UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

Decreto n. 3554

IL RETTORE

VISTO	il Piano Triennale per l'informatica nella Pubblica Amministrazione 2017-2019;
VISTO	il Codice dell'Amministrazione Digitale (D.lgs. n. 235/2010 e s.m.i.);
VISTA	la circolare AGID n. 2/2017 del 18.04.2017;
VISTO	il *Codice sul trattamento dei dati personali (Regolamento UE 2016/679 del 27.04.2016);*
VISTO	lo Statuto di Ateneo;
VISTO	Il Regolamento per l'Amministrazione, la finanza e la contabilità;
VISTO	lo Statuto del Centro Servizi Informatici (CSI), emanato con D.R. n. 3823 del 28.11.2016, in particolare l'art. 6,comma 2, lett. d);
VISTO	l'estratto dal verbale del Comitato Tecnico Scientifico (CTS) del CSI, relativo alla riunione del 27.07.2017, di approvazione, per quanto di competenza, del Regolamento *de quo;*
VISTA	la nota prot. n. 67076-I/10 del 22.09.2017, a firma del Direttore Generale, con la quale il testo del Regolamento in parola, nella formulazione approvata dal CTS, è stato trasmesso alle OO.SS. e alle RSU, per opportuna conoscenza;
VISTO	il testo del "*Regolamento per la sicurezza dei servizi ICT dell'Università degli Studi di Bari Aldo Moro",* modificato a seguito dell'incontro con le OO.SS. ed RSU, acquisito per le vie brevi il parere del CTS del CSI;
VISTA	la delibera del Senato Accademico del 26.10.2017, con la quale è stato espresso parere favorevole in ordine al testo del suddetto Regolamento;
VISTA	la delibera del Consiglio di Amministrazione del 27.10.2017, di approvazione del testo del medesimo Regolamento,

D E C R E T A

E' emanato il "*Regolamento per la sicurezza dei servizi ICT dell'Università degli Studi di Bari Aldo Moro",* che entra in vigore il giorno successivo alla pubblicazione sul sito web istituzionale – Bollettino ufficiale e Albo online di Ateneo, secondo la formulazione di seguito riportata:

Regolamento per la sicurezza dei servizi ICT dell'Università egli studi di Bari Aldo Moro

1. Premessa

Il presente regolamento disciplina il livello di sicurezza dei servizi ICT (Information and Communication Technology) dell'Università di Bari attraverso l'assunzione di regole per la corretta fruizione dei servizi stessi.

La rete telematica e i servizi ICT dell'Università di Bari rappresentano un bene comune e condiviso dell'Ateneo; in quanto strumenti di lavoro e di promozione delle attività accademiche amministrative, gestionali, di didattica e di ricerca, sono soggetti a restrizioni d'uso qualora siano verificate infrazioni che possano comprometterne il funzionamento o il rispetto delle normative di legge.

2. Finalità e Ambito di applicazione

Il presente regolamento contiene le misure minime di sicurezza ICT per l'Ateneo, da armonizzare successivamente all'emanazione della normativa tecnica relativa alla sicurezza informatica delle Amministrazioni Pubbliche da parte del Dipartimento per la Funzione Pubblica, in conformità al Regolamento Generale della Protezione Dati (GDPR). Esso recepisce le raccomandazioni della circolare AGID n.2/2017 del 18/4/2017, che costituisce parte integrante del presente regolamento (allegato n. 1) e disciplina il livello di sicurezza della rete telematica dell'Università di Bari e dei sistemi ad essa collegati. Si applica a tutti i soggetti che utilizzano la rete. Integra in materia di sicurezza le norme previste dal Regolamento sulla Posta Elettronica e dal Regolamento sull'Utilizzo delle Risorse Software e Hardware dell'Università degli Studi di Bari Aldo Moro.

3. Definizioni

APM - L'APM è il referente tecnico verso il GARR dell'intero sito appartenente ad un soggetto autorizzato ad accedere alla rete GARR. Collabora con il GARR-CERT per la gestione degli incidenti informatici.

Autenticazione informatica - la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso così come riferito nel Nuovo Codice dell'Amministrazione Digitale, D.lgs. 235/2010 art. 1b "autenticazione del documento informatico" e successive modifiche e integrazioni;

Centro servizi informatici - struttura preposta alla gestione tecnica dei servizi informatici di Ateneo e gestione delle banche dati ad uso dell'amministrazione centrale, d'ora in poi CSI;

Credenziali di accesso - dati utilizzati nelle operazioni di autenticazione utente (nome utente e password);

Dato - Tutte le informazioni, indipendentemente dal formato, che sono contenute o elaborate da risorse informatiche dell'Ateneo o che sono contenute o elaborate da risorse informatiche di altri soggetti per conto dell'Ateneo;

Dato personale - qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Fornitore di Servizio – soggetto autorizzato ad accedere ai servizi di rete dell'Ateneo attraverso la rete telematica per attività di supporto e manutenzione;

GARR - Gruppo Armonizzazione Reti per la Ricerca creato nel 1988 che opera sotto la direzione del Ministero dell'Università e della Ricerca (MIUR)

GARR-CERT - Servizio GARR per la gestione degli incidenti di sicurezza informatici in cui siano coinvolti enti collegati alla rete GARR;

