SOA - Statement of Applicability – ISO /IEC 27001:2022 - Annex A
DICHIARAZIONE DI APPLICABILITA' & PIANO DI SICUREZZA DELLE INFORMAZIONI

PIANO DI SICUREZZA DELLE INFORMAZIONI

L'organizzazione, all'interno del modulo **Identificazione e valutazione del rischio**, ha:

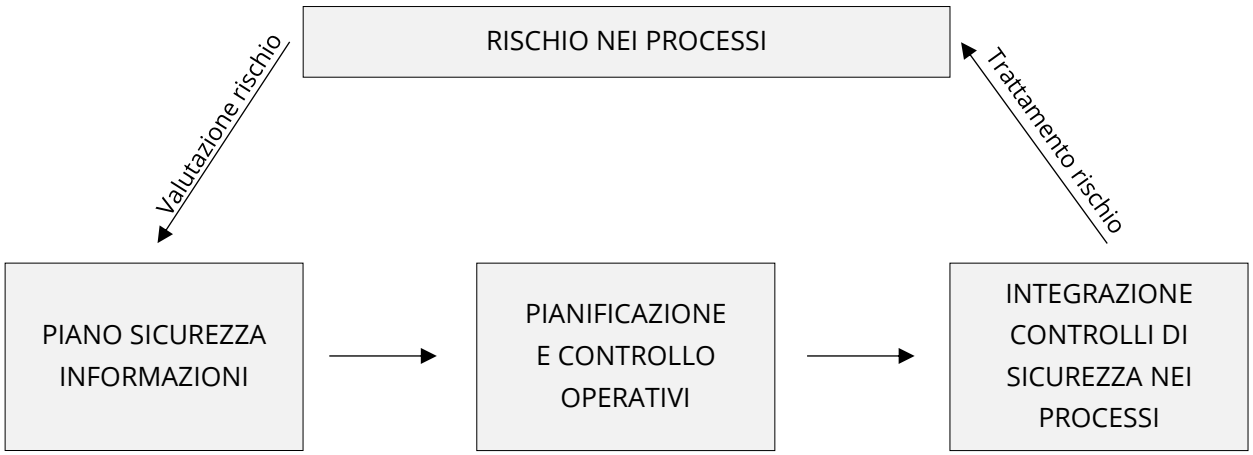
- Individuato e valutato i rischi per la sicurezza delle informazioni
- Classificato le informazioni da proteggere
- Collocato la presenza di tali informazioni all'interno di processi ben precisi
- Individuato le minacce che incombono sui singoli processi (sulle quali effettua attività di intelligence)

Il modulo indicato sopra, in sostanza, documenta l'attuazione delle azioni di pianificazione stabilite dalla procedura **Gestione rischi ed opportunità.**

Il presente **Piano di sicurezza delle informazioni** rappresenta la risposta alle condizioni di incertezza e di rischio riscontrate. L'organizzazione infatti, di seguito, ha stabilito i controlli di sicurezza che applicherà per affrontare il rischio.

A tale piano di sicurezza delle informazioni, segue una ulteriore pianificazione a carattere più operativo documentata nelle procedure che gestiscono il punto 8 della Norma e cioè le attività operative.

La parte riservata alla Pianificazione e controllo operativi, stabilita dalla Norma ISO 27001 al punto 8, è disciplinata dalla procedura **Pianificazione e controllo operativi.** Le successive procedure, del punto 8, documentano come, quanto pianificato in questo modulo, si trasferisce effettivamente nei processi dell'organizzazione attraverso l'integrazione dei controlli di sicurezza pianificati. La figura seguente illustra il percorso logico, dal rischio al suo trattamento.



