applicazione, disattivando porte e servizi non protetti, rimuovendo programmi e file non necessari e rinominando o rimuovendo gli account predefiniti..	Applicazioni	Proteggere		●	●
16.11	**Utilizzare Moduli o Servizi Controllati per i Componenti di Sicurezza delle Applicazioni** Utilizzare moduli o servizi controllati per i componenti di sicurezza delle applicazioni, come la gestione delle identità, la crittografia, il controllo e il logging. L'utilizzo delle funzionalità della piattaforma nelle funzioni di sicurezza più importanti ridurrà il carico di lavoro degli sviluppatori e ridurrà al minimo la probabilità di errori di progettazione o implementazione. I sistemi operativi moderni forniscono meccanismi efficaci per l'identificazione, l'autenticazione e l'autorizzazione e li rendono disponibili per le applicazioni. Utilizzare solo algoritmi di crittografia standardizzati, attualmente accettati e ampiamente controllati. I sistemi operativi forniscono anche meccanismi per creare e mantenere i log di controllo	Applicazioni	Proteggere		●	●
16.12	**Implementare Controlli di Sicurezza a Livello di Codice** Applicare strumenti di analisi statica e dinamica nel ciclo di vita dell'applicazione per verificare che vengano seguite pratiche di codifica sicura.	Applicazioni	Proteggere			●
16.13	**Effettuare Test di Penetrazione sull'Applicazione** Effettuare test di penetrazione sulle applicazioni. Per le applicazioni critiche, i test di penetrazione autenticati sono più adatti per trovare vulnerabilità rispetto alla scansione del codice e ai test di sicurezza automatizzati. Il test di penetrazione si basa sull'abilità del tester di manipolare un'applicazione come utente autenticato e non autenticato.	Applicazioni	Proteggere			●
16.14	**Effettuare la Modellazione delle Minacce** Effettuare la modellazione delle minacce. Consiste nell'identificazione e risoluzione dei difetti di progettazione della sicurezza delle applicazioni all'interno di un progetto, prima della creazione del codice. Viene realizzata attraverso personale appositamente addestrato che valuta la progettazione dell'applicazione misurando i rischi per la sicurezza per ogni punto di ingresso e livello di accesso. L'obiettivo è mappare l'applicazione, l'architettura e l'infrastruttura in modo strutturato per comprenderne i punti deboli.	Applicazioni	Proteggere			●

CONTROLLI 17

Gestione e Risposta agli Incidenti

SAFEGUARDS TOTAL	9	IG1	3/9	IG2	8/9	IG3	9/9

Panoramica

Stabilire un programma per sviluppare e mantenere una capacità di risposta agli incidenti (ad esempio criteri, piani, procedure, ruoli definiti, formazione e comunicazioni) per prepararsi a rilevare e rispondere rapidamente ad un attacco.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
17.1	**Designare il Personale Incaricato per la Gestione degli Incidenti** Designare una persona chiave e almeno un sostituto che dirigerà la procedura di gestione degli incidenti. Il personale di gestione è responsabile del coordinamento e della documentazione delle attività di risposta e agli incidenti e relativo ripristino; ci si può avvalere di dipendenti interni, terzi o scegliendo una soluzione ibrida. Se si utilizza un fornitore di terze parti, designare almeno una persona interna all'azienda per supervisionarne il lavoro. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere	●	●	●
17.2	**Stabilire e Mantenere le Informazioni di Contatto per la Segnalazione degli Incidenti di Sicurezza** Stabilire e mantenere l'elenco delle figure che devono essere informate degli incidenti di sicurezza. I contatti possono includere personale interno, fornitori di terze parti, forze dell'ordine, compagnie di assicurazione informatica, agenzie governative, partner del Centro di Condivisione e Analisi delle Informazioni (ISAC) o altre parti interessate. Verificare i contatti annualmente per garantire che le informazioni siano aggiornate.	N/A	Rispondere	●	●	●
17.3	**Stabilire e Mantenere una Procedura Aziendale di Segnalazione degli Incidenti** Stabilire e mantenere una procedura per il personale aziendale per segnalare gli incidenti di sicurezza. Sono inclusi i tempi di segnalazione, il personale di riferimento, il meccanismo di segnalazione e le informazioni minime da riportare. Assicurare che il procedimento sia disponibile pubblicamente per tutto il personale. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere	●	●	●
17.4	**Stabilire e Mantenere una Procedura di Risposta agli Incidenti** Stabilire e mantenere una procedura di risposta agli incidenti che preveda ruoli e responsabilità, requisiti di conformità e un piano di comunicazione. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere		●	●
17.5	**Assegnare Ruoli Chiave e Responsabilità** Assegnare ruoli chiave e responsabilità per la risposta agli incidenti, incluso il personale legale, IT, sicurezza delle informazioni, strutture, pubbliche relazioni, risorse umane, referenti di incidenti e analisti, se possibile. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere		●	●
17.6	**Definire i Meccanismi di Comunicazione Durante la Risposta agli Incidenti** Determinare quali modalità primarie e secondarie verranno utilizzati per comunicare e segnalare durante un incidente di sicurezza. I meccanismi possono includere telefonate, e-mail o lettere. Tenere presente che determinati meccanismi, come le e-mail, potrebbero non funzionare in seguito ad un incidente di sicurezza. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere		●	●
17.7	**Condurre Esercizi di Routine in Risposta agli Incidenti** Pianificare e condurre esercizi di routine e scenari in risposta agli incidenti per il personale chiave coinvolto nella procedura per prepararlo a fronteggiare l'eventualità in casi reali. Gli esercizi devono testare i canali di comunicazione, il processo decisionale e i flussi di lavoro. Effettuare test almeno su base annuale.	N/A	Recuperare		●	●
17.8	**Effettuare Revisioni Post-Incidente** Effettuare revisioni post-incidente. Le revisioni post-incidente aiutano a prevenire il ripetersi di incidenti attraverso l'identificazione delle lezioni apprese e l'azione di follow-up.	N/A	Recuperare		●	●
17.9	**Stabilire e Mantenere i Livelli per gli Incidenti di Sicurezza** Stabilire e mantenere i livelli per gli incidenti di sicurezza, inclusa, come minimo, la differenziazione tra un incidente e un evento. Gli esempi possono includere: attività anomale, vulnerabilità della sicurezza, debolezza della sicurezza, violazione dei dati, incidente di privacy, ecc. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Recuperare			●