GDPR - Regolamento Generale della Protezione Dati, con il quale la Commissione europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione europea (UE). Affronta anche il tema dell'esportazione di dati personali al di fuori dell'UE;

Hardening - Processo di verifica e messa in sicurezza di un computer, mediante l'adozione di specifiche tecniche per ridurre i punti di attacco da parte di un hacker;

Host - ogni computer, stampante, periferica, telefono, fax o qualsiasi dispositivo informatico, di proprietà dell'Ateneo, connesso alla Rete telematica;

Indirizzo IP - Numero che identifica univocamente un host nella Rete Telematica di Ateneo;

Log - Qualsiasi registrazione delle attività elaborative compiute da un'applicazione che permette di ricostruire le operazioni svolte da un utilizzatore identificato o identificabile;

PDL - Postazione di Lavoro in cui si presta abitualmente servizio e comprendente, nell'accezione intesa in questo regolamento, un elaboratore elettronico collegato alla Rete informatica di Ateneo;

Personale - personale docente, personale tecnico-amministrativo, collaboratori, consulenti e terzi autorizzati dall'Università e/o da uno dei suoi organi;

Punto rete - punto di connessione fonia/dati, al quale può essere collegato un host;

Responsabile - Soggetto che indipendentemente dalla struttura a cui appartiene (Dipartimento, Centro, Laboratorio, Biblioteca, ecc.) ha il compito di coordinare risorse umane e tecnologiche nell'ambito di un contesto ben definito;

Rete di ateneo - insieme di infrastrutture fisiche e logiche che consentono la comunicazione e la trasmissione dati e fonia sia all'interno dell'Ateneo che verso l'esterno attraverso la rete di interconnessione gestita dal GARR;

Rete Garr - la rete italiana della ricerca, attualmente gestita dal Consortium GARR, a cui si collegano gli enti CNR, Enea, INFN, CRUI, Università, etc.;

Rete Internet - la rete geografica basata sul protocollo di comunicazione TCP/IP;

Risorse informatiche - Qualsiasi tipo di hardware, mezzo di comunicazione elettronica, rete di trasmissione dati, software e informazione in formato elettronico di proprietà dell'Ateneo o ad esso concessi in licenza d'uso; In particolare le risorse informatiche includono:

- sistemi informativi;
- software applicativi;
- software di base e d'ambiente (sistemi operativi, software di rete, sistemi per il controllo degli accessi, database, package, utility, ecc.)
- file e banche dati
- mainframe, mini - micro - personal computer, notebook, palmari e ogni altro sistema di elaborazione elettronica delle informazioni;
- stampanti, scanner, plotter, apparecchiature per l'archiviazione elettronica dei dati e i relativi supporti di memorizzazione, video terminali, ecc.;
- modem, dispositivi di rete di ogni tipo (concentratori, ripetitori, bridge, router, switch, gateway, access point wireless, etc.);
- mezzi trasmissioni per reti locali e per reti geografiche.

Server centrali di Ateneo - si indicano i sistemi che ospitano i servizi informatici centrali di Ateneo;

Servizi di rete - servizi che utilizzano la Rete Telematica di Ateneo e che sono erogati da alcune strutture dell'Ateneo per attività dell'amministrazione centrale, della didattica e della ricerca, posta elettronica, protocollo informatico, servizi di segreteria, sistema di rilevazione e gestione presenze, portale web di Ateneo, servizi di autenticazione e autorizzazione, etc.

"Servizi centrali di Ateneo" - servizi informatici erogati in nome e per conto dell'Ateneo dalle strutture amministrative centrali e che vengono utilizzati per l'intera amministrazione dell'Ateneo e per la ricerca. Rientrano in questa definizione tutti i servizi erogati dal CSI e dal Sistema Bibliotecario di Ateneo (SiBA);

"Servizi periferici di Ateneo" - servizi informatici erogati e ad utilizzo di specifiche strutture;

Utente - Qualsiasi dipendente dell'Ateneo, di altro ente, docente, ricercatore, personale tecnico-amministrativo, collaboratore, consulente, borsista, assegnista, cultore della materia, studente, alumnus, dottorando, specializzando dell'Università che accede ai servizi di rete dell'Ateneo attraverso la Rete Telematica di Ateneo.

4. Organismi preposti alla sicurezza dei servizi ICT e loro funzioni

4.1. Responsabile della Sicurezza Informatica

Le funzioni di Responsabile della Sicurezza Informatica dell'Ateneo sono svolte dal Direttore Tecnico del CSI. In particolare, il Responsabile della Sicurezza Informatica ha il compito di:

- Presentare, annualmente entro il mese di dicembre, al CTS del CSI una relazione sul lavoro svolto, in particolare sulle problematiche che si sono presentate, sulle soluzioni adottate e sulla politica da adottare per la difesa delle infrastrutture software e hardware dell'Ateneo;

- interagire con i referenti di struttura, di cui al punto 4.3., per la risoluzione dei problemi legati alla sicurezza;

- rispondere in tempi brevi a eventi imprevisti riguardanti la sicurezza nella rete di Ateneo;

- per periodi di tempo limitati, o comunque da stabilirsi in relazione agli accadimenti, assumere tutte le misure necessarie atte a rispristinare il corretto funzionamento della rete o dei servizi d'Ateneo;

- svolgere attività di consulenza verso le Strutture in caso di incidenti di sicurezza;

- coordinare il Gruppo di sicurezza ICT.