SOA - Statement of Applicability – ISO /IEC 27001:2022 - Annex A
DICHIARAZIONE DI APPLICABILITA' & PIANO DI SICUREZZA DELLE INFORMAZIONI

DICHIARAZIONE DI APPLICABILITA'

Il **piano di sicurezza delle informazioni** adottato dalla nostra organizzazione elenca, nelle pagine a seguire, i controlli di sicurezza che abbiamo attuato per proteggere le informazioni che appartengono:

- Alle nostre attività operative di business
- Alle attività di business dei nostri committenti e dei nostri fornitori
- Alle persone fisiche delle rispettive organizzazioni

Di seguito, l'alta direzione dell'organizzazione, **nella persona Trotti Davide**, in relazione alle esigenze e alle aspettative delle parti interessate a cui tale documento è destinato, rilascia la seguente **dichiarazione di applicabilità in relazione al requisito 6.1.3 della Norma ISO 27001:2022**.

DICHIARA

di avere:

1. **Implementato il Sistema di Gestione** per la Sicurezza delle Informazioni ai sensi della ISO 27001:2022
2. **Conseguito la certificazione ISO 27001:2022**,
3. **Attuato i controlli di sicurezza** dell'Annex A previsti dalla Norma nella sua edizione 2022.

In relazione alla circostanza indicata, per il rilascio di tale Dichiarazione di Applicabilità resa ai sensi della Norma ISO 27001:2022, si fornisce di seguito il **Piano di sicurezza delle informazioni** adottato dall'organizzazione, nel quale abbiamo riportato:

1. La classe a cui i controlli di sicurezza applicati appartengono, secondo la suddivisione della Norma
2. Il numero identificativo del controllo riportato dall'Annex A della Norma
3. La denominazione del controllo
4. La descrizione del controllo
5. La documentazione comprovante l'attuazione del controllo

Ai fini di tale dichiarazione, si precisa che **il dr. Michelotto Carlo in qualità di CISO e il dr. RICCARDO PETRUZZELLIS**, in qualità di **Responsabile del sistema di gestione** per la sicurezza delle informazioni e amministratore di sistema, è **depositario della intera documentazione comprovante** l'attuazione dei controlli di sicurezza dichiarati nel Piano ed è incaricato di esibirla in relazione alle esigenze conoscitive della **vostra amministrazione in fase di istruttoria**.

Busto Arsizio (VA), lì 18 aprile 2024

FIRMA AD

.....

SOA - Statement of Applicability – ISO /IEC 27001:2022 - Annex A
DICHIARAZIONE DI APPLICABILITA' & PIANO DI SICUREZZA DELLE INFORMAZIONI

CONTROLLI ORGANIZZATIVI			
NUM	CONTROLLO	DESCRIZIONE	COLLOCAZIONE
5.1	Politiche per la sicurezza delle informazioni	La politica di sicurezza delle informazioni e le politiche specifiche per argomento devono essere definite, approvate dalla direzione, pubblicate, comunicate e riconosciute dal personale rilevante e dalle parti interessate pertinenti, e revisionate a intervalli pianificati e in caso di cambiamenti significativi.	Organizzazione del personale
5.2	Ruoli e responsabilità per la sicurezza delle informazioni	I ruoli e le responsabilità per la sicurezza delle informazioni devono essere definiti e assegnati in base alle esigenze dell'organizzazione.	Organizzazione del personale
5.3	Separazione dei compiti	I compiti in conflitto e le aree di responsabilità in conflitto devono essere separate.	Organizzazione del personale
5.4	Responsabilità della direzione	La direzione deve richiedere a tutto il personale di applicare la sicurezza delle informazioni in conformità con la politica di sicurezza delle informazioni stabilita, le politiche specifiche per argomento e le procedure dell'organizzazione.	Persone e competenze
5.5	Contatti con le autorità	L'organizzazione deve stabilire e mantenere contatti con le autorità pertinenti.	Organizzazione del personale
5.6	Contatti con gruppi di interesse speciale	L'organizzazione deve stabilire e mantenere contatti con gruppi di interesse speciale o altri forum specialistici sulla sicurezza e associazioni professionali.	Organizzazione del personale Persone e competenze
5.7	Intelligence sulle minacce	Le informazioni relative alle minacce alla sicurezza delle informazioni devono essere raccolte e analizzate per produrre intelligence sulle minacce.	Collocato sia on premise che nel cloud con gestione in tempo reale tramite EDR
5.8	Sicurezza delle informazioni nella gestione dei progetti	La sicurezza delle informazioni deve essere integrata nella gestione dei progetti.	Organizzazione del personale
5.9	Inventario delle informazioni e di altri asset associati	Deve essere sviluppato e mantenuto un inventario delle informazioni e degli altri asset associati, inclusi i proprietari.	Collocato nel cloud gestione tramite EDR
5.10	Utilizzo accettabile delle informazioni e di altri asset associati	Devono essere identificate, documentate e implementate regole per l'utilizzo accettabile e procedure per la gestione delle informazioni e degli altri asset associati.	Collocato nel cloud gestione tramite EDR

