

AZIENDA ULSS N. 8 BERICA

Viale F. Rodolfi n. 37 – 36100 VICENZA



**DELIBERAZIONE
DEL DIRETTORE GENERALE**

N. 1792 DEL 08/10/2026

O G G E T T O

RECEPIMENTO DIRETTIVA (UE) 2022/2555 (NIS 2) E D.LGS. N. 138/2024 – APPROVAZIONE
DEL DOCUMENTO DI INDIRIZZO STRATEGICO SULLA SICUREZZA INFORMATICA.

Proponente: UOC SISTEMI INFORMATIVI

Anno Proposta: 2026

Numero Proposta: 1973/26

Il Direttore dell' U.O.C. Sistemi Informativi riferisce che:

VISTA la Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 (Direttiva NIS 2);

VISTO il Decreto Legislativo 4 settembre 2024, n. 138 (nel seguito: Decreto), che recepisce nell'ordinamento nazionale la citata Direttiva;

RICHIAMATO l'art. 3 del Decreto, il quale definisce i soggetti che rientrano nell'ambito di applicazione dello stesso;

DATO ATTO che l'Azienda ULSS 8 Berica rientra nell'ambito di applicazione del Decreto ed è regolarmente registrata come tale sul portale dell'Agenzia per la Cybersicurezza Nazionale (ACN), come soggetto essenziale;

VISTA la DGR n. 1024 del 22/08/2023 che approva il progetto esecutivo del "Computer Emergency Response Team" (CERT) Regionale, ora CSIRT, in continuità con la DGR n. 1174 del 27/09/2022;

RICHIAMATA la Determinazione ACN n. 164179 del 14 aprile 2025, che ha approvato le Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del D.Lgs. n. 138/2024, individuando gli obblighi in capo agli organi di amministrazione e direttivi (individuati, per questa Azienda, nel Direttore Generale) e definendo le misure di sicurezza di base per i soggetti essenziali. Tale Determinazione ACN del 14 aprile 2025 prevede, all'Appendice C delle Linee Guida NIS – Specifiche di base, l'obbligo per gli organi direttivi di approvare specifici documenti fondamentali (tra cui: Politiche di sicurezza informatica, Piano di gestione del rischio, Piano di trattamento del rischio, Piano di continuità operativa, Piano di formazione, ecc.);

RICHIAMATA la Deliberazione del Direttore Generale n. 1712/2026, con la quale si dà definizione dei ruoli, responsabilità e poteri in materia di Cybersicurezza, ai sensi della direttiva "NIS2" e della Legge n. 90 del 28/06/2024, e si costituiscono il "Comitato Esecutivo Cybersicurezza" e il "Comitato di Gestione delle Crisi di Cybersicurezza – Unità di Crisi Cyber", aventi tra loro obiettivi operativi la predisposizione e/o aggiornamento dei documenti di cui al punto precedente;

PRESO ATTO che è stato predisposto a livello aziendale un Documento di indirizzo strategico sulla sicurezza informatica, allegato al presente Atto, che descrive sinteticamente i contenuti dei documenti sopra citati e la loro modalità di aggiornamento, al fine di renderne più efficientemente edotta la Direzione Generale e Strategica;

PRESO ATTO che il documento raccoglie, al livello minimo coerente con le funzioni tipiche di indirizzo e pianificazione proprie del vertice, i documenti e i piani la cui adozione e approvazione sono rimesse dalla normativa NIS agli organi di amministrazione e direttivi;

RITENUTO di demandare al "Comitato Esecutivo Cybersicurezza" aziendale il compito di curare il costante aggiornamento, la modifica e l'integrazione del *Documento di indirizzo strategico sulla sicurezza informatica* e delle relative politiche e procedure, nonché la predisposizione di eventuali nuove politiche e procedure che si rendessero in futuro necessarie, al fine di garantire il continuo allineamento della strategia aziendale all'evoluzione della normativa vigente e dei mutevoli scenari di rischio;

PRECISATO che il documento in oggetto si riferisce a procedure e politiche che sono depositate e conservate agli atti dell'U.O.C. Sistemi Informativi e accessibili esclusivamente ai soggetti autorizzati, agli organi di controllo e all'Agenzia per la Cybersicurezza Nazionale.

Il medesimo Dirigente ha attestato l'avvenuta regolare istruttoria della pratica anche in relazione alla sua compatibilità con la vigente legislazione regionale e statale in materia.

I Direttori Amministrativo, Sanitario e dei Servizi Socio-Sanitari hanno espresso il parere favorevole per quanto di rispettiva competenza.

IL DIRETTORE GENERALE

DELIBERA

Per tutto quanto in premessa, che qui si intende integralmente richiamato:

1. di approvare il *Documento di indirizzo strategico sulla sicurezza informatica* allegato, tramite l'adozione del presente atto, approvando, di conseguenza, tutti i documenti oggetto dell'obbligo di approvazione;
2. di incaricare il "Comitato Esecutivo Cybersicurezza" aziendale di curare la periodica revisione, l'aggiornamento e l'integrazione del *Documento di indirizzo strategico sulla sicurezza informatica* e delle relative politiche e procedure approvate col presente atto, oltre alla definizione e stesura di nuovi documenti strategici e operativi in ambito Cybersecurity che si renderanno necessari per il mantenimento della conformità normativa;
3. di trasmettere il presente provvedimento a tutti i soggetti coinvolti per gli adempimenti di rispettiva competenza;
4. di disporre che il presente atto venga pubblicato nell'Albo on-line dell'Azienda.

Parere favorevole, per quanto di competenza:

Il Direttore Amministrativo
(dott. Roberto Opizzi)

Il Direttore Sanitario
(dr. Alberto Rigo)

Il Direttore dei Servizi Socio-Sanitari
(dott. Leopoldo Ciato)

IL DIRETTORE GENERALE
(dott. Peter Assembergs)

Copia del presente atto viene inviato al Collegio Sindacale al momento della pubblicazione.

IL DIRETTORE
UOC AFFARI GENERALI E LEGALI

DOCUMENTO DI INDIRIZZO SULLA SICUREZZA INFORMATICA AI SENSI DEL DECRETO LEGISLATIVO N. 138/2024 (RECEPIMENTO DELLA NIS2)

Sommario

1 OBIETTIVO DEL DOCUMENTO	3
2 CONTESTO NORMATIVO E DI RIFERIMENTO	3
3 I DOCUMENTI DI INDIRIZZO STRATEGICO	4
3.1 Organizzazione per la sicurezza informatica	4
3.1.1 Finalità e indirizzo strategico	4
3.1.2 Attuazione e responsabilità operative	5
3.1.3 Documentazione di riferimento	5
3.2 Politiche di sicurezza informatica	6
3.2.1 Finalità e indirizzo strategico	6
3.2.2 Attuazione e responsabilità operative	7
3.2.3 Documenti di riferimento	7
3.3 Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete	8
3.3.1 Finalità e indirizzo strategico	8
3.3.2 Attuazione e responsabilità operative	9
3.3.3 Documenti di riferimento	9
3.4 Piano di trattamento del rischio	9
3.4.1 Finalità e indirizzo strategico	9
3.4.2 Attuazione e responsabilità operative	9
3.4.3 Documenti di riferimento	10
3.5 Piano di gestione delle vulnerabilità	10
3.5.1 Finalità e indirizzo strategico	10
3.5.2 Attuazione e responsabilità operative	11
3.5.3 Documenti di riferimento	11
3.6 Piano di adeguamento	11
3.6.1 Finalità e indirizzo strategico	11
3.6.2 Attuazione e responsabilità operative	12
3.6.3 Documenti di riferimento	12
3.7 Piano di continuità operativa	13
3.7.1 Finalità e indirizzo strategico	13
3.7.2 Attuazione e responsabilità operative	14
3.7.3 Documenti di riferimento	14
3.8 Piano di ripristino in caso di disastro	15
3.8.1 Finalità e indirizzo strategico	15
3.8.2 Attuazione e responsabilità operative	16
3.8.3 Documenti di riferimento	16
3.9 Piano di gestione delle crisi	17
3.9.1 Finalità e indirizzo strategico	17
3.9.2 Attuazione e responsabilità operative	18