4.2. Gruppo Sicurezza ICT

Il Gruppo Sicurezza ICT è costituito dai responsabili delle strutture del CSI (responsabile di Sezione e responsabili di Unità Operativa), dal Responsabile della Sicurezza, che lo coordina, e dall'APM di Ateneo.
Il Gruppo Sicurezza ICT svolge i seguenti compiti:

- monitorare i Servizi ICT d'Ateneo dal punto di vista della sicurezza;

- valutare l'opportunità di installare sulla rete dispositivi di filtraggio del traffico;

- valutare l'opportunità di installare sulla rete o su segmenti di rete dispositivi per l'analisi e il monitoraggio del traffico, al fine di favorire il controllo dell'effettiva applicazione delle direttive del presente Regolamento;

- occuparsi di problematiche relative a DOS/DDOS, intrusioni, virus e worm, pirateria informatica e in generale di problemi di sicurezza che possono assumere proporzioni tali da riguardare l'intera rete d'Ateneo o di una sua intera sottorete;

- rende operative le direttive di sicurezza assunte dal Responsabile della sicurezza informatica.

4.3. Referenti di struttura per la sicurezza

Ciascun Dipartimento, Direzione o altra Struttura prevista nel modello organizzativo di Ateneo individua uno o più referenti a cui affidare il compito della gestione locale dei sistemi e della rete, nel rispetto delle norme del presente Regolamento, provvedendo, in accordo con il CSI, alla funzionalità degli apparati attivi della rete presenti nella Struttura.
A tal fine è necessario che il referente:

- Conosca la topologia della rete LAN della Struttura di competenza implementando un inventario dei dispositivi di rete e delle risorse, mediante una procedura informatica resa disponibile dal CSI;

- Esegua periodiche scansioni sui sistemi al fine di rilevare la presenza di software non autorizzati;

- Verifichi che solo i servizi registrati e amministrati siano accessibili in rete dall'esterno della Struttura;

- Segnali al Responsabile della Sicurezza Informatica dell'Ateneo eventuali incidenti o problemi di sicurezza, intrusioni o tentativi di intrusione che abbiano avuto come oggetto host appartenenti alla Struttura di riferimento;

- Segnali al Responsabile della Sicurezza Informatica dell'Ateneo host che producono grandi flussi di dati in rete, applicazioni ad alto consumo di banda e qualunque altra attività in rete della Struttura di appartenenza che comporti un carico eccessivo sulla rete o un suo utilizzo improprio o non standard (streaming audio/video/multimedia, backup, salvataggi e archiviazioni, etc.).

- Esegua le attività indicate dal Responsabile della Sicurezza Informatica dell'Ateneo in presenza di anomalie del sistema al fine di portarlo a norma o isolarlo dalla rete;

- Effettui periodicamente una scansione delle vulnerabilità di sicurezza note, utilizzando strumenti che il CSI rende disponibili a tale scopo;

- Si assicuri di modificare opportunamente le credenziali predefinite di amministratore, prima di collegare alla rete un nuovo dispositivo;

- Gestisca l'attivazione di nuovi utenti dei sistemi e dei servizi secondo procedure predisposte dal CSI, informando sulle modalità di accesso, fornendo l'assistenza necessaria per la corretta procedura di connessione e rendendo noto che, in caso di emergenza e per motivi di sicurezza, le userid possono essere disattivate anche senza preavviso.

5. Regole di sicurezza fisica dei sistemi

Al fine di proteggere i sistemi, i locali che li ospitano dovranno possedere alcune caratteristiche indipendenti dal tipo di piattaforme hardware e dai sistemi software adottati. Di norma tali locali devono essere:

- dedicati ai server e preferibilmente presidiati;

- dotati di un sistema, meccanico o elettronico, di selezione e controllo degli accessi;

- equipaggiati con dispositivi di stabilizzazione e continuità della tensione;

- climatizzati;

- dotati di un sistema di estinzione degli incendi

6. Regole per la sicurezza logica dei servizi ICT, dei server e dei sistemi centrali d'ateneo

Tutti i server dell'università devono uniformarsi alle direttive di sicurezza e continuità del servizio descritte di seguito:

- Sicurezza fisica e controllo accessi

- Continuità del Servizio e disaster recovery
- Integrità dati e sistemi
- Protezione da programmi malevoli (antivirus/worm/Trojan)
- Aggiornamento dei sistemi operativi
- Gestione dei criteri di sicurezza e complessità delle password
- Management locale e remoto
- Log di sistema e loro gestione
- Configurazioni di base per la sicurezza e Hardening
- Controllo di interventi sui sistemi da parte di personale esterno autorizzato

Quali ulteriori misure di sicurezza è consigliabile:

- impostare password per l'accesso al BIOS, in modo da consentire l'avvio del sistema esclusivamente da disco rigido;
- disabilitare le porte TCP e UDP inutili e potenzialmente pericolose;
- prestare attenzione agli *alert* in tema di sicurezza (con particolare riferimento alla vulnerabilità dei sistemi operativi e alle applicazioni di base), installare le patch non appena disponibili valutando in ogni caso le azioni da intraprendere nel periodo intermedio in base al tipo e livello di rischio. In ogni caso i sistemi operativi e i pacchetti di base dovranno essere regolarmente aggiornati, compatibilmente con le applicazioni installate sui sistemi.

