Piano di gestione delle vulnerabilità

Autore: DIREZIONE IT

Tipo Documento: Aziendale

Versione	Data	Descrizione
1.0	28 – 08- 2026	Creazione documento
1.1	30 – 08 – 2026	Aggiornamento alla Determinazione ACN 379907/2025; raccordo SIR/rischio e disciplina dell'accettazione del rischio residuo
1.2	30 – 08 – 2026	Allineamento esplicito di ID.RA-08 ai canali CSIRT Italia, CERT e ISAC settoriali

Ai fini della NIS2, il presente documento tiene in considerazione lo stato della conoscenza attuale dei sistemi rilevanti di Ateneo derivabili dalla documentazione relativa alla certificazione della ISO27001.

EXECUTIVE SUMMARY

Il contesto e la necessità di governo

I sistemi informatici presentano costantemente falle di sicurezza (vulnerabilità del software o di configurazione) che rappresentano la principale porta di ingresso per gli attacchi informatici. Per adempiere alle specifiche obbligatorie dell'Agenzia per la Cybersicurezza Nazionale (ACN) e della Direttiva NIS 2, l'Ateneo formalizza un processo sistematico per individuare, dare priorità e correggere tali debolezze prima che possano essere sfruttate da soggetti terzi.

Come funziona il processo operativo

Il piano organizza la gestione delle vulnerabilità come un ciclo continuo articolato su tre direttrici:

- Ascolto Continuo delle Fonti Esterne (Threat Intelligence): Monitoraggio periodico (massimo ogni 15 giorni) dei bollettini di allerta emessi dalle autorità competenti (CSIRT Italia, eventuali CERT e Information Sharing & Analysis Centre (ISAC) settoriali, CERT-AGID, ENISA, NIST) e dai fornitori dei software critici adottati dall'Ateneo.
- Scansioni Tecniche e Test Preventivi (Vulnerability Assessment): Scansioni periodiche programmate sui sistemi e verifiche obbligatorie prima della messa in esercizio di nuovi apparati o servizi.
- Prioritizzazione e Tempi Massimi di Risoluzione: Le falle individuate vengono classificate per gravità (*Critical, High, Medium*). A ogni livello corrispondono scadenze tassative di intervento per l'applicazione delle patch correttive (*remediation*), l'adozione di misure compensative temporanee o l'eventuale gestione con i fornitori terzi.

Implicazioni e decisioni cardine richieste al cda

1. Approvazione Formale del Piano: Adottare il documento per soddisfare il requisito normativo vincolante ACN (misura ID.RA-08).
2. Autorità sull'Accettazione dei Rischi Residui: una vulnerabilità tecnica non eliminabile nell'immediato non comporta automaticamente un'accettazione da parte del CdA. La vulnerabilità alimenta la valutazione del rischio; l'eccezione tecnica temporanea è gestita entro le deleghe e con misure compensative. È riservata al Consiglio di Amministrazione l'accettazione del rischio residuo effettivo risultante quando è di classe Molto alto (12–16), eccede le deleghe, richiede una deroga sostanziale alle misure applicabili o presenta conseguenze strategiche o finanziarie rilevanti.
3. Supervisione e Riesame Biennale: Ricevere gli esiti periodici delle verifiche e approvare i riesami del piano (con cadenza almeno biennale o straordinaria in caso di incidenti e cambiamenti normativi).

1 SCOPO

Il presente Piano definisce, ad alto livello, il processo adottato dall'Organizzazione per la gestione delle vulnerabilità dei sistemi informativi e di rete, in coerenza con le misure ID.RA-01, ID.RA-05, ID.RA-06 e ID.RA-08 della Determinazione ACN n. 379907 del 19 dicembre 2025, applicabile dal 15 gennaio 2026, e relativi allegati tecnici vigenti.

Il Piano coordina le attività di acquisizione delle informazioni sulle vulnerabilità, identificazione tecnica, registrazione, analisi, prioritizzazione, trattamento e verifica della chiusura, rinviando per le modalità operative alle procedure PRO003 - Procedura per i contatti con le autorità ed i gruppi specialistici e PRO004 - Procedura per Vulnerability Assessment.

Per gli aspetti di valutazione e trattamento del rischio, il presente Piano costituisce il raccordo con il processo generale di gestione del rischio dell'Organizzazione e non sostituisce la relativa valutazione del rischio né il piano di trattamento del rischio previsti dalle misure ID.RA-05 e ID.RA-06.