3.9.3 Documenti di riferimento	18
3.10 Piano di formazione	19
3.10.1 Finalità e indirizzo strategico	19
3.10.2 Attuazione e responsabilità operative	20
3.10.3 Documenti di riferimento	20
3.11 Piano per la gestione degli incidenti di sicurezza informatica	21
3.11.1 Finalità e indirizzo strategico	21
3.11.2 Attuazione e responsabilità operative	22
3.11.3 Documenti di riferimento	22
4 DISPOSIZIONI FINALI	23
4.1 Approvazione e revisione	23
4.2 Rapporto con i presidi documentali e organizzativi	23
4.3 Delega delle attività operative	24

1 OBIETTIVO DEL DOCUMENTO

Il presente documento di indirizzo strategico unico (di seguito il «Documento di Indirizzo Strategico») è lo strumento attraverso cui gli organi di amministrazione e direttivi del soggetto NIS esercitano in modo consapevole la propria funzione di gestione complessiva, indirizzo e pianificazione strategica in materia di sicurezza informatica, come da Atto Aziendale.

Esso raccoglie, al livello minimo coerente con le funzioni tipiche di indirizzo e pianificazione proprie del vertice, i documenti e i piani la cui adozione e approvazione sono rimesse dalla normativa NIS agli organi di amministrazione e direttivi.

A tal fine, il documento sintetizza unicamente i riferimenti e i contenuti di natura strategico-organizzativa posti sotto la diretta approvazione della Direzione; sono viceversa demandati a separata e specifica approvazione tutti gli altri protocolli, procedure e specifiche di natura meramente tecnica.

2 CONTESTO NORMATIVO E DI RIFERIMENTO

Il quadro di riferimento è costituito dalla disciplina nazionale di recepimento della direttiva (UE) 2022/2555 (Direttiva NIS2), ossia il decreto legislativo 4 settembre 2024, n. 138 (in seguito denominato «decreto NIS»). A esso si aggiungono le determinazioni dell'Agenzia per la cybersicurezza nazionale (ACN), che definiscono le specifiche di base per l'adempimento agli obblighi stabiliti dalla normativa in materia di cybersicurezza.

Le misure di sicurezza sono strutturate secondo le Funzioni del Framework Nazionale per la Cybersecurity e la Data Protection (GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER) e i relativi codici di misura. Il presente documento richiama, per ciascun capitolo, la specifica misura e il punto che ne prevede l'approvazione da parte degli organi di amministrazione e direttivi.

3 I DOCUMENTI DI INDIRIZZO STRATEGICO

La presente sezione raccoglie i documenti e i piani sottoposti all'approvazione degli organi di amministrazione e direttivi. Per ciascuno sono indicati la misura di riferimento, la finalità e l'indirizzo strategico, i contenuti minimi individuati a livello di indirizzo strategico e la ripartizione tra indirizzo (di competenza del vertice) e attuazione operativa (demandata alle articolazioni competenti). Di seguito si riporta il prospetto della documentazione prodotta:

- 3.1.1 Organizzazione Sicurezza Informatica
- 3.2.1 Politica di gestione dei backup
- 3.2.2 Politica di Sicurezza delle reti e delle telecomunicazioni
- 3.2.3 Politica di gestione del rischio
- 3.2.4 Politica di affidabilità delle Risorse Umane, Formazione del Personale e Consapevolezza
- 3.2.5 Politica di conformità e audit di sicurezza
- 3.2.6 Politica di Gestione dei Rischi per la Sicurezza Informatica della Catena di Approvvigionamento
- 3.2.7 Politica di gestione degli asset
- 3.2.8 Politica di sicurezza delle informazioni
- 3.2.9 Politica dei ruoli e responsabilità
- 3.2.10 Politica di continuità operativa, ripristino in caso di disastro e gestione delle crisi
- 3.2.11 Politica di sicurezza fisica
- 3.2.12 Politica sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete
- 3.2.13 Politica monitoraggio degli eventi di sicurezza
- 3.2.14 Politica di gestione dei log
- 3.2.15 Politica di gestione delle utenze
- 3.2.16 Politica di cifratura e sicurezza dei dati
- 3.2.17 Politica di gestione sicura degli incidenti di sicurezza
- 3.2.18 Politica di gestione delle vulnerabilità
- 3.2.19 Politica di gestione dell'inventario degli asset
- 3.2.20 Politica di Classificazione delle Informazioni
- 3.3.1 Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete
- 3.4.1 Piano di trattamento del rischio
- 3.5.1 Piano di gestione delle vulnerabilità
- 3.6.1 Piano di adeguamento
- 3.7.1 Piano di continuità operativa
- 3.8.1 Piano di Disaster Recovery
- 3.8.2 Procedura di gestione dei backup
- 3.9.1 Piano di gestione della crisi cyber
- 3.9.2 Comitato di Gestione delle Crisi di Cybersicurezza - Unità di Crisi Cyber
- 3.9.3 Incident Response Plan
- 3.10.1 Piano di formazione sulla sicurezza informatica
- 3.11.1 Piano di gestione della crisi cyber
- 3.11.2 Comitato di Gestione delle Crisi di Cybersicurezza - Unità di Crisi Cyber
- 3.11.3 Incident Response Plan

3.1 ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA

Misura di riferimento	GV.RR-02 (punto 1)
Funzione (FNCDP)	GOVERN (GV) – GV.RR «Ruoli, responsabilità e autorità»

3.1.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione dell'organizzazione per la sicurezza informatica del soggetto NIS, definendone ruoli, responsabilità e autorità. Tale organizzazione deve essere comunicata a tutte le articolazioni aziendali. La sicurezza informatica è ricondotta a una responsabilità di vertice, non delegabile nella sua funzione di indirizzo.

L'organizzazione così definita costituisce il presidio attraverso cui l'Azienda governa il rischio informatico, integra la cybersecurity nelle pratiche di gestione delle risorse umane e presidia i rapporti con fornitori e terze parti.

Sintesi del contenuto del documento corrispettivo

L'Azienda ULSS8 riconosce la sicurezza informatica come una funzione organizzativa strutturata, formalmente definita e integrata nei processi di governo dell'Ente, attribuendo in modo chiaro ruoli, responsabilità, autorità e obblighi in materia di cybersicurezza. La gestione della sicurezza non è demandata all'iniziativa individuale, ma si fonda su un modello organizzativo formalizzato che assicura la corretta pianificazione, attuazione, supervisione e miglioramento continuo delle misure di protezione delle informazioni, dei sistemi informativi e dei servizi digitali.

A tal fine, l'Ente individua e assegna specifici ruoli di sicurezza al personale interno e, ove applicabile, al personale esterno autorizzato, definendone compiti, responsabilità, livelli decisionali e ambiti di competenza. Tali attribuzioni sono coerenti con i requisiti previsti dalla Direttiva NIS 2, dal D.Lgs. 138/2024 e dalle Misure di Sicurezza di Base dell'Agenzia per la Cybersicurezza Nazionale, garantendo la chiara identificazione dei soggetti responsabili delle attività di prevenzione, protezione, monitoraggio, risposta e ripristino.

La struttura organizzativa della sicurezza è definita in modo coordinato con gli altri processi di resilienza dell'Ente, assicurando l'allineamento con il Piano di Gestione degli Incidenti di Sicurezza, il Piano di Continuità Operativa, il Piano di Disaster Recovery e il Piano di Gestione delle Crisi. Tale integrazione consente di garantire una chiara catena decisionale e un efficace coordinamento tra le funzioni coinvolte nella gestione di eventi cyber, emergenze operative e situazioni di crisi.