CONTROLLI 18

Test di Penetrazione

SAFEGUARDS TOTAL	5	IG1	0/5	IG2	3/5	IG3	5/5

Panoramica

Verificare l'efficacia e la resilienza delle risorse aziendali identificando e sfruttando i punti deboli nei controlli (persone, processi e tecnologia) e simulando obiettivi ed azioni di un utente malintenzionato.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
18.1	**Stabilire e Mantenere un Programma di Test di Penetrazione** Stabilire e mantenere un programma di test di penetrazione adeguato alle dimensioni, alla complessità e alla maturità dell'azienda. Le caratteristiche del programma di test di penetrazione includono ambiti di rete, applicazioni Web, API (Interfaccia di Programmazione di un'Applicazione), servizi ospitati e controlli della sede fisica; frequenza, limitazioni (come orari accettabili e tipi di attacco esclusi), informazioni sul punto di contatto, azioni di rimedio (come i risultati verranno indirizzati internamente), requisiti retroattivi.	N/A	Identificare		●	●
18.2	**Eseguire Periodicamente Test di Penetrazione Esterni** Eseguire periodicamente test di penetrazione esterni basati sui requisiti del programma, almeno annualmente. I test di penetrazione esterni devono includere l'ispezione dell'impresa e dell'ambiente per rilevare le informazioni soggette ad exploit. Questi test richiedono competenze ed esperienze specifiche e devono essere condotti da personale qualificato. I test possono avvenire in modalità "clear box" oppure "opaque box".	Rete	Identificare		●	●
18.3	**Correggere Considerando i Risultati del Test di Penetrazione** Rimediare in base ai risultati dei test di penetrazione considerando i criteri aziendali riferiti all'ambito di correzione ed ai livelli di priorità.	Rete	Proteggere		●	●
18.4	**Convalidare le Misure di Sicurezza** Convalidare le misure di sicurezza dopo ogni test di penetrazione. Se si ritiene necessario, modificare i set di regole e le capacità di rilevamento delle tecniche utilizzate durante i test.	Rete	Proteggere			●
18.5	**Eseguire Periodicamente Test di Penetrazione Interni** Eseguire periodicamente i test di penetrazione interni basati sui requisiti del programma, almeno annualmente. I test possono avvenire in modalità "clear box" oppure "opaque box".	N/A	Identificare			●

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Relationship	Control #	Control Title	Control Text
1				**Inventory and Control of Enterprise Assets** ***Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.***							
1	1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	X	X	X	Subset	5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.
1	1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	X	X	X	Subset	8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.
1	1.2	Devices	Respond	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	X	X	X				
1	1.3	Devices	Detect	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.		X	X				
1	1.4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.		X	X				
1	1.5	Devices	Detect	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.			X				