5.11	Restituzione degli asset	Il personale e altre parti interessate, se appropriato, devono restituire tutti gli asset dell'organizzazione in loro possesso al momento del cambiamento o della cessazione del loro impiego, contratto o accordo.	Gestione degli asset
5.12	Classificazione delle informazioni	Le informazioni devono essere classificate in base alle esigenze di sicurezza delle informazioni dell'organizzazione, in base a confidenzialità, integrità, disponibilità e requisiti pertinenti delle parti interessate.	Gestione rischi ed opportunità , EDR per la gestione del rischio e delle compliance
5.13	Etichettatura delle informazioni	Deve essere sviluppato e implementato un insieme appropriato di procedure per l'etichettatura delle informazioni, in conformità con lo schema di classificazione delle informazioni adottato dall'organizzazione.	Gestione rischi ed opportunità , EDR per la gestione del rischio e delle compliance
5.14	Trasferimento delle informazioni	Devono essere in vigore un insieme di regole, procedure o accordi per il trasferimento delle informazioni in tutti i tipi di strutture di trasferimento all'interno dell'organizzazione e tra l'organizzazione e altre parti.	Gestione degli asset
5.15	Controllo degli accessi	Devono essere stabilite e implementate regole per controllare l'accesso fisico e logico alle informazioni e ad altri asset associati, in base ai requisiti aziendali e di sicurezza delle informazioni.	Controllo d'accesso , Azure IAM con EDR
5.16	Gestione delle identità	Il ciclo di vita completo delle identità deve essere gestito.	Controllo d'accesso , Azure IAM con EDR
5.17	Informazioni di autenticazione	L'assegnazione e la gestione delle informazioni di autenticazione devono essere controllate da un processo gestionale, incluso l'avviso al personale sull'adeguato trattamento delle informazioni di autenticazione.	Controllo d'accesso , Azure IAM con EDR
5.18	Diritti di accesso	I diritti di accesso alle informazioni e ad altri asset associati devono essere forniti, revisionati, modificati e rimossi in conformità con la politica specifica per argomento e le regole dell'organizzazione per il controllo degli accessi.	Controllo d'accesso , Azure IAM con EDR
5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Devono essere definite e implementate procedure e processi per gestire i rischi per la sicurezza delle informazioni associati all'uso dei prodotti o servizi del fornitore.	Outsourcing
5.20	Affrontare la sicurezza delle informazioni nei contratti con i fornitori	Requisiti pertinenti per la sicurezza delle informazioni devono essere stabiliti e concordati con ciascun fornitore in base al tipo di relazione con il fornitore.	Outsourcing
5.21	Gestione della sicurezza delle informazioni nella catena di approvvigionamento ICT	Devono essere definiti e implementati processi e procedure per gestire i rischi per la sicurezza delle informazioni associati alla catena di approvvigionamento di prodotti e servizi ICT.	Outsourcing