L'organizzazione mantiene una mappatura completa, formalizzata e costantemente aggiornata dei ruoli di sicurezza, delle persone assegnate, delle relative responsabilità e delle deleghe eventualmente conferite. La documentazione organizzativa individua chiaramente i soggetti responsabili delle diverse attività di governance e gestione della sicurezza e viene comunicata alle funzioni interessate affinché ciascun soggetto sia consapevole dei propri obblighi, delle proprie responsabilità e delle modalità di interazione con gli altri attori coinvolti nel sistema di gestione della sicurezza.

In conformità alla normativa NIS, L'Azienda ULSS 8 designa formalmente il punto di contatto con l'Autorità nazionale competente e un relativo sostituto, nonché il referente CSIRT ed il suo sostituto, assicurando la disponibilità di referenti individuati per la gestione delle comunicazioni istituzionali, delle notifiche degli incidenti e degli adempimenti previsti dalla regolamentazione applicabile.

L'Ente definisce inoltre requisiti e criteri di affidabilità per il personale che svolge attività con impatto sulla sicurezza delle informazioni, compresi gli amministratori di sistema, i fornitori di servizi ICT, i consulenti e tutti i soggetti che, a qualsiasi titolo, accedono ai sistemi, ai dati o alle infrastrutture dell'organizzazione. Tali criteri sono applicati in modo proporzionato ai ruoli

ricoperti e ai privilegi assegnati, al fine di ridurre il rischio derivante da comportamenti impropri, errori umani o minacce interne.

La struttura dei ruoli e delle responsabilità è sottoposta a monitoraggio e aggiornamento continuo per garantirne la coerenza con l'evoluzione dell'organizzazione, dei processi aziendali, del contesto normativo e del panorama delle minacce cyber. Il modello organizzativo della sicurezza viene riesaminato in occasione di modifiche organizzative significative, introduzione di nuovi servizi o tecnologie, variazioni delle responsabilità assegnate, esiti di audit e verifiche, incidenti di sicurezza rilevanti o cambiamenti nel profilo di rischio dell'Ente. In ogni caso, il riesame formale dell'assetto organizzativo e delle responsabilità in materia di sicurezza è effettuato con periodicità almeno biennale, al fine di assicurarne l'efficacia, l'adequatezza e il continuo allineamento ai requisiti normativi e agli obiettivi di resilienza dell'organizzazione.

3.1.2 Attuazione e responsabilità operative

L'organizzazione relativa alla cybersicurezza è disciplinata e mantenuta aggiornata dalle articolazioni competenti del soggetto NIS mediante procedure e documenti interni, senza necessità di nuova approvazione da parte degli organi di amministrazione e direttivi.

3.1.3 Documentazione di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.1.1 Organizzazione Sicurezza Informatica

3.2 POLITICHE DI SICUREZZA INFORMATICA

Misura di riferimento	GV.PO-01 (punto 3)
Funzione (FNCDP)	GOVERN (GV) – GV.PO «Politica»

3.2.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione delle politiche di sicurezza informatica, stabilite in coerenza con il contesto organizzativo, la strategia di cybersecurity e le priorità del soggetto NIS. Le politiche, indicando principi, ruoli e responsabilità, rappresentano il quadro di indirizzo di rango primario da cui discendono tutti i successivi presidi documentali e organizzativi.

Le politiche sono riesaminate e, se opportuno, aggiornate periodicamente e comunque almeno con cadenza annuale, nonché a fronte di evoluzioni normative, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione al rischio (GV.PO-02).

Sintesi del contenuto del documento corrispettivo

L'Azienda ULSS8 ha definito e mantiene un sistema organico di politiche di sicurezza che costituisce il riferimento formale e permanente per la gestione della sicurezza delle informazioni, dei sistemi informativi e dei servizi digitali dell'Ente. Le politiche sono sviluppate in coerenza con il contesto organizzativo, gli obiettivi strategici, il profilo di rischio e i requisiti normativi applicabili, recependo integralmente le Misure Minime di Sicurezza ICT e le Misure di Sicurezza di Base dell'Agenzia per la Cybersicurezza Nazionale, con particolare riferimento alla misura GV.PO-01.

Il corpus documentale copre in modo completo tutti gli ambiti di governo, protezione, rilevazione, risposta e ripristino richiesti dal quadro normativo e regolamentare di riferimento, garantendo l'assenza di aree non presidiate. In particolare, le politiche disciplinano la gestione del rischio cyber, la definizione di ruoli e responsabilità, la sicurezza delle risorse umane, la gestione della

catena di fornitura, la gestione degli asset, la gestione delle vulnerabilità, la continuità operativa e il disaster recovery, il controllo degli accessi, la sicurezza fisica e ambientale, la formazione e la consapevolezza del personale, la protezione dei dati e dei sistemi, la sicurezza delle reti e delle telecomunicazioni, il monitoraggio degli eventi di sicurezza, la gestione dei log, il rilevamento delle minacce e la gestione degli incidenti di sicurezza.

Le politiche rappresentano il livello normativo interno di riferimento dal quale discendono procedure operative, standard tecnici, istruzioni di lavoro e linee guida, assicurando la piena tracciabilità tra requisiti legislativi e regolamentari, misure di sicurezza adottate e documentazione di attuazione. Ciascuna politica è redatta secondo una struttura documentale uniforme che comprende almeno finalità, ambito di applicazione, principi, requisiti, ruoli e responsabilità, attività di controllo, modalità di monitoraggio, riferimenti normativi e criteri di revisione e aggiornamento.

Le disposizioni contenute nelle politiche si applicano al personale dipendente, ai collaboratori, ai fornitori e a qualsiasi soggetto che, a qualsiasi titolo, acceda, utilizzi o gestisca informazioni, sistemi, reti o servizi di competenza dell'Azienda ULSS8.

Al fine di garantirne l'efficacia e la costante aderenza all'evoluzione del contesto interno ed esterno, le politiche sono sottoposte a riesame almeno annuale e, in ogni caso, in occasione di modifiche normative, cambiamenti organizzativi, evoluzione del panorama delle minacce, introduzione di nuove tecnologie, eventi di sicurezza significativi o esiti di attività di audit e riesame. Tutte le revisioni sono formalmente approvate, registrate e tracciate mediante apposito storico delle modifiche, assicurando la disponibilità delle versioni vigenti e la corretta conservazione di quelle obsolete.

L'adozione, l'approvazione e il mantenimento delle politiche di sicurezza costituiscono una responsabilità degli organi di amministrazione e direttivi, che ne assicurano l'allineamento agli obiettivi istituzionali e alle esigenze di protezione delle informazioni, promuovendone la diffusione, la conoscenza e l'applicazione all'interno dell'organizzazione.

3.2.2 Attuazione e responsabilità operative

Il contenuto tecnico e operativo di ciascun ambito di politica (regole di dettaglio, standard, baseline di configurazione, istruzioni) è definito e aggiornato dalle articolazioni competenti tramite procedure, istruzioni operative e manuali interni, nel rispetto degli indirizzi qui approvati.

