CORSI SECURITY MANAGEMENT A.A. 2020/2021

CORSO DI PERFEZIONAMENTO E FORMAZIONE IN «SECURITY MANAGEMENT»

14 gennaio 2022

ALESSANDRO MANFREDINI

Sistemi di Gestione della Security Aziendale

Modello di Organizzazione e Gestione ai sensi del D.Lgs 231/2001, allocazione di responsabilità.

Principali aspetti manageriali collegati ai sistemi standardizzati OHSAS 18001:2007, ai sistemi di gestione della cultura e della leadership e ai sistemi di gestione dei comportamenti aziendali (BBS) e cenni ai sistemi di gestione integrati safety e security previsti per le infrastrutture critiche.

I trend internazionali ed europei collegati alla responsabilità sociale e allo sviluppo sostenibile di un'organizzazione

dott. Alessandro Manfredini

Direttore Group Security & Cyber Defence – Gruppo A2A

Vicepresidente – AIPSA *Associazione Italiana Professionisti Security Aziendale*

alessandro.manfredini@a2a.eu

Introduzione

- Per affrontare le tematiche di security occorre organizzare le proprie attività in modo sistematico e con “metodo” non è più concepibile, né tanto meno conveniente (anche dal punto di vista economico) improvvisare azioni che a lungo andare potrebbero addirittura dimostrarsi in contrasto fra di loro.

- Occorre aver progettato un Sistema di Gestione della Security che si fondi su criteri di pianificazione, azione, controllo, revisione e miglioramento anche per le risorse economiche messe in campo.

La security secondo la norma UNI 10459:2017

La security è:

Attività volta a prevenire, fronteggiare e superare gli eventi che possono verificarsi a seguito di azioni in prevalenza illecite e che espongono le **persone** e i **beni (materiali e immateriali)** dell'Organizzazione a potenziali effetti lesivi e/o dannosi

Nota Nell'accezione della Norma per azione illecita si intende non solo un comportamento antigiuridico (doloso e/o colposo), ma anche qualsiasi attività operata in contrasto con le procedure interne all'Organizzazione