5.22	Monitoraggio, revisione e gestione dei servizi dei fornitori	L'organizzazione deve monitorare regolarmente, revisionare, valutare e gestire i cambiamenti nelle pratiche di sicurezza delle informazioni e nella fornitura dei servizi da parte dei fornitori.	Outsourcing
5.23	Sicurezza delle informazioni per l'uso dei servizi cloud	Devono essere stabiliti processi per l'acquisizione, l'uso, la gestione e l'uscita dai servizi cloud in conformità con i requisiti di sicurezza delle informazioni dell'organizzazione.	Gestione degli asset , Azure IAM con EDR
5.24	Pianificazione e preparazione per la gestione degli incidenti di sicurezza delle informazioni	L'organizzazione deve pianificare e prepararsi per gestire gli incidenti di sicurezza delle informazioni definendo, istituendo e comunicando processi, ruoli e responsabilità per la gestione degli incidenti di sicurezza delle informazioni.	gestione incidenti , Azure IAM con EDR , framework Vera ISO 27001
5.25	Valutazione e decisione sugli eventi di sicurezza delle informazioni	L'organizzazione deve valutare gli eventi di sicurezza delle informazioni e decidere se devono essere categorizzati come incidenti di sicurezza delle informazioni.	gestione incidenti , Azure IAM con EDR , framework Vera ISO 27001
5.26	Risposta agli incidenti di sicurezza delle informazioni	Gli incidenti di sicurezza delle informazioni devono essere gestiti in conformità con le procedure documentate.	gestione incidenti Azure IAM con EDR , framework Vera ISO 27001
5.27	Apprendimento dagli incidenti di sicurezza delle informazioni	Le conoscenze acquisite dagli incidenti di sicurezza delle informazioni devono essere utilizzate per rafforzare e migliorare i controlli della sicurezza delle informazioni.	gestione incidenti Azure IAM con EDR , framework Vera ISO 27001
5.28	Raccolta di prove	L'organizzazione deve stabilire e implementare procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione di prove relative agli eventi di sicurezza delle informazioni.	gestione incidenti Azure IAM con EDR , framework Vera ISO 27001
5.29	Sicurezza delle informazioni durante la distruzione	L'organizzazione deve pianificare come mantenere la sicurezza delle informazioni ad un livello appropriato durante la distruzione.	gestione incidenti , Azure IAM con EDR , framework Vera ISO 27001
5.30	Prontezza ICT per la continuità aziendale	La prontezza ICT deve essere pianificata, implementata, mantenuta e testata in base agli obiettivi di continuità aziendale e ai requisiti di continuità ICT.	gestione incidenti , Azure IAM con EDR , framework Vera ISO 27001
5.31	Requisiti legali, statutari, regolamentari e contrattuali	I requisiti legali, statutari, regolamentari e contrattuali rilevanti per la sicurezza delle informazioni devono essere identificati, documentati e mantenuti aggiornati.	Monitoraggio del contesto
5.32	Diritti di proprietà intellettuale	L'organizzazione deve implementare procedure appropriate per proteggere i diritti di proprietà intellettuale.	Monitoraggio del contesto

5.33	Protezione dei documenti	I documenti devono essere protetti da perdita, distruzione, falsificazione, accesso non autorizzato e divulgazione non autorizzata.	Monitoraggio del contesto , Azure IAM con EDR , framework Vera ISO 27001
5.34	Privacy e protezione delle informazioni personali identificabili (PII)	L'organizzazione deve identificare e soddisfare i requisiti relativi alla tutela della privacy e alla protezione delle PII in conformità alle leggi, ai regolamenti applicabili e ai requisiti contrattuali.	Monitoraggio del contesto , Azure IAM con EDR , framework Vera ISO 27001
5.35	Revisione indipendente della sicurezza delle informazioni	L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e la sua implementazione, compresi persone, processi e tecnologie, devono essere periodicamente riesaminati in modo indipendente a intervalli pianificati o in caso di cambiamenti significativi.	Riesame di direzione
5.36	Conformità alle politiche, regole e standard per la sicurezza delle informazioni	La conformità alla politica di sicurezza delle informazioni dell'organizzazione, alle politiche specifiche per argomento, alle regole e agli standard deve essere regolarmente riesaminata.	Audit interni , Audit esterni
5.37	Procedure operative documentate	Le procedure operative per le strutture di elaborazione delle informazioni devono essere documentate e messe a disposizione del personale che ne ha bisogno.	Requisiti Progettazione Outsourcing Produzione Preservazione Controllo output non conformi