3.2.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.2.1 Politica di gestione dei backup
- 3.2.2 Politica di Sicurezza delle reti e delle telecomunicazioni
- 3.2.3 Politica di gestione del rischio
- 3.2.4 Politica di affidabilità delle Risorse Umane, Formazione del Personale e Consapevolezza
- 3.2.5 Politica di conformità e audit di sicurezza
- 3.2.6 Politica di Gestione dei Rischi per la Sicurezza Informatica della Catena di Approvvigionamento
- 3.2.7 Politica di gestione degli asset
- 3.2.8 Politica di sicurezza delle informazioni
- 3.2.9 Politica dei ruoli e responsabilità
- 3.2.10 Politica di continuità operativa, ripristino in caso di disastro e gestione delle crisi
- 3.2.11 Politica di sicurezza fisica
- 3.2.12 Politica sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete
- 3.2.13 Politica monitoraggio degli eventi di sicurezza
- 3.2.14 Politica di gestione dei log
- 3.2.15 Politica di gestione delle utenze

- 3.2.16 Politica di cifratura e sicurezza dei dati
- 3.2.17 Politica di gestione sicura degli incidenti di sicurezza
- 3.2.18 Politica di gestione delle vulnerabilità
- 3.2.19 Politica di gestione dell'inventario degli asset
- 3.2.20 Politica di Classificazione delle Informazioni

3.3 VALUTAZIONE DEL RISCHIO POSTO ALLA SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE

Misura di riferimento	ID.RA-05 (punto 3)
Funzione (FNCDP)	IDENTIFY (ID) – ID.RA «Valutazione del rischio»

3.3.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione della valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete, eseguita in coerenza con il piano di gestione dei rischi per la sicurezza informatica (GV.RM-03) e ricompresa nei processi complessivi di gestione del rischio dell'Azienda.

La valutazione è eseguita a intervalli pianificati e comunque almeno ogni due anni, nonché a fronte di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi (ID.RA-05, punto 2).

Sintesi del contenuto del documento corrispettivo

Le decisioni in materia di sicurezza si basano su una conoscenza oggettiva, documentata e costantemente aggiornata dei rischi cui sono esposti i sistemi informativi e di rete dell'organizzazione. La valutazione del rischio è condotta secondo un processo strutturato e metodologicamente definito, fondato su criteri chiari, coerenti e verificabili, al fine di garantire decisioni supportate da evidenze e non da valutazioni soggettive.

Il processo di valutazione consente di identificare, analizzare e valutare sistematicamente le minacce interne ed esterne, le vulnerabilità presenti o non ancora risolte e le potenziali conseguenze derivanti dal verificarsi di incidenti di sicurezza. L'analisi considera in particolare gli impatti che tali eventi potrebbero generare sulla riservatezza, sull'integrità e sulla disponibilità delle informazioni, dei servizi e delle infrastrutture a supporto delle attività istituzionali e operative.

Ogni rischio individuato è classificato sulla base di livelli di probabilità e impatto definiti attraverso apposite scale di valutazione, al fine di determinarne la rilevanza e stabilire le priorità di intervento. A ciascun rischio è associato un responsabile incaricato del relativo monitoraggio e della gestione delle azioni di trattamento, garantendo una chiara attribuzione delle responsabilità. Tale approccio consente di distinguere i rischi accettabili da quelli che richiedono l'adozione di misure di trattamento finalizzate a riportarne il livello entro le soglie di accettabilità definite dall'organizzazione, mediante azioni di mitigazione, trasferimento, eliminazione della sorgente del rischio o altre modalità di gestione del rischio.

La valutazione del rischio è riesaminata periodicamente e mantenuta costantemente aggiornata per riflettere l'evoluzione del contesto organizzativo, tecnologico, normativo e delle minacce. In ogni caso, il processo è svolto con cadenza almeno biennale e ogniqualvolta si verifichino incidenti significativi, modifiche sostanziali ai sistemi informativi, ai servizi erogati o al profilo di esposizione al rischio, al fine di garantire l'efficacia e l'adequatezza delle misure di sicurezza adottate nel tempo.

3.3.2 Attuazione e responsabilità operative

La metodologia di dettaglio è definita e mantenuta dalle articolazioni competenti attraverso procedure e strumenti operativi, in coerenza con l'indirizzo approvato.

3.3.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.3.1 Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete

3.4 PIANO DI TRATTAMENTO DEL RISCHIO

Misura di riferimento	ID.RA-06 (punto 3)
Funzione (FNCDP)	IDENTIFY (ID) – ID.RA «Valutazione del rischio»

3.4.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione del piano di trattamento del rischio, ivi compresa l'accettazione degli eventuali rischi residui. L'accettazione del rischio residuo è una prerogativa di indirizzo strategico che resta in capo al vertice e non è delegabile.

Sintesi del contenuto del piano

Il Piano di Trattamento del Rischio documenta le opzioni selezionate, le misure da implementare, le relative priorità, i responsabili dell'attuazione e le tempistiche previste per il completamento delle azioni, garantendo un monitoraggio efficace dello stato di avanzamento.

Qualora specifici requisiti tecnici o misure di sicurezza non possano essere attuati per motivate ragioni di natura organizzativa, tecnica o economica, tale circostanza è adeguatamente documentata come eccezione e, ove necessario, sono individuate e implementate misure compensative idonee a mantenere il rischio entro livelli accettabili.

Particolare attenzione è riservata al rischio residuo, inteso come il livello di rischio che permane dopo l'attuazione delle misure di trattamento previste. Ogni decisione di accettazione del rischio residuo deve essere formalmente motivata, documentata e sottoposta all'approvazione della funzione o dell'organo competente, in conformità al modello di governance e alle soglie di accettabilità definite dall'organizzazione. Tale accettazione deve essere riesaminata periodicamente o in occasione di cambiamenti significativi del contesto di rischio.

3.4.2 Attuazione e responsabilità operative

Il tracciamento operativo delle misure di trattamento (piani di azione, assegnatari, milestone, stato di avanzamento) è gestito dalle articolazioni competenti mediante strumenti e registri interni, con reportistica periodica al vertice.

3.4.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.4.1 Piano di trattamento del rischio

3.5 PIANO DI GESTIONE DELLE VULNERABILITÀ

Misura di riferimento	ID.RA-08 (punto 4)
Funzione (FNCDP)	IDENTIFY (ID) – ID.RA «Valutazione del rischio»

3.5.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione del piano di gestione delle vulnerabilità, quale presidio strutturato per l'identificazione, il monitoraggio, l'analisi e la risposta alle vulnerabilità dei sistemi informativi e di rete.

Sintesi del contenuto del piano

L'Azienda ULSS8 adotta un processo strutturato e continuativo di gestione delle vulnerabilità finalizzato a identificare tempestivamente le debolezze che possono interessare i sistemi informativi e di rete e ad assicurarne la valutazione e il trattamento prima che possano essere sfruttate da soggetti malevoli. La gestione delle vulnerabilità costituisce parte integrante del sistema di gestione del rischio cyber e concorre al mantenimento di un adeguato livello di sicurezza delle informazioni e dei servizi erogati.

Il processo disciplina la raccolta, l'analisi e la valutazione delle informazioni relative alle vulnerabilità note, la verifica della loro applicabilità al contesto organizzativo e tecnologico dell'Azienda e la loro classificazione e prioritizzazione sulla base di criteri di rischio che tengano conto della criticità degli asset coinvolti, della probabilità di sfruttamento e dei potenziali impatti operativi, economici, normativi e reputazionali.

Le attività di identificazione e valutazione delle vulnerabilità sono supportate da iniziative periodiche di Vulnerability Assessment e Penetration Test, nonché dal monitoraggio continuo delle fonti informative ritenute autorevoli e rilevanti, tra cui il CSIRT Italia, il CERT regionale, i fornitori di tecnologie e software critici e altre fonti specializzate di threat intelligence e sicurezza informatica.

Per ciascuna vulnerabilità individuata sono definite le relative azioni di trattamento, le priorità di intervento, i responsabili dell'attuazione e le tempistiche previste per la risoluzione. Eventuali eccezioni o deroghe sono formalmente motivate, autorizzate dalle articolazioni competenti nel soggetto NIS e adeguatamente documentate. Tutte le vulnerabilità, le misure correttive e le eventuali eccezioni sono tracciate e monitorate fino alla loro chiusura, mantenendo il collegamento con gli asset, i servizi essenziali e i rischi correlati.