CeSIntES

Security

Salute e Sicurezza nei luoghi di lavoro

Direttiva NIS Perimetro Sicurezza Nazionale Cibernetica

Privacy

Responsabilità degli enti

Qualità

COMPANY WITH INFORMATION SECURITY MANAGEMENT SYSTEM CERTIFIED BY DNV =ISO / IEC 27001:2005=

UNI 10459:2017

D.Lgs. 81/08

Normativa tecnica

GDPR

D.Lgs. 231/01

ISO 9000

Modello Organizzativo Sicurezza Aziendale Integrata

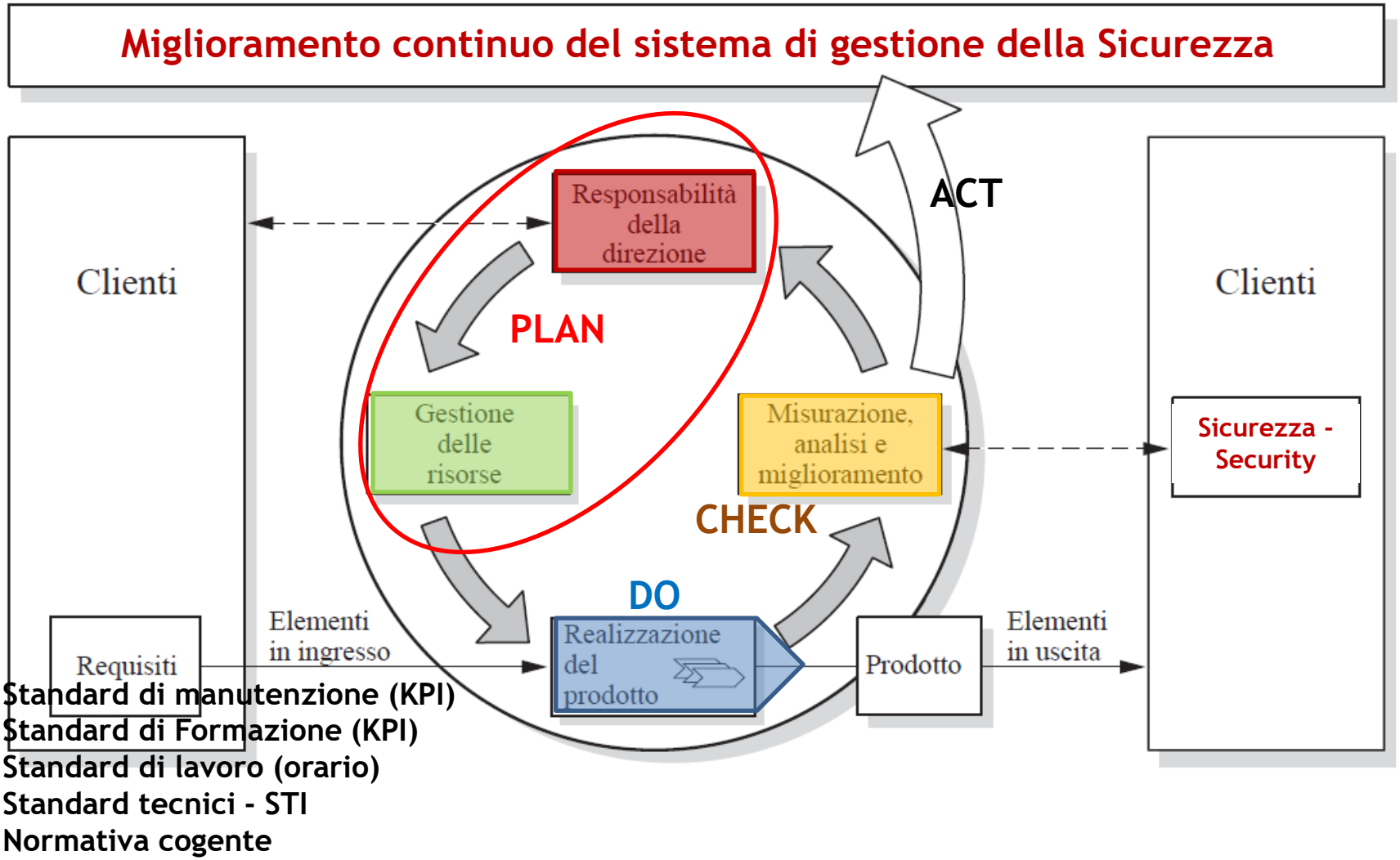
M.O.S.A.I.

La sicurezza come risultato di un GIOCO di SQUADRA

La “Sicurezza non è un prodotto, ma un **processo**”
(Bruce Schneier)

Il miglioramento continuo: il «modello»

- Il modello che si fonda sugli standard di qualità ISO 9001 raccomanda di seguire il classico Ciclo di Deming (PDCA).
  - ❑ Plan
    - ✓ Pianifico le esigenze
  - ❑ Do
    - ✓ Implemento le scelte fatte
  - ❑ Check
    - ✓ Verifico che le soluzioni implementate siano coerenti con quanto pianificato
  - ❑ Act
    - ✓ Attuo i miglioramenti necessari per raggiungere gli obiettivi



Ciclo di Deming – ISO 9001:2015

Sistema di Gestione della Security Aziendale


PRESIDENZA DEL CONSIGLIO DEI MINISTRI
SISTEMA DI INFORMAZIONE
PER LA SICUREZZA DELLA REPUBBLICA
ARCHITETTURA NAZIONALE DI CYBER RESILIENCE
1

TRASFORMAZIONE DIGITALE

Sistema di informazione per la sicurezza della Repubblica

FUNZIONI E SERVIZI ESSENZIALI DELLO STATO ORMAI DIGITALIZZATI

Governativo · Telecomunicazioni · Energia · Finanza · Previdenza · Difesa · Spazio · Tecnologie · Trasporti · Interno

	Governativo	Telecomunicazioni	Energia	Finanza	Previdenza	Difesa	Spazio	Tecnologie	Trasporti	Interno
esempi	Gestione debito pubblico	Gestione servizi comunicazione	Produzione	Mercato finanziario	Gestione cassa integrazione	Sviluppo nuovi mezzi	Controllo orbitale	Sicurezza biologica e nucleare	Gestione traffico ferroviario	Gestione Schengen
	Bilancio dello stato	IdIXP, PEC e entità	Distribuzione	Servizi pagamento	Gestione pensioni	Manutenzione sistemi	Controllo lancio	AI, HPC e Cybersecurity	Assistenza al volo	Sistema AFIS