SOA - Statement of Applicability – ISO /IEC 27001:2022 - Annex A
DICHIARAZIONE DI APPLICABILITA' & PIANO DI SICUREZZA DELLE INFORMAZIONI

CONTROLLI SULLE PERSONE			
NUM	CONTROLLO	DESCRIZIONE	COLLOCAZIONE
6.1	Screening	Verifiche di verifica del background su tutti i candidati per diventare personale devono essere effettuate prima di entrare a far parte dell'organizzazione e in modo continuativo, prendendo in considerazione le leggi, i regolamenti, l'etica applicabile e proporzionalmente alle esigenze aziendali, alla classificazione delle informazioni da accedere e ai rischi percepiti.	Persone e competenze
6.2	Termini e condizioni di impiego	I contratti di lavoro devono specificare le responsabilità del personale e dell'organizzazione per la sicurezza delle informazioni.	Persone e competenze
6.3	Consapevolezza, formazione ed educazione sulla sicurezza delle informazioni	Il personale dell'organizzazione e le parti interessate pertinenti devono ricevere adeguate consapevolezza, formazione ed educazione sulla sicurezza delle informazioni e aggiornamenti regolari della politica di sicurezza delle informazioni dell'organizzazione, delle politiche specifiche per argomento e delle procedure, in relazione alle loro mansioni.	Persone e competenze
6.4	Processo disciplinare	Un processo disciplinare deve essere formalizzato e comunicato per intraprendere azioni contro il personale e altre parti interessate pertinenti che hanno commesso una violazione della politica di sicurezza delle informazioni.	Persone e competenze
6.5	Responsabilità dopo la cessazione o il cambio di impiego	Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o il cambio di impiego devono essere definiti, attuati e comunicati al personale e alle altre parti interessate pertinenti.	Persone e competenze
6.6	Accordi di riservatezza o non divulgazione	Gli accordi di riservatezza o non divulgazione che riflettono le esigenze dell'organizzazione per la protezione delle informazioni devono essere identificati, documentati, regolarmente riesaminati e firmati dal personale e dalle altre parti interessate pertinenti.	Persone e competenze
6.7	Lavoro remoto	Devono essere implementate misure di sicurezza quando il personale lavora in remoto per proteggere le informazioni a cui si accede, elabora o memorizza al di fuori dei locali dell'organizzazione.	Persone e competenze , Azure IAM con EDR , framework Vera ISO 27001
6.8	Segnalazione degli eventi relativi alla sicurezza delle informazioni	L'organizzazione deve fornire un meccanismo affinché il personale possa segnalare in modo tempestivo eventi di sicurezza delle informazioni osservati o sospettati attraverso canali appropriati.	gestione incidenti Azure IAM con EDR , framework Vera ISO 27001

SOA - Statement of Applicability – ISO /IEC 27001:2022 - Annex A
DICHIARAZIONE DI APPLICABILITA' & PIANO DI SICUREZZA DELLE INFORMAZIONI