Tale approccio consente di ridurre il tempo di esposizione alle vulnerabilità critiche, di assicurare che ogni segnalazione rilevante sia presa in carico e gestita in modo tempestivo e di garantire una costante riduzione del rischio residuo associato ai sistemi informativi e di rete dell'organizzazione.

3.5.2 Attuazione e responsabilità operative

L'esecuzione tecnica (scansioni, test, gestione delle patch, ticketing e remediation) è disciplinata dalle articolazioni competenti mediante procedure tecniche e istruzioni operative, in coerenza con il piano di trattamento del rischio ([ID.RA-06](#)).

3.5.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.5.1 Piano di gestione delle vulnerabilità

3.6 PIANO DI ADEGUAMENTO

Misura di riferimento	ID.IM-01 (punto 1)
Funzione (FNCDP)	IDENTIFY (ID) – ID.IM «Miglioramento»

3.6.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione del piano di adeguamento, che individua gli interventi necessari ad assicurare l'attuazione delle politiche di sicurezza, in esito al riesame di cui alla misura GV.PO-02.

Il vertice è informato mediante apposite relazioni periodiche sugli esiti del piano di adeguamento e sul piano per la valutazione dell'efficacia delle misure di gestione del rischio (ID.IM-01).

Sintesi del contenuto del piano

La conformità alle politiche e alle misure di sicurezza è oggetto di monitoraggio e verifica continua, nell'ambito di un processo strutturato di miglioramento continuo volto a garantire l'efficacia del sistema di gestione della sicurezza delle informazioni e della cybersicurezza. Gli esiti delle attività di riesame, controllo e valutazione sono utilizzati per identificare eventuali carenze, scostamenti o opportunità di miglioramento e per definire le azioni necessarie al loro trattamento.

A tal fine, è predisposto un Piano di Adeguamento che individua in modo chiaro e documentato gli interventi correttivi e migliorativi da realizzare, le priorità di attuazione, le responsabilità assegnate e le relative tempistiche. Il piano costituisce lo strumento attraverso il quale l'organizzazione assicura la progressiva risoluzione delle non conformità rilevate e la piena attuazione delle politiche, delle procedure e delle misure di sicurezza adottate.

Lo stato di avanzamento delle attività previste dal Piano di Adeguamento è monitorato periodicamente e i relativi risultati sono riportati attraverso appositi flussi informativi destinati alla Direzione e agli organi competenti. Tali relazioni forniscono evidenza del livello di conformità raggiunto, delle azioni completate, delle eventuali criticità riscontrate e delle attività ancora in corso, consentendo al vertice aziendale di esercitare una supervisione effettiva e informata sull'attuazione delle misure di sicurezza e sul processo di miglioramento continuo.

Il monitoraggio continuo dell'avanzamento degli interventi e la regolare rendicontazione ai livelli decisionali garantiscono che il processo di adeguamento non si traduca in un mero adempimento formale, ma contribuisca concretamente al rafforzamento della resilienza e della sicurezza dei sistemi informativi e di rete dell'organizzazione.

3.6.2 Attuazione e responsabilità operative

Le schede di dettaglio degli interventi, la definizione di responsabili e tempistiche, il monitoraggio dell'avanzamento e la relativa reportistica sono definiti e aggiornati dalle articolazioni competenti mediante procedure e istruzioni operative, senza necessità di nuova approvazione del piano.

3.6.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.6.1 Piano di adeguamento

3.7 PIANO DI CONTINUITÀ OPERATIVA

Misura di riferimento	ID.IM-04 (punto 4)
-----------------------	--------------------

3.7.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione del piano di continuità operativa, definito per almeno i sistemi informativi e di rete rilevanti, quale presidio per assicurare la continuità dei servizi essenziali del soggetto NIS. Il piano è riesaminato e, se opportuno, aggiornato a fronte di incidenti significativi o mutamenti dell'esposizione al rischio (ID.IM-04, punto 5).

Sintesi del contenuto del piano

La continuità operativa dei servizi essenziali rappresenta un obiettivo prioritario per l'Azienda ULSS8 e costituisce un elemento fondamentale per garantire l'erogazione delle prestazioni sanitarie e il perseguimento delle finalità istituzionali anche in presenza di eventi avversi. L'organizzazione adotta pertanto misure e processi volti ad assicurare la capacità di mantenere, ripristinare o riprendere tempestivamente i servizi critici e le relative risorse informative e tecnologiche in caso di interruzioni, malfunzionamenti o situazioni di emergenza.

A tal fine, l'Azienda ULSS8 definisce e mantiene un Piano di Continuità Operativa che disciplina le modalità di gestione degli eventi in grado di compromettere, totalmente o parzialmente, la disponibilità dei sistemi informativi e di rete rilevanti, garantendo una risposta coordinata ed efficace e, ove necessario, la prosecuzione dei processi critici mediante modalità operative alternative o degradate.

Il Piano di Continuità Operativa individua con chiarezza le finalità e l'ambito di applicazione, i processi e i servizi essenziali da salvaguardare, le dipendenze tecnologiche e organizzative, i ruoli e le responsabilità delle funzioni coinvolte, nonché i flussi informativi, i canali di comunicazione e le procedure di escalation da attivare nelle diverse situazioni di emergenza. Il piano definisce inoltre le condizioni per l'attivazione e la chiusura dello stato di emergenza, le modalità di coordinamento delle attività di risposta e ripristino e le risorse necessarie per garantire la continuità delle operazioni.

Tra tali risorse rientrano le soluzioni di backup e ripristino dei dati, i meccanismi di ridondanza delle componenti critiche, le infrastrutture e i siti alternativi di elaborazione, nonché eventuali misure compensative predisposte per ridurre l'impatto di indisponibilità prolungate o di specifiche limitazioni operative. Le strategie di continuità e ripristino sono definite in funzione della criticità dei servizi e dei relativi requisiti di disponibilità, tenendo conto degli obiettivi di recupero stabiliti dall'organizzazione.

L'ambito del Piano di Continuità Operativa comprende sia gli scenari di indisponibilità programmata sia quelli derivanti da eventi non pianificati, inclusi guasti tecnologici, interruzioni dei servizi essenziali, incidenti di sicurezza informatica, indisponibilità delle infrastrutture, errori operativi ed eventi di natura fisica o ambientale. Ove rilevante, il piano coinvolge anche fornitori esterni, partner tecnologici e soggetti terzi dai quali dipendono i servizi erogati, definendo le relative modalità di coordinamento e comunicazione.

Il piano si applica all'infrastruttura che abilita gli applicativi aziendali utilizzati dall'organizzazione ed è sottoposto a riesame, aggiornamento e verifica periodica mediante attività di test ed esercitazione, al fine di garantirne l'efficacia e l'adeguatezza rispetto all'evoluzione del contesto organizzativo, tecnologico e delle minacce.

3.7.2 Attuazione e responsabilità operative

Le procedure operative di continuità comprendono i runbook, le soluzioni di ridondanza e la gestione dei backup, ivi incluse le copie offline per i sistemi rilevanti (cfr. PR.DS-11). Tali procedure sono definite e mantenute dalle articolazioni competenti mediante documentazione tecnica dedicata.

3.7.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.7.1 Piano di continuità operativa

3.8 PIANO DI RIPRISTINO IN CASO DI DISASTRO

Misura di riferimento	ID.IM-04 (punto 4)
Funzione (FNCDP)	IDENTIFY (ID) – ID.IM «Miglioramento»

3.8.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione del piano di ripristino in caso di disastro (disaster recovery), definito per almeno i sistemi informativi e di rete rilevanti, per garantire il recupero delle capacità operative a seguito di eventi gravemente lesivi.

