b) L'organizzazione conserva i registri delle qualifiche e dell'esperienza del proprio personale coinvolto nelle attività di gestione della sicurezza delle informazioni.

1) I registri delle qualifiche e dell'esperienza del personale sono conservati per tutto il tempo in cui la persona lavora per l'impresa e per almeno tre anni dalla cessazione del rapporto di lavoro con la stessa.

2) Su richiesta, i membri del personale hanno accesso ai loro registri individuali. Su richiesta, l'impresa fornisce loro inoltre una copia dei rispettivi registri individuali al momento della cessazione del rapporto di lavoro con la stessa.

c) Il formato dei registri è specificato nelle procedure dell'impresa.

d) I registri sono conservati in modo da garantire la protezione da danni, alterazioni e furti, identificando le informazioni, se necessario, in base al loro livello di classificazione di sicurezza. L'impresa garantisce che i registri siano conservati utilizzando strumenti che garantiscano l'integrità, l'autenticità e l'accesso autorizzato.

IS.D.OR.250 Manuale di gestione della sicurezza delle informazioni (ISMM)

a) L'impresa mette a disposizione dell'autorità competente un manuale di gestione della sicurezza delle informazioni (ISMM) e, ove applicabile, manuali e procedure di riferimento associati e pertinenti, contenenti:

1) una dichiarazione firmata dal dirigente responsabile o, nel caso delle imprese di progettazione, dal capo dell'impresa di progettazione, che confermi che l'impresa opererà sempre conformemente al presente allegato e all'ISMM. Se il dirigente responsabile o, nel caso di imprese di progettazione, il capo dell'impresa di progettazione, non è l'amministratore delegato dell'impresa, tale amministratore delegato controfirma la dichiarazione;

2) il titolo (o i titoli), il nome (o i nomi), i compiti, le responsabilità e le autorità della persona o delle persone di cui al punto IS.D.OR.240, lettere b) e c);

3) il titolo, il nome, i compiti, le responsabilità e le autorità della persona responsabile comune di cui al punto IS.D.OR.240, lettera d), se del caso;

4) la politica in materia di sicurezza delle informazioni dell'impresa di cui al punto IS.D.OR.200, lettera a), punto 1);

5) una descrizione generale del numero e delle categorie del personale e del sistema in atto per pianificare la disponibilità del personale, come richiesto al punto IS.D.OR.240;

6) il titolo (o i titoli), il nome (o i nomi), i compiti, le responsabilità e le autorità delle persone di riferimento responsabili dell'attuazione del punto IS.D.OR.200, tra cui la persona o le persone responsabili della funzione di monitoraggio della conformità di cui al punto IS.D.OR.200, lettera a), punto 12);

7) un organigramma che mostri le catene associate di responsabilità per le persone di cui ai punti 2) e 6);

8) la descrizione del sistema di segnalazione interna di cui al punto IS.D.OR.215;

9) le procedure che specificano in che modo l'impresa garantisce la conformità alla presente parte, in particolare:

i) la documentazione di cui al punto IS.D.OR.200, lettera c);

ii) le procedure che definiscono il modo in cui l'impresa controlla le attività appaltate di cui al punto IS.D.OR.200, lettera a), punto 9);

iii) la procedura di modifica dell'ISMM di cui alla lettera c);

10) i dettagli dei metodi alternativi di rispondenza attualmente approvati.

b) Il rilascio iniziale dell'ISMM è approvato e l'autorità competente ne conserva una copia. L'ISMM è modificato in base alle necessità per riflettere sempre una descrizione aggiornata dell'ISMS dell'impresa. Una copia delle eventuali modifiche dell'ISMM è fornita all'autorità competente.

c) Le modifiche all'ISMM sono gestite secondo una procedura stabilita dall'impresa. Le modifiche non incluse nell'ambito di applicazione di tale procedura e quelle connesse alle modifiche di cui al punto IS.D.OR.255, lettera b), sono approvate dall'autorità competente.