CONTROLLI FISICI			
NUM	CONTROLLO	DESCRIZIONE	COLLOCAZIONE
7.1	Perimetri di sicurezza fisica	I perimetri di sicurezza devono essere definiti e utilizzati per proteggere aree che contengono informazioni e altri asset associati.	Sicurezza fisica
7.2	Accesso fisico	Le aree sicure devono essere protette da controlli di accesso appropriati e punti di accesso.	Sicurezza fisica
7.3	Sicurezza degli uffici, delle stanze e delle strutture	La sicurezza fisica degli uffici, delle stanze e delle strutture deve essere progettata e implementata.	Sicurezza fisica
7.4	Monitoraggio della sicurezza fisica	I locali devono essere monitorati continuamente per l'accesso fisico non autorizzato.	Sicurezza fisica
7.5	Protezione contro minacce fisiche e ambientali	La protezione contro minacce fisiche ed ambientali, come disastri naturali o altre minacce fisiche intenzionali o non intenzionali all'infrastruttura, deve essere progettata ed implementata.	Sicurezza fisica
7.6	Lavoro in aree sicure	Misure di sicurezza per lavorare in aree sicure devono essere progettate ed implementate.	Sicurezza fisica
7.7	Area di lavoro e schermo puliti	Norme per la pulizia della scrivania per documenti e supporti rimovibili e regole per lo schermo dei sistemi di elaborazione delle informazioni devono essere definite e applicate in modo appropriato.	Sicurezza fisica
7.8	Posizionamento e protezione dell'attrezzatura	L'attrezzatura deve essere posizionata in modo sicuro e protetta.	Sicurezza fisica
7.9	Sicurezza dei beni fuori sede	I beni fuori sede devono essere protetti.	Sicurezza fisica
7.10	Supporti di memorizzazione	I supporti di memorizzazione devono essere gestiti durante il loro ciclo di vita di acquisizione, utilizzo, trasporto e smaltimento in conformità con lo schema di classificazione e i requisiti di gestione dell'organizzazione.	Gestione degli asset Sicurezza fisica
7.11	Servizi di supporto	Le strutture di elaborazione delle informazioni devono essere protette da interruzioni di corrente e da altre interruzioni causate da malfunzionamenti nei servizi di supporto.	Sicurezza fisica

7.12	Sicurezza dei cavi	I cavi che trasportano alimentazione, dati o servizi di informazione di supporto devono essere protetti da intercettazioni, interferenze o danneggiamenti.	Sicurezza fisica
7.13	Manutenzione dell'attrezzatura	L'attrezzatura deve essere mantenuta correttamente per garantire la disponibilità, l'integrità e la riservatezza delle informazioni.	Gestione degli asset Sicurezza fisica
7.14	Smaltimento sicuro o riutilizzo dell'attrezzatura	Gli elementi di attrezzatura contenenti supporti di memorizzazione devono essere verificati per garantire che tutti i dati sensibili e i software con licenza siano stati rimossi o sovrascritti in modo sicuro prima dello smaltimento o riutilizzo.	Gestione degli asset Sicurezza fisica

SOA - Statement of Applicability – ISO /IEC 27001:2022 - Annex A
DICHIARAZIONE DI APPLICABILITA' & PIANO DI SICUREZZA DELLE INFORMAZIONI