Sintesi del contenuto del piano

L'Azienda ULSS8 adotta un approccio strutturato alla gestione del ripristino dei sistemi informativi e di rete, al fine di garantire il recupero tempestivo delle capacità operative in seguito a eventi che ne compromettano significativamente la disponibilità o l'integrità. L'organizzazione deve essere in grado di ripristinare i servizi e le funzioni critiche secondo modalità e tempi predefiniti, limitando gli impatti operativi, assistenziali, economici e reputazionali derivanti da incidenti, guasti o situazioni di emergenza.

A tal fine, è definito e mantenuto un Piano di Disaster Recovery che si applica almeno ai sistemi informativi e di rete rilevanti e che è sviluppato in coerenza con standard e buone pratiche riconosciute a livello internazionale, quali il NIST SP 800-34, la ISO 22301:2019 e altri riferimenti applicabili. Il piano individua e disciplina i diversi scenari di ripristino, prevedendo procedure differenziate per situazioni di perdita parziale dei servizi, indisponibilità di specifiche componenti infrastrutturali o applicative, nonché per eventi che comportino l'inagibilità totale o prolungata dei siti primari.

Il Piano di Disaster Recovery definisce le strategie di recupero e l'ordine di priorità con cui devono essere ripristinati i processi, i servizi essenziali e le relative risorse tecnologiche, individuando le procedure operative da adottare, le modalità di utilizzo di infrastrutture o siti alternativi e le eventuali dipendenze da fornitori e soggetti terzi coinvolti nelle attività di ripristino.

Per ciascun sistema, servizio o processo critico sono stabiliti specifici obiettivi di recupero, espressi attraverso il Recovery Time Objective (RTO) e il Recovery Point Objective (RPO), in funzione della criticità degli asset e delle esigenze di continuità operativa dell'organizzazione. Il piano definisce inoltre i ruoli e le responsabilità delle funzioni coinvolte, i flussi di comunicazione interni ed esterni, le procedure di escalation e le risorse umane, tecnologiche e logistiche necessarie per l'esecuzione delle attività di ripristino.

Il Piano di Disaster Recovery individua i soggetti autorizzati a dichiarare lo stato di disastro e a richiedere l'attivazione delle procedure di ripristino, definendo in modo chiaro la ripartizione delle responsabilità tra le strutture interne, i fornitori di servizi ICT, i partner tecnologici e gli altri soggetti coinvolti. Le modalità di coordinamento tra le diverse parti interessate sono formalizzate al fine di garantire una gestione efficace e tempestiva delle attività di recupero.

La capacità di ripristino dell'organizzazione non è considerata presunta, ma deve essere periodicamente verificata attraverso attività di test, simulazione ed esercitazione, finalizzate a comprovare l'efficacia delle strategie adottate, la raggiungibilità degli obiettivi di recupero definiti e l'adeguatezza delle risorse disponibili. Gli esiti delle verifiche sono documentati, analizzati e

utilizzati per aggiornare e migliorare continuamente il Piano di Disaster Recovery, assicurandone la costante efficacia e coerenza rispetto all'evoluzione del contesto operativo, tecnologico e delle minacce.

3.8.2 Attuazione e responsabilità operative

Le procedure tecniche di ripristino, i test di recovery e la verifica dell'utilizzabilità dei backup (PR.DS-11) sono definiti ed eseguiti dalle articolazioni competenti mediante istruzioni operative e relazioni di test.

3.8.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.8.1 Piano di Disaster Recovery
- 3.8.2 Procedura di gestione dei backup

3.9 PIANO DI GESTIONE DELLE CRISI

Misura di riferimento	ID.IM-04 (punto 4)
Funzione (FNCDP)	IDENTIFY (ID) – ID.IM «Miglioramento»

3.9.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione del piano per la gestione delle crisi, quale presidio di governo delle situazioni critiche che coinvolge, ove necessario, anche i fornitori e definisce le modalità di raccordo con le autorità competenti.

Sintesi del contenuto del piano

L'Azienda ULSS8 adotta un approccio strutturato alla gestione delle emergenze e delle crisi, al fine di garantire una risposta tempestiva, coordinata ed efficace agli eventi che possono compromettere la disponibilità dei servizi essenziali, la sicurezza delle informazioni, l'operatività delle strutture o il perseguimento delle proprie finalità istituzionali. La gestione delle situazioni emergenziali e di crisi è disciplinata attraverso processi formalizzati che consentono di assumere decisioni rapide e informate, riducendo gli impatti sull'organizzazione e sugli stakeholder coinvolti.

Il modello di gestione distingue chiaramente tra emergenza e crisi. L'emergenza è rappresentata da un evento che richiede una risposta immediata da parte delle strutture competenti, mentre la crisi costituisce una situazione caratterizzata da un impatto elevato, effettivo o potenziale, tale da richiedere il coinvolgimento del vertice aziendale, il coordinamento di più funzioni e l'adozione di decisioni straordinarie. La gestione della crisi rappresenta pertanto l'evoluzione organizzativa dell'emergenza qualora la gravità, l'estensione o la durata dell'evento eccedano le normali capacità di risposta operativa.

Il Piano di Gestione delle Crisi disciplina la gestione di eventi originati sia da fattori interni sia da fattori esterni, inclusi attacchi informatici, interruzioni prolungate dei servizi critici, indisponibilità dei sistemi informativi e di rete, eventi di natura fisica o ambientale, indisponibilità di fornitori strategici e altre situazioni in grado di compromettere la continuità delle attività aziendali. Il piano definisce le modalità di rilevazione, classificazione, escalation e gestione degli eventi, stabilendo in anticipo le azioni da intraprendere, i soggetti coinvolti e le responsabilità attribuite a ciascuna funzione.

Il piano disciplina, inoltre, i flussi di comunicazione e coordinamento necessari durante la gestione dell'evento, definendo le modalità di comunicazione interna tra le strutture coinvolte e le procedure di comunicazione esterna verso le autorità competenti, gli organismi istituzionali, gli

utenti, i fornitori, i partner tecnologici e gli altri stakeholder interessati. Ove necessario, sono previste specifiche modalità di coinvolgimento e coordinamento dei fornitori e delle terze parti che contribuiscono all'erogazione dei servizi essenziali o alla gestione delle attività di risposta e ripristino.

L'assetto organizzativo per la gestione delle emergenze e delle crisi prevede livelli di governance differenziati in funzione della gravità dell'evento. Per le crisi di maggiore rilevanza è istituito un organo direttivo di alto livello, responsabile dell'indirizzo strategico, dell'assunzione delle decisioni straordinarie e del coordinamento complessivo delle attività. Per gli eventi di minore gravità è invece prevista una struttura operativa incaricata di gestire le attività di risposta, contenimento e recupero nell'ambito delle responsabilità ordinarie.

Ruoli, responsabilità, criteri di attivazione, livelli di escalation e modalità di coordinamento tra le diverse strutture organizzative sono definiti preventivamente e formalizzati nei relativi piani e procedure operative. Tale assetto consente di garantire una risposta organizzata, tempestiva e coerente con la gravità dell'evento, evitando ritardi decisionali e incertezze operative nelle fasi più critiche.

La gestione delle emergenze e delle crisi opera in stretto coordinamento con i processi di continuità operativa, disaster recovery, gestione degli incidenti e sicurezza delle informazioni, assicurando un approccio integrato alla resilienza organizzativa. L'efficacia dell'assetto organizzativo e delle procedure di risposta è verificata periodicamente mediante attività di test, esercitazioni e simulazioni, i cui risultati sono utilizzati per il miglioramento continuo delle capacità di gestione delle crisi e della resilienza complessiva dell'organizzazione.

3.9.2 Attuazione e responsabilità operative

L'attivazione operativa del comitato di crisi, gli scenari, gli alberi di escalation e le check-list sono disciplinati dalle articolazioni competenti mediante procedure interne dedicate.

