

Kit Software Documentale Sistema di Gestione Sicurezza delle Informazioni, CyberSecurity e Protezione della Privacy ISO 27001:2024 | Aggiornato AMD-1 2024

Questo PDF contiene un esempio dei materiali Winple. Per verificare la versione, i contenuti completi, gli altri dimostrativi e la disponibilità, visita la scheda del prodotto.

APRI LA SCHEDA DEL PRODOTTO



www.wingle.it/kit-documentale-sicurezza-informazioni-iso-27001-2024/

**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 della dott.ssa Letizia Gramolini**, 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 27001:2024**.

DICHIARAZIONE DI APPLICABILITA'

Io sottoscritto in qualità di rappresentate della
in occasione della partecipazione alla GARA D'APPALTO
indetta da CAPITOLATO DEL.....

in data dichiaro di avere:

1. **Implementato il Sistema di Gestione** per la Sicurezza delle Informazioni ai sensi della ISO 27001:2024
2. **Conseguito la certificazione ISO 27001:2024**, rilasciata da.....il.....cod.....
3. **Attuato i controlli di sicurezza** dell'Annex A previsti dalla Norma nella sua edizione 2024.

In relazione alla circostanza indicata, per il rilascio di tale Dichiarazione di Applicabilità resa ai sensi della Norma ISO 27001:2024, 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 **dott. Massimo Belardi**, in qualità di **Responsabile del sistema di gestione** per la sicurezza delle informazioni, 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**.

FIRMA AD

.....

**PIANO DI SICUREZZA DELLE INFORMAZIONI**

L'organizzazione, all'interno del modulo **MOD-610 A Identificazione e valutazione del rischio**, ha:

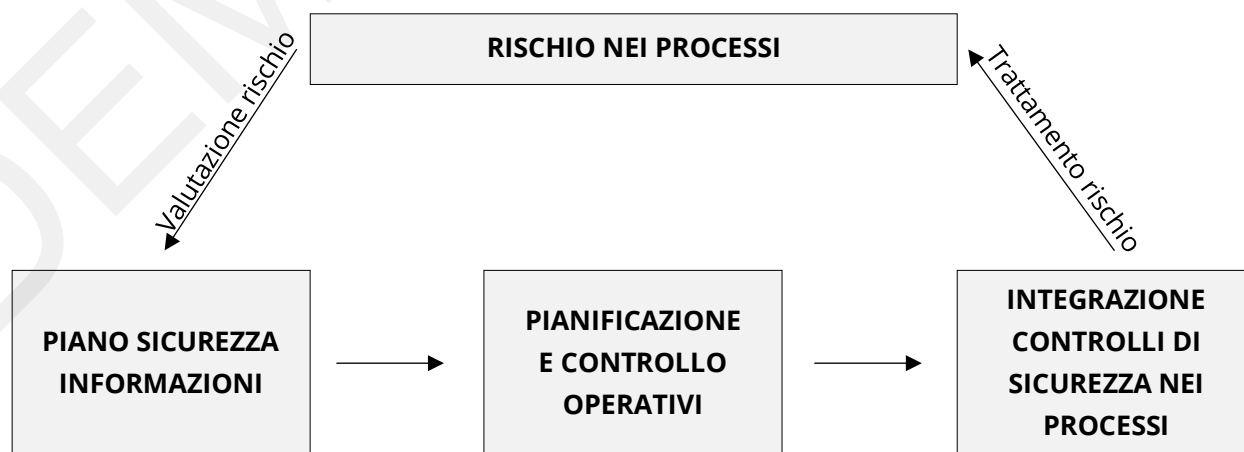
- Individuato e valutato i rischi per la sicurezza delle informazioni
- Classificato le informazioni da proteggere
- Collocato la presenza di tali informazioni all'interno di processi ben precisi
- Individuato le minacce che incombono sui singoli processi (sulle quali effettua attività di intelligence)

Il modulo indicato sopra, in sostanza, documenta l'attuazione delle azioni di pianificazione stabilite dalla procedura **PROC-610 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 **PROC-810 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.



**CONTROLLI ORGANIZZATIVI**

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.	PROC-710 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.	PROC-610 Gestione rischi ed opportunità
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.	PROC-610 Gestione rischi ed opportunità
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.	PROC-710 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.	PSI-01 Controllo d'accesso
5.16	Gestione delle identità	Il ciclo di vita completo delle identità deve essere gestito.	PSI-01 Controllo d'accesso
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.	PSI-01 Controllo d'accesso

**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.	PROC-720 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.	PROC-720 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.	PROC-720 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.	PROC-720 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.	PROC-720 Persone e competenze

**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.	PS-02 Sicurezza fisica
7.2	Accesso fisico	Le aree sicure devono essere protette da controlli di accesso appropriati e punti di accesso.	PS-02 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.	PS-02 Sicurezza fisica
7.4	Monitoraggio della sicurezza fisica	I locali devono essere monitorati continuamente per l'accesso fisico non autorizzato.	PS-02 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.	PS-02 Sicurezza fisica
7.6	Lavoro in aree sicure	Misure di sicurezza per lavorare in aree sicure devono essere progettate ed implementate.	PS-02 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.	PS-02 Sicurezza fisica
7.8	Posizionamento e protezione dell'attrezzatura	L'attrezzatura deve essere posizionata in modo sicuro e protetta.	PS-02 Sicurezza fisica
7.9	Sicurezza dei beni fuori sede	I beni fuori sede devono essere protetti.	PS-02 Sicurezza fisica



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.	PSI-01 Controllo d'accesso
8.2	Diritti di accesso privilegiati	L'assegnazione e l'uso dei diritti di accesso privilegiati devono essere limitati e gestiti.	PSI-01 Controllo d'accesso
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.	PROC-710 Gestione degli asset PSI-01 Controllo d'accesso
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.	PSI-01 Controllo d'accesso
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.	PSI-01 Controllo d'accesso
8.6	Gestione delle capacità	L'uso delle risorse deve essere monitorato e adattato in linea con i requisiti di capacità attuali e previsti.	PROC-710 Gestione degli asset
8.7	Protezione contro malware	La protezione contro malware deve essere implementata e supportata da un'adeguata consapevolezza degli utenti.	PROC-812 Requisiti PROC-813 Progettazione PROC-814 Outsourcing PROC-815 Produzione PROC-816 Preservazione PROC-817 Controllo output non conformi