7. Regole per la sicurezza logica dei servizi ICT periferici

7.1. Soggetti coinvolti

L'accesso alla rete telematica d'ateneo e ai relativi servizi, incluso il Wi-Fi, è reso disponibile a tutti gli utenti, alle strutture dell'Ateneo e agli Enti e organizzazioni universitarie autorizzati dal Consiglio di Amministrazione.

7.2 Autenticazione dei soggetti in rete

Tutti gli utenti a cui vengono forniti accessi alla rete di Ateneo devono essere riconosciuti ed identificabili; fanno eccezione, gli utenti dei computer nel corso delle lezioni ed esercitazioni tenute presso le aule informatiche sotto la sorveglianza del docente, per le quali è richiesta la identificazione dei partecipanti mediante la compilazione di un modulo/registro messo a disposizione dal CSI, ma non è necessaria la identificazione dell'utente della singola postazione.
Al di fuori di questa ipotesi è vietata l'assegnazione di password collettive o non riconducibili ad un singolo soggetto fisico.
L'accesso e la navigazione Internet avvengono attraverso il sistema di autenticazione dell'Università di Bari.

7.3. Protocolli e programmi consentiti

Nella rete di Ateneo viene garantito il supporto per la suite di protocolli TCP/IP; le strutture hanno facoltà di utilizzare al loro interno anche altri protocolli, dandone comunicazione preventiva al

Responsabile della Sicurezza Informatica dell'Ateneo, a patto che rimangano totalmente confinati all'interno delle strutture medesime. La propagazione di altri protocolli di rete non può essere consentita esternamente alle strutture salvo casi particolari da concordare con il Responsabile della Sicurezza Informatica dell'Ateneo.
Non è consentito installare programmi non esplicitamente autorizzati e certificati dall'Amministrazione Universitaria. Gli amministratori dei sistemi informatici, di cui al punto 8., utilizzati per la didattica e la ricerca, sono responsabili dei programmi installati su tali sistemi.
Eventuali applicazioni software o file ritenuti pericolosi, non a norma o che violino il diritto d'autore devono essere eliminati.

7.4. Accesso ed estensioni della rete

- Sono vietate estensioni della rete di Ateneo, temporanee o permanenti, via VPN o altri meccanismi di tunneling analoghi, a meno di casi particolari concordati e autorizzati dal CSI.

- L'accesso alle postazioni personali o sistemi di calcolo dall'esterno della rete di Ateneo è consentito solo in caso di particolari esigenze lavorative e previa autorizzazione del CSI.

- Le operazioni di amministrazione remota di server, workstation, dispositivi di reti e analoghe apparecchiature devono essere eseguite secondo le indicazioni del Responsabile della Sicurezza Informatica per la Sicurezza.

- L'implementazione di una rete via radio (wireless) è consentita previa autorizzazione del CSI. Come le sotto reti cablate dell'università, anche reti Wireless devono essere progettate e realizzate dal CSI in accordo con la Struttura che ne ha fatto richiesta. L'implementazione della soluzione wireless deve essere tale da garantire l'accesso soltanto agli utenti abilitati previa autenticazione.

7.5. Collegamento di un client alla rete

Per ogni postazione client collegata alla rete occorre:

- Installare la protezione antivirus di Ateneo;

- Controllare se la macchina eroga servizi di rete non autorizzati ed eliminarli tutti;

- Applicare tempestivamente tutte le patch di sicurezza del sistema e degli applicativi di cui si intende fare uso e mantenerne nel tempo l'aggiornamento. La persona a cui la macchina in rete è data in consegna è responsabile per quella macchina e per la sua attività nella rete di Ateneo e in Internet.

7.6. Collegamento di un server/apparato alla rete

Per il collegamento di un server/apparato alla rete, il responsabile della Struttura deve compilare e sottoscrivere un apposito modulo predisposto dal CSI individuando l'amministratore del sistema e il responsabile tecnico e amministrativo in termini di sicurezza e affidabilità del sistema.

7.7. Aule informatiche/laboratori informatici per l'accesso degli studenti

Le aule informatiche e i laboratori devono essere strutturate valutando con il CSI le modalità di implementazione.
I server presenti nelle aule sono da considerarsi server di rete locale e i servizi da loro offerti devono essere confinati all'interno dell'aula informatica.
L'autenticazione degli utenti all'interno delle aule può essere a carico delle singole aule informatizzate o appoggiarsi a un sistema di autenticazione centralizzato di ateneo.