CONTROLLI TECNOLOGICI			
NUM	CONTROLLO	DESCRIZIONE	COLLOCAZIONE
8.1	Dispositivi terminali dell'utente	Le informazioni memorizzate su, elaborate da o accessibili tramite dispositivi terminali dell'utente devono essere protette.	Controllo d'accesso Azure IAM con EDR , framework Vera ISO 27001
8.2	Diritti di accesso privilegiati	L'assegnazione e l'uso dei diritti di accesso privilegiati devono essere limitati e gestiti.	Controllo d'accesso , Azure IAM con EDR , framework Vera ISO 27001
8.3	Restrizione dell'accesso alle informazioni	L'accesso alle informazioni e ad altri asset associati deve essere limitato in conformità con la politica specifica per argomento sul controllo degli accessi.	Gestione degli asset Controllo d'accesso Azure IAM con EDR , framework Vera ISO 27001
8.4	Accesso al codice sorgente	L'accesso in lettura e scrittura al codice sorgente, agli strumenti di sviluppo e alle librerie software deve essere gestito in modo appropriato.	Controllo d'accesso , Azure IAM con EDR , framework Vera ISO 27001
8.5	Autenticazione sicura	Tecnologie e procedure di autenticazione sicura devono essere implementate in base alle restrizioni di accesso alle informazioni e alla politica specifica per argomento sul controllo degli accessi.	Controllo d'accesso , Azure IAM con EDR , framework Vera ISO 27001
8.6	Gestione delle capacità	L'uso delle risorse deve essere monitorato e adattato in linea con i requisiti di capacità attuali e previsti.	Gestione degli asset
8.7	Protezione contro malware	La protezione contro malware deve essere implementata e supportata da un'adeguata consapevolezza degli utenti.	Requisiti Progettazione Outsourcing Produzione Preservazione Controllo output non conformi
8.8	Gestione delle vulnerabilità tecniche	Deve essere ottenuta informazione sulle vulnerabilità tecniche dei sistemi informativi in uso, valutata l'esposizione dell'organizzazione a tali vulnerabilità e adottate misure appropriate.	Requisiti Progettazione Outsourcing Produzione Preservazione Controllo output non conformi Non conformità e azioni correttive
8.9	Gestione della configurazione	Le configurazioni, inclusa la configurazione della sicurezza, dell'hardware, del software, dei servizi e delle reti, devono essere stabilite, documentate, implementate, monitorate e revisionate.	Gestione degli asset , Azure IAM con EDR , framework Vera ISO 27001
8.10	Eliminazione delle informazioni	Le informazioni memorizzate nei sistemi informativi, nei dispositivi o in qualsiasi altro supporto di memorizzazione devono essere eliminate quando non sono più necessarie.	Gestione degli asset

8.11	Mascheramento dei dati	Il mascheramento dei dati deve essere utilizzato in conformità con la politica specifica per argomento sull'accesso e altre politiche specifiche correlate, e ai requisiti aziendali, considerando la legislazione applicabile.	Gestione degli asset Azure IAM con EDR , framework Vera ISO 27001
8.12	Prevenzione della fuga di dati	Misure di prevenzione della fuga di dati devono essere applicate a sistemi, reti e ad altri dispositivi che elaborano, memorizzano o trasmettono informazioni sensibili.	Gestione degli asset , Azure IAM con EDR , framework Vera ISO 27001
8.13	Backup delle informazioni	Copie di backup di informazioni, software e sistemi devono essere mantenute e regolarmente testate in conformità con la politica specifica per argomento sul backup concordata.	Requisiti Progettazione Outsourcing Produzione Preservazione Controllo output non conformi Azure IAM con EDR , f
8.14	Ridondanza delle strutture di elaborazione delle informazioni	Le strutture di elaborazione delle informazioni devono essere implementate con una ridondanza sufficiente per soddisfare i requisiti di disponibilità.	Gestione degli asset
8.15	Registrazione	I registri che registrano attività, eccezioni, guasti e altri eventi rilevanti devono essere prodotti, memorizzati, protetti ed analizzati.	Requisiti Progettazione Outsourcing Produzione Preservazione Controllo output non conformi
8.16	Monitoraggio delle attività	Reti, sistemi e applicazioni devono essere monitorati per comportamenti anomali e devono essere adottate azioni appropriate per valutare potenziali incidenti di sicurezza delle informazioni.	Preparazione e gestione incidenti , Azure IAM con EDR , framework Vera ISO 27001
8.17	Sincronizzazione dell'orologio	Gli orologi dei sistemi di elaborazione delle informazioni utilizzati dall'organizzazione devono essere sincronizzati con fonti temporali approvate.	Lavoro in rete , Azure IAM con EDR , framework Vera ISO 27001
8.18	Utilizzo di programmi utility privilegiati	L'uso di programmi utility che possono essere in grado di aggirare i controlli di sistema e delle applicazioni deve essere limitato e strettamente controllato.	Lavoro in rete , Azure IAM con EDR , framework Vera ISO 27001
8.19	Installazione di software sui sistemi operativi	Procedure e misure devono essere implementate per gestire in modo sicuro l'installazione di software sui sistemi operativi.	Lavoro in rete , Azure IAM con EDR , framework Vera ISO 27001
8.20	Sicurezza delle reti	Le reti e i dispositivi di rete devono essere protetti, gestiti e controllati per proteggere le informazioni nei sistemi.	Lavoro in rete , Azure IAM con EDR , framework Vera ISO 27001
8.21	Sicurezza dei servizi di rete Controllo	I meccanismi di sicurezza, i livelli di servizio e i requisiti di servizio dei servizi di rete devono essere identificati, implementati e monitorati.	Lavoro in rete , Azure IAM con EDR , framework Vera ISO 27001