Fonti autoritative. Il documento «Organizzazione per la sicurezza informatica» e la Matrice RACI governano ruoli e responsabilità; la Valutazione del rischio e ALL004 governano metodologia e registro; il Piano di trattamento del rischio e di gestione delle crisi governa decisioni di trattamento ed escalation; il Piano di adeguamento governa le azioni strutturali derivanti da gap e verifiche. Ogni vulnerabilità rilevante deve essere collegata al SIR interessato, al relativo Responsabile SIR, al rischio registrato in ALL004 quando applicabile e all'eventuale azione di trattamento o adeguamento.

2 CAMPO DI APPLICAZIONE

Il Piano si applica ai sistemi informativi e di rete rientranti nel perimetro NIS dell'Ateneo. Alla data di emissione il perimetro utilizza come base quello del SGSI ISO 27001 della Direzione IT, che copre secondo la ricognizione disponibile circa il 95–98% dei SIR rilevanti, ed è soggetto a ricognizione continua. Per un SIR esterno al perimetro gestionale della Direzione IT, il governo dell'attività spetta al Responsabile SIR formalmente individuato e l'esecuzione al Gestore tecnico; Direzione IT e RSGSI assicurano raccordo, standard comuni e supporto. Sono coinvolti, secondo competenza, amministratori di sistema, responsabili di servizio e soggetti esterni che gestiscono tecnicamente sistemi o apparati.

L'identificazione delle vulnerabilità è effettuata sia mediante fonti informative esterne, sia mediante attività tecniche di vulnerability assessment. Per i sistemi rilevanti, le attività sono pianificate con periodicità definita e devono essere integrate nel ciclo di messa in esercizio e gestione del sistema.

3 RESPONSABILITÀ

Ruolo	Responsabilità

Organi di Ateneo	Approvano il Piano e sorvegliano il processo; il Consiglio di Amministrazione accetta il rischio residuo effettivo nei casi riservati (12–16, fuori delega, deroga sostanziale o rilievo strategico/finanziario), non la vulnerabilità tecnica in quanto tale.
RSGSI Direzione IT	Coordina il Piano; mantiene e verifica le fonti informative previste dalla PRO003; assicura il raccordo con il processo di gestione del rischio e monitora l'attuazione delle misure.
Responsabile del servizio di Vulnerability Assessment	Gestisce il servizio di scansione, la configurazione delle attività periodiche e il supporto alla registrazione e verifica delle vulnerabilità secondo PRO004.
Amministratori di sistema / Responsabili dei sistemi	Assicurano l'inclusione dei sistemi nelle scansioni, analizzano i risultati, attuano le correzioni e documentano le azioni; segnalano le vulnerabilità non mitigabili.
Referente interno per sistemi gestiti da terzi	Coordina con il fornitore gli interventi tecnici sui sistemi o apparati esternalizzati e mantiene l'evidenza delle attività.
Direzione IT	Verifica periodicamente l'applicazione delle procedure e assicura le decisioni di escalation di competenza.

4 REQUISITI E DOCUMENTI COLLEGATI

Il presente Piano è definito in coerenza con:

- Direttiva (UE) 2022/2555 (NIS2);
- Decreto Legislativo 4 settembre 2024, n. 138;
- **Determinazione ACN n. 379907 del 19 dicembre 2025 - specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS, applicabile dal 15 gennaio 2026, con particolare riferimento alle misure ID.RA-01, ID.RA-05, ID.RA-06 e ID.RA-08;**
- **PRO003 - Procedura per i contatti con le autorità ed i gruppi specialistici;**
- PRO004 - Procedura per Vulnerability Assessment.

5 PIANO DI GESTIONE DELLE VULNERABILITÀ

Il processo è organizzato come un ciclo continuo: acquisizione delle informazioni, identificazione tecnica, registrazione, valutazione, trattamento, verifica e riesame. Le due procedure operative PRO003 e PRO004 costituiscono i principali meccanismi di attuazione del presente Piano.

5.1 Monitoraggio delle fonti e ricezione delle informazioni

In attuazione della PRO003, l'RSGSI della Direzione IT mantiene l'elenco delle fonti delle autorità di controllo e le verifica con periodicità non superiore a 15 giorni; i singoli amministratori di sistema o gestori di sistemi/software fanno analogamente per i gruppi specialistici pertinenti. Le informazioni di interesse vengono sintetizzate e comunicate ai soggetti tecnici competenti.