7.8. Servizi erogati in rete da parte delle strutture periferiche.

Per tutti i servizi di rete che vengono erogati da host appartenenti alla rete di Ateneo è necessario individuare uno o più responsabili che se ne occupino in maniera continuativa. Essi dovranno definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, portatili, etc.); a ciascuna azione per la risoluzione delle vulnerabilità sarà attribuito un livello di priorità in base al rischio associato. In particolare, le patch per le vulnerabilità devono essere applicate a partire da quelle più critiche, valutando eventuali misure alternative.
I servizi ICT devono essere accessibili esclusivamente dal bacino di utenza al quale sono indirizzati. Eventuali servizi ICT non necessari vanno disattivati.
I server devono essere sincronizzati con i server NTP ufficiali per permettere una corretta manutenzione del servizio. L'accesso privilegiato al sistema deve essere riservato al solo amministratore in modalità *console* o in modalità cifrata se effettuato da remoto (ad esempio tramite il protocollo SSH).
Il responsabile del servizio deve garantire la protezione fisica della macchina da accessi incontrollati, ovvero è necessario autenticare gli utenti, le macchine e le reti che devono poter accedere ad eventuali parti riservate del servizio.

7.9. Servizi in outsourcing

I servizi in outsourcing devono rispettare le norme del presente regolamento.

7.10. Attività di logging e auditing

Il CSI può effettuare attività di logging e auditing sugli apparati della rete UniBa allo scopo di produrre statistiche sull'utilizzo, sull'occupazione di banda e sulla tipologia di servizi o protocolli, al fine di ottimizzare i flussi di dati entro la rete stessa.

8. Regole per gli amministratori dei sistemi e delle applicazioni

- L'amministratore di sistema provvede alla gestione e manutenzione di sistemi di elaborazione o delle loro componenti. Esso è individuato dal responsabile della Struttura.
- L'amministratore di sistema assegna a ciascun utente una userid personale per l'accesso ai sistemi: una stessa userid non può essere assegnata a persone diverse neanche in tempi diversi, con l'eccezione degli userid di amministrazione se i sistemi operativi usati ammettono un solo livello di userid per l'amministrazione. Gli accessi degli amministratori devono comunque avvenire in prima istanza con la userid personale per consentire la tracciabilità delle sessioni.
- L' amministratore deve prontamente disattivare le userid degli utenti se questi perdono il diritto di accesso ai sistemi o se le userid rimangono inutilizzate per più di sei mesi.
- Le password di amministrazione dei sistemi dovranno essere:
  - cambiate periodicamente;
  - note esclusivamente agli amministratori;
  - diverse per ciascun sistema;
  - diverse da quelle già utilizzate in passato;

- non coincidenti con le userid di amministrazione, neanche temporaneamente;
- non banali e comunque di complessità adeguata al tipo di sistema;
- non usate per scopi diversi dall'amministrazione dei sistemi.

Nessun applicativo deve far uso delle password di amministrazione, né aver bisogno dei privilegi di amministratore per il corretto funzionamento.

- L'amministratore di sistema deve installare i sistemi di protezione antivirus informatici d'Ateneo. Le applicazioni antivirus dovranno essere aggiornate in maniera automatica su base periodica; dovranno inoltre consentire la possibilità di aggiornamento manuale per far fronte ai casi di emergenza, come ad esempio in seguito a segnalazioni di diffusione di virus importanti.

- L'amministratore di sistema dovrà supervisionare eventuali accessi ai sistemi da parte di personale esterno, quale ad esempio fornitori di hardware o di servizi. Qualora l'amministratore debba comunicare a consulenti esterni una o più password di amministrazione, di sistema o di base dati, le stesse dovranno essere sostituite prima e dopo il periodo di utilizzo.

- Gli accessi con i privilegi di amministrazione devono di norma avvenire da postazioni interne alla struttura. Eventuali accessi dall'esterno dovranno essere ridotti al minimo indispensabile e con connessioni cifrate.

8.1. Monitoraggio e Logging

I sistemi dovranno disporre di procedure per la registrazione dei messaggi di sistema e delle applicazioni di base attraverso meccanismi di logging per tutte le operazioni critiche.
I log di sistema devono essere analizzati regolarmente, preferibilmente per mezzo di meccanismi automatici di scansione in grado di generare allarmi a seguito di eventi rilevanti per la sicurezza del sistema.
I sistemi dovranno essere configurati in modo da accettare connessioni solo da parte dei client autorizzati e dagli amministratori.
Ove possibile, a livello di rete dovranno essere adottati sistemi per il controllo e la selezione del traffico di rete (traffic filtering, firewalling, etc.) previo accordo con il Responsabile della Sicurezza Informatica e il CSI.
Nel caso in cui l'amministrazione dei server venga effettuata anche da remoto, la comunicazione tra il client e il server dovrà avvenire in maniera cifrata, il server dovrà essere configurato in modo da non accettare chiamate dirette all'utente superuser e le chiamate dovranno essere limitate ad un gruppo identificato di indirizzi IP sorgenti.