3.9.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.9.1 Piano di gestione della crisi cyber
- 3.9.2 Comitato di Gestione di Gestione della Crisi Cyber
- 3.9.3 Incident Response Plan

3.10 PIANO DI FORMAZIONE

Misura di riferimento	PR.AT-01 (punto 2)
Funzione (FNCDP)	PROTECT (PR) – PR.AT «Sensibilizzazione e formazione»

3.10.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione del piano di formazione in materia di sicurezza informatica per lo sviluppo delle competenze di tutto il personale dipendente. Alcune specifiche attività formative sono indirizzate alla Direzione Strategica.

Sintesi del contenuto del piano

La sicurezza e la resilienza dell'organizzazione dipendono in misura determinante dalla consapevolezza, dalle competenze e dai comportamenti delle persone. L'Azienda ULSS8 promuove pertanto un programma strutturato e continuativo di formazione e sensibilizzazione in materia di cybersicurezza, volto a garantire che tutto il personale, nonché gli organi di amministrazione,

direzione e controllo, comprendano i rischi ai quali l'organizzazione è esposta e contribuiscano attivamente alla loro prevenzione e gestione.

In conformità agli obblighi previsti dalla normativa NIS 2, dalle disposizioni nazionali applicabili e dalle specifiche di base emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN), l'organizzazione definisce e mantiene un Piano di Formazione e Consapevolezza che individua obiettivi, contenuti, destinatari, modalità di erogazione e criteri di verifica delle attività formative (es. campagna di phishing). Il piano è aggiornato annualmente tenendo conto dell'evoluzione delle minacce, delle tecnologie adottate, delle esigenze organizzative e delle modifiche del quadro normativo.

Le attività formative sono differenziate in funzione dei ruoli, delle responsabilità e del livello di esposizione ai rischi cyber. A tutto il personale sono rivolte iniziative di sensibilizzazione volte a promuovere comportamenti sicuri e a rafforzare la capacità di riconoscere e segnalare tempestivamente eventi anomali, tentativi di frode, campagne di phishing e altre minacce informatiche. Specifici percorsi formativi sono inoltre previsti per il management, per i responsabili di processo e per il personale che ricopre funzioni con responsabilità organizzative, al fine di assicurare una piena comprensione dei requisiti normativi, dei rischi e delle responsabilità correlate alla sicurezza delle informazioni.

Particolare attenzione è dedicata alle figure tecniche e specialistiche che svolgono attività rilevanti ai fini della sicurezza informatica, tra cui gli amministratori di sistema, il personale ICT, i responsabili della sicurezza e gli altri soggetti coinvolti nella gestione, protezione e monitoraggio dei sistemi informativi e di rete. Per tali ruoli sono previsti percorsi di formazione specialistica e di aggiornamento professionale finalizzati a garantire il mantenimento delle competenze necessarie per affrontare efficacemente l'evoluzione delle minacce e delle tecnologie.

L'organizzazione assicura inoltre lo sviluppo continuo delle competenze del personale incaricato del monitoraggio, della rilevazione e della risposta agli eventi e agli incidenti di sicurezza, affinché sia in grado di identificare tempestivamente i segnali di compromissione, valutare correttamente le minacce emergenti e attivare le opportune misure di risposta e contenimento. Analogamente, sono promosse iniziative di aggiornamento continuo volte a garantire il mantenimento nel tempo della conformità ai requisiti normativi, regolamentari e organizzativi applicabili.

Ove ritenuto opportuno in relazione ai contenuti trattati e ai rischi da mitigare, le attività formative possono prevedere meccanismi di verifica dell'apprendimento e dell'efficacia, inclusi test, esercitazioni, simulazioni e altre forme di valutazione finalizzate a misurare il livello di consapevolezza e competenza acquisito.

Tutte le attività di formazione, sensibilizzazione e aggiornamento devono essere adeguatamente documentate e tracciate, garantendo la disponibilità di evidenze che consentano di dimostrarne l'effettiva erogazione, la partecipazione dei destinatari e, ove applicabile, il superamento delle verifiche previste. Tale approccio consente all'Azienda ULSS8 di assicurare la crescita continua della cultura della sicurezza, il rafforzamento delle capacità di risposta ai rischi cyber e il mantenimento di un adeguato livello di conformità nel tempo.

3.10.2 Attuazione e responsabilità operative

La realizzazione delle attività formative realizzate in sede (calendari, contenuti di dettaglio, piattaforme, registri delle presenze e delle verifiche) è gestita dalla UOSD Formazione mediante documentazione operativa, senza necessità di riapprovazione da parte del vertice. Inoltre vengono gestite le richieste di partecipazione ad attività formative realizzate da soggetti terzi.

3.10.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.10.1 Piano di formazione sulla sicurezza informatica

3.11 PIANO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

Misura di riferimento	RS.MA-01 (punto 2)
Funzione (FNCDP)	RESPOND (RS) – RS.MA «Gestione degli incidenti»

3.11.1 Finalità e indirizzo strategico

Gli organi di amministrazione e direttivi adottano e approvano le modalità di implementazione del piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, in coerenza con l'articolo 25 del decreto NIS. Il piano assicura il tempestivo coinvolgimento del vertice nelle comunicazioni interne rilevanti ed è riesaminato almeno ogni due anni, integrando le lezioni apprese (RS.MA-01, punto 3).

Sintesi del contenuto del piano

L'Azienda ULSS8 adotta un processo strutturato di gestione degli incidenti di sicurezza informatica al fine di garantire la tempestiva identificazione, classificazione, gestione, contenimento e risoluzione degli eventi che possono compromettere la riservatezza, l'integrità, l'autenticità e la disponibilità delle informazioni, dei sistemi informativi e dei servizi essenziali. Tale processo assicura una risposta coordinata e conforme agli obblighi normativi applicabili, contribuendo a limitare gli impatti operativi, economici, reputazionali e normativi derivanti dal verificarsi di incidenti di sicurezza.

A tal fine, è definito e mantenuto un Piano di Gestione e Notifica degli Incidenti che disciplina l'intero ciclo di vita dell'incidente, dalla fase di rilevazione e segnalazione iniziale fino alle attività di contenimento, eradicazione, ripristino e analisi post-evento. Il piano stabilisce procedure formalizzate per la gestione e la notifica degli incidenti significativi alle autorità competenti, in conformità a quanto previsto dall'articolo 25 del Decreto Legislativo n. 138/2024 di recepimento della Direttiva NIS 2 e dalle disposizioni emanate dall'Agenzia per la Cybersicurezza Nazionale.

Il piano definisce ruoli, responsabilità e livelli di coinvolgimento delle diverse funzioni aziendali, individuando con chiarezza i soggetti responsabili della rilevazione, valutazione, classificazione e gestione degli incidenti. Sono inoltre definiti i canali di segnalazione, i punti di contatto, le procedure di escalation e le modalità di coordinamento tra le strutture organizzative coinvolte, al fine di assicurare una gestione efficace e tempestiva degli eventi di sicurezza.

Particolare attenzione è dedicata agli obblighi di comunicazione e notifica, sia verso l'interno dell'organizzazione sia verso soggetti esterni. Il piano disciplina le modalità di comunicazione verso il CSIRT Italia, l'Autorità Nazionale Competente NIS, le altre autorità eventualmente coinvolte, nonché verso utenti, fornitori, partner e stakeholder interessati, quando richiesto dalla natura e dalla gravità dell'evento. Sono inoltre definiti i modelli di reportistica, la documentazione da produrre e le evidenze da conservare durante tutte le fasi di gestione dell'incidente.