Le fonti comprendono almeno i canali di CSIRT Italia e degli eventuali CERT e Information Sharing & Analysis Centre (ISAC) settoriali e, tra le ulteriori fonti pertinenti, CERT-AGID, ENISA, NIST e i principali gruppi o produttori tecnologici. Per il software ritenuto critico, devono essere inclusi nel monitoraggio anche i canali del relativo fornitore, in coerenza con ID.RA-08.

Le informazioni ricevute sono valutate per stabilire l'eventuale applicabilità ai sistemi dell'Organizzazione. Se pertinenti, alimentano le attività di identificazione, verifica e trattamento di cui ai paragrafi successivi.

Per il dettaglio operativo si rimanda alla procedura stessa (Cfr. PRO003 - Procedura per i contatti con le autorità ed i gruppi specialistici)

5.2 Identificazione, conferma e registrazione delle vulnerabilità

La PRO004 disciplina le scansioni di vulnerabilità sui server e apparati gestiti dalla Direzione IT e, per i sistemi rilevanti ai fini NIS2, sul perimetro di Ateneo.

Le vulnerabilità identificate sono analizzate considerando almeno il livello di severità tecnica, la rilevanza del sistema, l'esposizione, le minacce applicabili, la probabilità di sfruttamento e il possibile impatto sulla riservatezza, integrità e disponibilità dei servizi e delle informazioni. Tali elementi alimentano la valutazione del rischio prevista da ID.RA-05 e supportano la priorità di intervento.

La PRO004 stabilisce termini massimi di gestione per le vulnerabilità classificate tra Critical e Medium, compreso il loro trattamento, mitigazione e accettazione del rischio, con tracciabilità delle operazioni eseguite (in accordo a ID.RA-01).

Per il dettaglio operativo si rimanda alla procedura stessa (Cfr. PRO004 Procedura per Vulnerability Assessment).

6 SINTESI: MAPPATURA DEI CONTROLLI ACN

Controllo	Requisito ad alto livello	Attuazione nel Piano	Riferimenti operativi
ID.RA-01	Identificare, confermare e registrare le vulnerabilità; svolgere attività periodiche e prima della messa in esercizio; documentare attività ed esiti.	Fonti esterne + VA; registrazione in report/ticket; tracciabilità delle vulnerabilità e delle verifiche.	PRO003 §§4.1-4.3; PRO004 §§4.1-4.5
ID.RA-05	Usare minacce, vulnerabilità, probabilità e impatti nella valutazione del rischio e nella prioritizzazione della risposta.	Le vulnerabilità tecniche alimentano il risk assessment e la priorità di rimedio, tenendo conto della rilevanza del sistema e dell'impatto potenziale.	PRO004 §4.4, in raccordo con il processo generale di gestione del rischio
ID.RA-06	Definire e monitorare il trattamento dei rischi, le priorità, i responsabili, le tempistiche, le misure compensative e il rischio residuo.	Remediation tecnica, mitigazioni alternative, escalation e accettazione documentata del rischio residuo.	PRO004 §§4.4 e Registrazione azioni correttive, in raccordo con il piano di trattamento del rischio

ID.RA-08	Monitorare i canali di divulgazione, analizzare e rispondere alle informazioni sulle vulnerabilità; definire e approvare il piano; monitorare i fornitori del software critico.	Monitoraggio fonti, valutazione di applicabilità, scansioni, ticket, mitigazione/accettazione e riesame del Piano.	PRO003 §§4.1-4.3; PRO004 §§4.1-4.5; presente Piano

7 DOCUMENTAZIONE, RIESAME E APPROVAZIONE

Le evidenze prodotte nell'ambito del Piano comprendono almeno: elenco delle fonti monitorate, report di vulnerability assessment, ticket di rimedio, comunicazioni sulle vulnerabilità non mitigabili, registrazioni delle azioni correttive, decisioni di mitigazione o accettazione del rischio e risultati delle verifiche successive.

Il Piano è riesaminato periodicamente, almeno ogni due anni, e comunque in presenza di variazioni rilevanti del perimetro, mutamenti significativi dell'esposizione alle minacce, incidenti significativi o modifiche normative che incidano sul processo di gestione delle vulnerabilità.