8.2. Continuità del Servizio e Disaster Recovery

In caso di interruzioni dei servizi causate da guasti hardware o software, gli amministratori di sistema dovranno adoperarsi per ripristinare nel più breve tempo possibile i servizi stessi.
A tale scopo, essi dovranno dotarsi preventivamente di parti di ricambio o sistemi alternativi per far fronte alle emergenze con mezzi propri nei tempi stabiliti.
In alternativa è possibile stipulare contratti di manutenzione nei quali siano specificati i tempi di intervento

9. Regole per gli sviluppatori di applicazioni

Per tutte le applicazioni e i programmi installati sui sistemi, siano essi shareware, con licenza di pubblico utilizzo, acquistati su licenza o sviluppati ad hoc internamente o da aziende esterne fornitrici di servizi, è necessario:

- che la password di amministrazione sia sempre distinta da quella dell'applicazione;
- che in nessun caso il servizio applicativo acquisisca privilegi di amministratore di sistema;
- evitare password *embedded*, cioè inserite nel corpo del programma. Nel caso in cui tale pratica sia indispensabile, si devono osservare le seguenti regole:
  - l'utente deve essere sempre identificabile: non è consentito effettuare tutte le autenticazioni in automatico ma almeno una password deve essere inserita manualmente dall'utente;
  - le password non possono essere memorizzate in chiaro;
  - le password devono poter essere cambiate: deve esistere una procedura attivabile centralmente che ne permetta la sostituzione senza intervento da parte degli utenti;
  - gli utenti non devono conoscere le password *embedded*;
  - una password *embedded* deve essere relativa ad una sola applicazione, non può coincidere con le password di amministrazione e non deve essere usata per altri scopi;
- che le attività di sviluppo, testing e staging del software avvengano su appositi sistemi diversi da quelli di produzione ma il più possibile allineati.

10. Regole per gli utenti finali

Gli utenti sono tenuti a:

- utilizzare i permessi di accesso esclusivamente per le finalità previste;
- non cedere la propria coppia userid-password a terzi;
- non lasciare in vista note o appunti che riportano userid e password;
- effettuare il logout dalle applicazioni e/o dal sistema oppure bloccare la workstation o attivare lo screen-saver con password in caso di allontanamento dalla stazione di lavoro;
- adottare password con il seguente criterio di conformità:
  - Non devono contenere parti significative del nome di account o del nome dell'utente
  - Devono essere composte almeno da 8 caratteri
  - Devono contenere caratteri appartenenti a tre delle quattro categorie seguenti:
    - Lettere maiuscole (dalla A alla Z)
    - Lettere minuscole (dalla a alla z)
    - I primi 10 numeri di base (da 0 a 9)

- Caratteri non alfabetici (ad esempio, !, $, #, %)

- sostituire periodicamente le password personali senza riutilizzare quelle già adottate in passato.

11. Sanzioni

A fronte di violazioni accertate delle regole stabilite dal presente regolamento, al fine di evitare ripercussioni sulla Rete Telematica e sui servizi, i responsabili delle Unità Operative del Centro Servizi Informatici, competenti nella materia, possono disporre la sospensione temporanea delle credenziali di identità digitale che consentono la fruizione dei servizi di Ateneo. Detta sospensione deve essere comunicata immediatamente all'interessato e al Gruppo Sicurezza ICT (art. 4.2 del Regolamento per la Sicurezza dei servizi ICT dell'Università degli Studi di Bari Aldo Moro).

Il CSI può disattivare in qualsiasi momento un codice d'accesso personale e/o una password, apparati ritenuti non conformi o pericolosi ai fini della sicurezza, disconnettere un host dalla rete, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento della Rete Telematica di Ateneo, oppure qualora vi sia evidenza che l'utente abbia violato il presente Regolamento.

Il CSI si riserva la possibilità di erogare assistenza in caso di violazione del presente regolamento, ferma restando la segnalazione agli Organi competenti di Ateneo, e le eventuali applicazioni di sanzioni disciplinari, civili per danni e penali.

12. Disciplina di modifica del presente regolamento

Il presente regolamento è approvato dal Consiglio di Amministrazione previo parere del Senato Accademico, su proposta del Comitato Tecnico Scientifico del CSI, viene emanato con Decreto del Rettore ed entra in vigore il giorno successivo alla pubblicazione sul sito web istituzionale.
Eventuali modifiche e integrazioni al presente regolamento seguiranno la medesima procedura di cui sopra.

Sommario

Bari, 15.11.2017

IL RETTORE
F.to Prof. Antonio Felice Uricchio

ALLEGATO 1

AGENZIA PER L'ITALIA DIGITALE

CIRCOLARE 18 aprile 2017, n. 2/2017

Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060)

(GU n.103 del 5-5-2017)

Vigente al: 5-5-2017

Premessa.

L'art. 14-bis del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera a), tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonche' di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica.

La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovra' rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia e' parte.

La presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella Gazzetta Ufficiale n. 79 del 4 aprile 2017).

Art. 1

Scopo

Obiettivo della presente circolare e' indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce piu' comuni e frequenti cui sono soggetti i loro sistemi informativi.

Le misure minime di cui al comma precedente sono contenute nell'allegato 1, che costituisce parte integrante della presente circolare.

Art. 2

Amministrazioni destinatarie

Destinatari della presente circolare sono i soggetti di cui all'art. 2, comma 2 del C.A.D.

Art. 3

Attuazione delle misure minime

Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato, ha la responsabilita' della attuazione delle misure minime di cui all'art. 1.

Art. 4

Modulo di implementazione delle MMS-PA

Le modalita' con cui ciascuna misura e' implementata presso l'amministrazione debbono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2, anch'esso parte integrante della presente circolare.