8.22	Segregazione delle reti	Gruppi di servizi informativi, utenti e sistemi informativi devono essere segregati nelle reti dell'organizzazione.	Lavoro in rete , Azure IAM con EDR , framework Vera ISO 27001
8.23	Filtraggio web	L'accesso ai siti web esterni deve essere gestito per ridurre l'esposizione a contenuti dannosi.	Lavoro in rete , Azure IAM con EDR , framework Vera ISO 27001
8.24	Utilizzo della crittografia	Devono essere definite e implementate regole per l'efficace utilizzo della crittografia, inclusa la gestione delle chiavi crittografiche.	Lavoro in rete , Azure IAM con EDR , framework Vera ISO 27001
8.25	Ciclo di vita dello sviluppo sicuro	Devono essere stabiliti e applicati principi per lo sviluppo sicuro di software e sistemi.	Produzione . estrema all'ambito
8.26	Requisiti di sicurezza delle applicazioni	I requisiti di sicurezza delle informazioni devono essere identificati, specificati e approvati durante lo sviluppo o l'acquisizione di applicazioni.	Produzione , Azure IAM con EDR , framework Vera ISO 27001
8.27	Architettura di sistema sicuro e principi di ingegneria	Devono essere stabiliti, documentati, mantenuti e applicati principi per l'ingegneria di sistemi sicuri a tutte le attività di sviluppo di sistemi informativi.	Produzione estrema all'ambito
8.28	Codifica sicura	Principi di codifica sicura devono essere applicati allo sviluppo del software.	Produzione estrema all'ambito
8.29	Test di sicurezza nello sviluppo e nell'accettazione	I processi di test di sicurezza devono essere definiti e implementati nel ciclo di vita dello sviluppo.	Produzione estrema all'ambito
8.30	Sviluppo esterno	L'organizzazione deve dirigere, monitorare e rivedere le attività relative allo sviluppo esterno dei sistemi.	Produzione estrema all'ambito
8.31	Separazione degli ambienti di sviluppo, test e produzione	Gli ambienti di sviluppo, test e produzione devono essere separati e protetti.	Produzione estrema all'ambito
8.32	Gestione dei cambiamenti	I cambiamenti alle strutture di elaborazione delle informazioni e ai sistemi informativi devono essere soggetti a procedure di gestione dei cambiamenti.	Produzione estrema all'ambito

8.33	Informazioni di test	Le informazioni di test devono essere selezionate, protette e gestite in modo appropriato.	Produzione estrema all'ambito
8.34	Protezione dei sistemi informativi durante i test di audit	I test di audit e altre attività di garanzia che coinvolgono la valutazione dei sistemi operativi devono essere pianificati e concordati tra il tester e la gestione appropriata.	Produzione Azure IAM con EDR , framework Vera ISO 27001