Il Piano e i suoi aggiornamenti sono approvati dagli Organi di Ateneo, come richiesto dalla misura ID.RA-08.

Procedura per i contatti con le autorità ed i gruppi specialistici

1. Scopo

Lo scopo della presente procedura è quello di definire come avviene la gestione dei contatti con le autorità e con i gruppi specialistici al fine di avere informazioni tempestive sulla sicurezza informatica, individuando per tempo eventuali minacce o vulnerabilità

2. Campo di applicazione

La presente procedura si applica a tutto il personale della Direzione Informatica e Tecnologie dell'Università di Verona e ad eventuali soggetti esterni che collaborano con la stessa per il raggiungimento dello scopo previsto al punto 1.

3. Responsabilità

Ruolo	Responsabilità
RSGSI	Definisce la procedura
RSGSI e i singoli AdS per le aree da loro gestite	Implementano l'applicazione della procedura
Direzione	Periodicamente controlla che la procedura sia seguita.

4. Procedura

4.1 Definizione delle autorità di controllo

Sono considerate autorità di controllo tutti gli organismi governativi o di derivazione governativa che offrono informazioni relative alla sicurezza informatica o alla gestione dei dati. A titolo non esaustivo, vengono individuati, ad esempio, i seguenti:

- Csirt nazionale
- CERT-AGID
- Garante della Privacy
- Polizia di Stato con particolare riferimento alla polizia postale
- Ministero dell'Istruzione
- Guardia di Finanza, nucleo speciale antifrode

4.2 Definizione dei gruppi specialistici

Sono considerati gruppi specialistici tutti gli organismi che offrono informazioni relative alla sicurezza informatica in determinati specifici ambienti gestiti dagli AdS . A titolo non esaustivo, vengono individuati, ad esempio, i seguenti:

- Microsoft
- Cisco
- Palo Alto
- Oracle

- Greenbone
- Mondoprivacy
- Enisa
- Nist

4.3 Attività da svolgere

Per quanto riguarda le autorità di controllo, il RSGSI gestisce i seguenti compiti:

1. Compila e mantiene aggiornato almeno annualmente l'allegato ALL039_Feed_Sicurezza.xlsx con l'elenco delle fonti delle autorità di controllo seguite;
2. Con periodicità non superiore ai 15 giorni verifica i siti internet delle autorità di controllo selezionate, valutando se vi sono informazioni che possano essere di interesse per la Direzione IT;
3. Successivamente, con newsletter periodiche, riassume quanto individuato in una mail, per i vari AdS;
4. Verifica periodicamente a campione che i vari AdS abbiano analizzato quanto comunicato.

Per quanto riguarda i gruppi specialistici, i singoli AdS o gestori di sistemi/software gestiscono i seguenti compiti:

1. Individuano i gruppi specialistici che definiscono di seguire in base alle loro specifiche attività;
2. Aggiornano almeno annualmente l'allegato ALL039_Feed_Sicurezza.xlsx con l'elenco delle fonti dei gruppi specialistici seguiti;
3. Con periodicità non superiore ai 15 giorni verificano i siti internet dei gruppi specialistici selezionati, valutando se vi sono informazioni che possano essere di interesse per altri colleghi della Direzione IT;
4. Nel caso vi siano informazioni di interesse per altri colleghi della Direzione IT, riassumono quanto individuato in una mail da indirizzare ai colleghi individuati;
5. Verificano periodicamente a campione che i vari componenti del loro gruppo abbiano analizzato quanto comunicato.

CHANGELOG

Versione 1.4:

- Aggiornati i riferimenti alla Direzione (intestazione, piè di pagina e riferimenti interni) in seguito a cambio di nome da riorganizzazione;
- Aggiornato l'elenco delle autorità di controllo (Aggiunto cert-agid).

Versione 1.3:

- Aggiornato l'elenco delle autorità di controllo da seguire per l'RSGSI
- Esplicitate con maggiore precisione le modalità di notifica delle notizie al resto della Direzione
- Aggiunto al sistema e collegato alla procedura un nuovo documento, ALL039_Feed_Sicurezza.xlsx, che raccoglie e classifica le fonti seguite da RSGSI e dai singoli AdS
- Indicate le modalità di aggiornamento del documento ALL039_Feed_Sicurezza.xslx