Il modulo di implementazione dovra' essere firmato digitalmente con marcatura temporale dal soggetto di cui all'art. 3 e dal responsabile legale della struttura. Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

Art. 5

Tempi di attuazione

Entro il 31 dicembre 2017 le amministrazioni dovranno attuare gli adempimenti di cui agli articoli precedenti.

Roma, 18 aprile 2017

Il Presidente: Samaritani

Allegato 1

Parte di provvedimento in formato grafico

1. GENERALITA'.

1.1. Scopo.

Il presente documento contiene le misure minime di sicurezza ICT per le pubbliche amministrazioni le quali costituiscono parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni.

Questo documento e' emesso in attuazione della direttiva del Presidente del Consiglio dei ministri 1° agosto 2015 e costituisce un'anticipazione urgente della regolamentazione completa in corso di emanazione, al fine di fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

Parte di provvedimento in formato grafico

2. PREMESSA.

La direttiva del Presidente del Consiglio dei ministri 1° agosto 2015, in considerazione dell'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacita' di risposta delle singole amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici a carico della pubblica amministrazione, sollecita tutte le amministrazioni e gli organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi, secondo una tempistica definita e comunque nel piu' breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici. A fine di agevolare tale processo l'Agenzia per l'Italia digitale e' stata impegnata a rendere prontamente disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia e' parte.

L'Agenzia e' costantemente impegnata nell'aggiornamento continuo della normativa tecnica relativa alla sicurezza informatica della pubblica amministrazione ed in particolare delle regole tecniche per la sicurezza informatica delle pubbliche amministrazioni la cui emanazione e' pero' di competenza del Dipartimento per la funzione pubblica e richiede l'espletamento delle procedure previste dalla normativa comunitaria per la regolamentazione tecnica. Pertanto il presente documento, che contiene le misure minime di sicurezza ICT per le pubbliche amministrazioni e costituisce parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni, viene pubblicato, in attuazione della direttiva sopra citata, come anticipazione urgente della regolamentazione in corso di emanazione, al fine di fornire un riferimento utile a stabilire se il livello di protezione offerto da un'infrastruttura risponde alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

La scelta di prendere le mosse dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» nella versione 6.0 di ottobre 2015, trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, dal fatto che esso nasce con una particolare sensibilita' per i costi di vario genere che l'implementazione di una misura di sicurezza richiede, ed i benefici che per contro e' in grado di offrire. L'elenco dei venti controlli in cui esso si articola, normalmente riferiti come Critical Security Control (CSC), e' ordinato sulla base dell'impatto sulla sicurezza dei sistemi; per cui ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua. E' comune convinzione che i primi cinque controlli siano quelli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni e da questi si e' partiti per stabilire le misure minime di sicurezza per la pubblica amministrazione italiana, avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le oltre ventimila amministrazioni pubbliche.

In realta' nel definire gli AgID Basic Security Control(s) (ABSC) si e' partiti dal confronto tra le versioni 6.0 e 5.1 dei CCSC, che puo' essere assunto quale indicatore dell'evoluzione della minaccia

cibernetica nel corso degli ultimi anni. E' infatti evidente l'aumento di importanza delle misure relative agli amministratori di sistema, che balzano dal 12° al 5° posto, entrando nella rosa dei Quick Win, mentre la sicurezza applicativa scivola dal 6° al 18° posto e gli accessi wireless dal 7° al 15° a causa della diffusione delle contromisure atte a contrastare le vulnerabilita' tipiche di tali ambiti.

In definitiva, anche per facilitare il confronto con la definizione originale, si e' deciso di fare riferimento, nell'identificazione degli ABSC, alla versione 6 dei CCSC. Tuttavia l'insieme dei controlli definiti e' piu' vicino a quello della versione 5.1 poiche' si e' ritenuto che molti di quelli che nel passaggio alla nuova versione sono stati eliminati, probabilmente perche' non piu' attuali nella realta' statunitense, siano ancora importanti nel contesto della pubblica amministrazione italiana.

Occorre inoltre osservare che il CCSC e' stato concepito essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, ragione per la quale non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualita' quali guasti ed eventi naturali. Per questa ragione, ai controlli delle prime cinque classi si e' deciso di aggiungere quelli della CSC8, relativa alle difese contro i malware, della CSC10, relativa alle copie di sicurezza, unico strumento in grado di proteggere sempre e comunque le informazioni dal rischio di perdita, e della CSC13, riferita alla protezione dei dati rilevanti contro i rischi di esfiltrazione.

In realta' ciascun CSC e' costituito da una famiglia di misure di dettaglio piu' fine, che possono essere adottate in modo indipendente, consentendo un'ulteriore modulazione utile ad adattare il sistema di sicurezza alla effettiva realta' locale. Nonostante cio' si e' ritenuto che anche al secondo livello ci fosse una granularita' ancora eccessiva, soprattutto sotto il profilo implementativo, che avrebbe costretto soprattutto le piccole amministrazioni ad introdurre misure esagerate per la propria organizzazione. Per tale ragione e' stato introdotto un ulteriore terzo livello, nel quale la misura di secondo livello viene decomposta in misure elementari, ancora una volta implementabili in modo indipendente. Pertanto un ABSC e' identificato da un identificatore gerarchico a tre livelli x, y, z, dove x e y sono i numeri che identificano il CSC concettualmente corrispondente e z individua ciascuno dei controlli di livello 3 in cui questo e' stato raffinato.