Per gli incidenti classificati come significativi o ad elevato impatto è previsto il tempestivo coinvolgimento della Direzione Strategica e delle altre funzioni di governo competenti, affinché possano assumere le decisioni necessarie, garantire il coordinamento delle attività di risposta e valutare gli impatti operativi, organizzativi e reputazionali derivanti dall'evento. Il flusso di comunicazione verso il vertice aziendale è definito preventivamente e costituisce un elemento essenziale del modello di governance della gestione degli incidenti.

Il Piano di Gestione e Notifica degli Incidenti opera in coordinamento con i processi di gestione delle crisi, continuità operativa e disaster recovery, assicurando una risposta integrata agli eventi di maggiore gravità e favorendo il rapido ripristino delle normali condizioni operative. Al termine di ciascun incidente significativo sono inoltre svolte attività di analisi e riesame finalizzate all'individuazione delle cause, delle eventuali carenze organizzative o tecniche e delle opportunità di miglioramento delle misure di sicurezza adottate.

Il piano è sottoposto a riesame e aggiornamento periodico, con cadenza almeno biennale o a seguito di modifiche rilevanti del contesto organizzativo, tecnologico o normativo. Le lezioni apprese derivanti dalla gestione degli incidenti, dai test e dalle esercitazioni sono sistematicamente raccolte, documentate e utilizzate per il miglioramento continuo delle capacità di prevenzione, rilevazione, risposta e recupero dell'organizzazione, contribuendo al rafforzamento della resilienza complessiva dei sistemi informativi e di rete dell'Azienda ULSS8.

3.11.2 Attuazione e responsabilità operative

I playbook di risposta, le procedure di triage, le modalità operative di notifica e la reportistica di dettaglio sono definiti e aggiornati dalle articolazioni competenti mediante procedure tecniche e istruzioni operative.

3.11.3 Documenti di riferimento

I documenti di riferimento collegati a questa sezione sono:

- 3.11.1 Piano di gestione della crisi cyber
- 3.11.2 Comitato di Gestione di Gestione della Crisi Cyber
- 3.11.3 Incident Response Plan

4 DISPOSIZIONI FINALI

4.1 APPROVAZIONE E REVISIONE

Il presente documento definisce i principi e gli indirizzi generali adottati dall'Azienda ULSS8 in materia di cybersicurezza e resilienza dei sistemi informativi e di rete ed è formalmente approvato dagli organi di amministrazione e direttivi competenti. In conformità ai requisiti normativi applicabili e ai principi di governance della sicurezza, la responsabilità della sua approvazione rimane in capo agli organi di vertice e non può essere delegata ad altre funzioni o soggetti.

Il documento è stato redatto in conformità con gli obiettivi strategici dell'organizzazione, con il profilo di rischio dell'Azienda e con il quadro normativo vigente. Il documento viene diffuso a cura delle strutture aziendali competenti.

Il documento è sottoposto a riesame ogni qualvolta intervengano modifiche sostanziali del contesto normativo, organizzativo o tecnologico, nonché a seguito di incidenti di sicurezza significativi, eventi di crisi, cambiamenti rilevanti dei sistemi informativi e di rete o variazioni del livello di esposizione ai rischi cyber. Il riesame ha lo scopo di verificare l'adeguatezza, l'efficacia e la continua coerenza delle disposizioni contenute nel documento rispetto alle esigenze dell'organizzazione e ai requisiti applicabili.

In assenza di modifiche significative che ne rendano necessario l'aggiornamento, il presente documento mantiene la propria validità senza richiedere una revisione periodica obbligatoria, fermo restando l'obbligo dei soggetti competenti di monitorarne costantemente l'adeguatezza e di promuoverne l'aggiornamento qualora emergano nuove esigenze, vulnerabilità, minacce o prescrizioni normative.

Ogni modifica, integrazione o revisione del documento è soggetta al medesimo processo di approvazione previsto per la sua adozione iniziale, al fine di garantire la piena assunzione di responsabilità da parte degli organi di amministrazione e direttivi e il mantenimento di un efficace sistema di governo della cybersicurezza e della resilienza organizzativa.

4.2 RAPPORTO CON I PRESIDI DOCUMENTALI E ORGANIZZATIVI

Gli indirizzi, i principi e gli obiettivi definiti nel presente documento sono attuati dalle strutture organizzative competenti dell'Azienda ULSS8 Berica attraverso la predisposizione e il mantenimento di procedure, istruzioni operative, standard tecnici, manuali, linee guida, piani, registrazioni e altra documentazione di supporto necessaria a garantirne la concreta applicazione. Tali strumenti disciplinano gli aspetti operativi, organizzativi e tecnologici connessi alla gestione della cybersicurezza e della resilienza dei sistemi informativi e di rete, assicurando l'effettiva implementazione delle disposizioni qui contenute.

I soggetti competenti sono responsabili della definizione, dell'aggiornamento e del monitoraggio di tali presidi operativi, nel rispetto degli indirizzi strategici approvati e delle responsabilità attribuite dal modello di governance della sicurezza. L'evoluzione del contesto normativo, organizzativo, tecnologico e di rischio può rendere necessario l'adeguamento delle procedure e della documentazione di dettaglio, al fine di garantirne la costante efficacia e coerenza con le esigenze dell'organizzazione.

L'aggiornamento delle procedure, delle istruzioni operative, dei manuali, dei piani e degli altri documenti attuativi non richiede una nuova approvazione del presente documento, purché tali modifiche non comportino variazioni sostanziali degli indirizzi strategici, dei principi di governo, degli obiettivi o delle responsabilità qui definiti. In tali casi, gli aggiornamenti sono approvati secondo i processi e le competenze previste dal sistema documentale interno.

Qualora, invece, le modifiche ai documenti attuativi determinino la necessità di rivedere gli indirizzi strategici, il modello di governance, gli obiettivi di sicurezza o altri elementi strategici disciplinati dal presente documento, dovrà essere avviato il relativo processo di revisione e sottoposta all'approvazione degli organi di amministrazione e direttivi la nuova versione del documento, secondo le modalità previste per la sua adozione.

4.3 DELEGA DELLE ATTIVITÀ OPERATIVE

Fermo restando il carattere non delegabile delle responsabilità attribuite agli organi di amministrazione e direttivi, e in particolare dell'approvazione del presente documento e delle decisioni strategiche in materia di cybersicurezza, tali organi possono attribuire alle strutture e alle funzioni competenti l'esecuzione delle attività operative necessarie all'attuazione delle misure previste dalla normativa applicabile e dal sistema di gestione della sicurezza.

Le articolazioni organizzative competenti sono responsabili della pianificazione, dell'implementazione, del monitoraggio e del mantenimento dei processi, delle procedure e delle misure tecniche e organizzative necessarie a garantire la conformità ai requisiti di sicurezza e resilienza dei sistemi informativi e di rete. L'attribuzione di tali compiti operativi non comporta il trasferimento delle responsabilità di indirizzo, supervisione e controllo che rimangono in capo agli organi di amministrazione e direttivi.

Al fine di consentire l'effettivo esercizio delle proprie funzioni di governo e vigilanza, sono definiti adeguati flussi informativi tra le strutture operative e il vertice dell'organizzazione. Tali flussi assicurano una rendicontazione periodica e tempestiva sullo stato di attuazione delle misure di sicurezza, sul livello di esposizione al rischio, sugli incidenti rilevanti, sulle eventuali criticità riscontrate e sullo stato di avanzamento delle attività di adeguamento e miglioramento.

Le informazioni fornite agli organi di amministrazione e direttivi devono essere complete, accurate e commisurate alla rilevanza delle decisioni da assumere, affinché il vertice possa esercitare in modo consapevole le proprie responsabilità in materia di gestione del rischio cyber, sicurezza delle informazioni e resilienza operativa. Tale modello di governance garantisce un efficace equilibrio tra responsabilità strategica e attuazione operativa, assicurando al contempo il necessario livello di supervisione e controllo da parte degli organi competenti.