Al primo livello, che corrisponde ad una famiglia di controlli destinati al perseguimento del medesimo obiettivo, e' associata una tabella che li contiene tutti. Nella prima colonna, sviluppata gerarchicamente su tre livelli, viene definito l'identificatore univoco di ciascuno di essi. La successiva colonna «Descrizione» specifica il controllo attraverso una definizione sintetica.

Nella terza colonna, «FNSC» (Framework nazionale di sicurezza cibernetica), viene indicato l'identificatore della Subcategory del Framework Core del Framework nazionale per la Cyber Security, proposto con il 2015 Italian Cyber Security Report del CIS «La Sapienza» presentato lo scorso 4 febbraio 2016, al quale il controllo e' riconducibile. Pur non intendendo costituire una contestualizzazione del Framework, le misure minime concretizzano praticamente le piu' importanti ed efficaci azioni che questo guida ad intraprendere. Per il diverso contesto di provenienza ed il differente obiettivo che i due strumenti intendono perseguire, le misure minime pongono l'accento sopra gli aspetti di prevenzione piuttosto che su quelli di risposta e ripristino.

Le ultime tre colonne sono booleane e costituiscono una linea guida che indica quali controlli dovrebbero essere implementati per ottenere un determinato livello di sicurezza. La prima, «Minimo», specifica il livello sotto il quale nessuna amministrazione puo' scendere: i controlli in essa indicati debbono riguardarsi come obbligatori. La seconda, «Standard», puo' essere assunta come base di riferimento nella maggior parte dei casi, mentre la terza, «Alto», puo' riguardarsi come un obiettivo a cui tendere.

Il raggiungimento di elevati livelli di sicurezza, quando e' molto elevata la complessita' della struttura e l'eterogeneita' dei servizi erogati, puo' essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto ogni amministrazione dovra' avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneita' di requisiti ed obiettivi di sicurezza, all'interno dei quali potra' applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi.

Le amministrazioni NSC, per l'infrastruttura che gestisce dati NSC, dovrebbero collocarsi almeno a livello "standard" in assenza di requisiti piu' elevati.

3. LA MINACCIA CIBERNETICA PER LA PUBBLICA AMMINISTRAZIONE.

Nel recente passato si e' assistito ad una rapida evoluzione della minaccia cibernetica ed in particolare per quella incombente sulla pubblica amministrazione, che e' divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

Se da un lato la pubblica amministrazione continua ad essere oggetto di attacchi dimostrativi, provenienti da soggetti spinti da motivazioni politiche ed ideologiche, sono divenuti importanti e pericolose le attivita' condotte da gruppi organizzati, non solo di stampo propriamente criminale.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi. Il primo e' la quantita' di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati. Il secondo e' che il primo obiettivo perseguito e' il mascheramento dell'attivita', in modo tale che questa possa procedere senza destare sospetti. La combinazione di questi due fattori fa si' che queste misure minime, pur tenendo nella massima considerazione le difese tradizionali, quali gli antivirus e la difesa perimetrale, pongano l'accento sulle misure rivolte ad assicurare che le attivita' degli utenti rimangano sempre all'interno dei limiti previsti. Infatti elemento comune e caratteristico degli attacchi piu' pericolosi e' l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

Nei fatti le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario e' avvenuto e quello in cui le conseguenze vengono scoperte. Oltre tutto una lunga latenza della compromissione rende estremamente complessa, per la mancanza di log, modifiche di configurazione e anche avvicendamenti del personale, l'individuazione dell'attacco primario, impedendo l'attivazione di strumenti efficaci di prevenzione che possano sicuramente impedire il ripetersi degli eventi.

In questo quadro diviene fondamentale la rilevazione delle anomalie operative e cio' rende conto dell'importanza data agli inventari, che costituiscono le prime due classi di misure, nonche' la protezione della configurazione, che e' quella immediatamente successiva.

La quarta classe deve la sua priorita' alla duplice rilevanza dell'analisi delle vulnerabilita'. In primo luogo le vulnerabilita' sono l'elemento essenziale per la scalata ai privilegi che e' condizione determinante per il successo dell'attacco; pertanto la loro eliminazione e' la misura di prevenzione piu' efficace. Secondariamente si deve considerare che l'analisi dei sistemi e' il momento in cui e' piu' facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso.

La quinta classe e' rivolta alla gestione degli utenti, in particolare gli amministratori. La sua rilevanza e' dimostrata dall'ascesa, accennata in premessa, dal 12° al 5° posto nelle SANS 20, motivata dalle considerazioni cui si e' fatto riferimento poco dianzi.

La sesta classe deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase l'installazione di codice malevolo e la sua individuazione puo' impedirne il successo o rilevarne la presenza.

Le copie di sicurezza, settima classe, sono alla fine dei conti l'unico strumento che garantisce il ripristino dopo un incidente.

L'ultima classe, la protezione dei dati, deve la sua presenza alla considerazione che l'obiettivo principale degli attacchi piu' gravi e' la sottrazione di informazioni.

Parte di provvedimento in formato grafico

Allegato 2

Parte di provvedimento in formato grafico