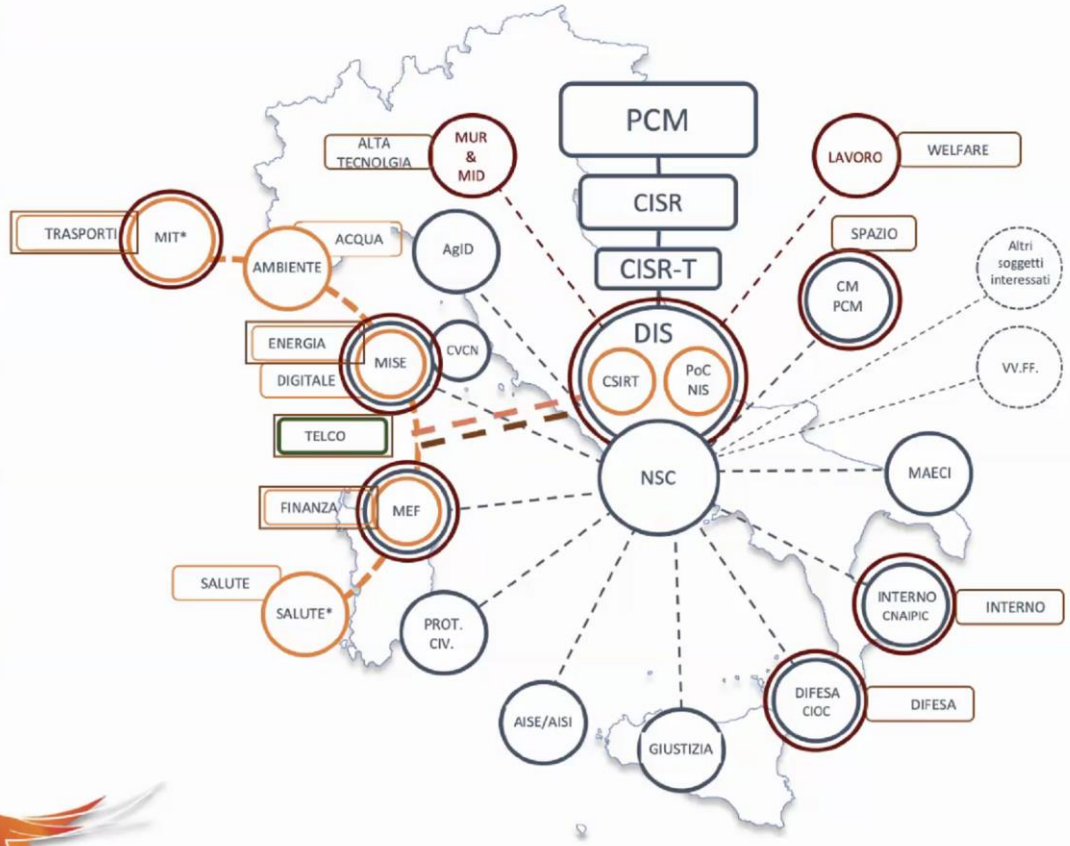
Attacchi cyber alle funzioni e ai servizi essenziali dello Stato

PREGIUDIZIO ALLA SICUREZZA NAZIONALE

in termini di interessi politici, militari, economici, scientifici e industriali

ARCHITETTURA NAZIONALE DI CYBER RESILIENCE

Sistema di informazione per la sicurezza della Repubblica



Architettura nazionale cyber (DPCM 17.2.2017)

- NSC composizione ordinaria
- NSC composizione in caso di crisi
- Collaborazione funzionale

Direttiva NIS (D.L.vo 65/2018)

Orientata alla disponibilità dei servizi

- Attori NIS
- Comitato tecnico di raccordo
- OSE Operatori di Servizi Essenziali
- FSD Fornitori di Servizi Digitali
- * più regioni e province autonome di Trento e Bolzano

Decreto «Telco» 12.12.2018

Decreto CSIRT (DPCM 8 agosto 2019)

L 133/2019 perimetro di sicurezza nazionale cibernetica

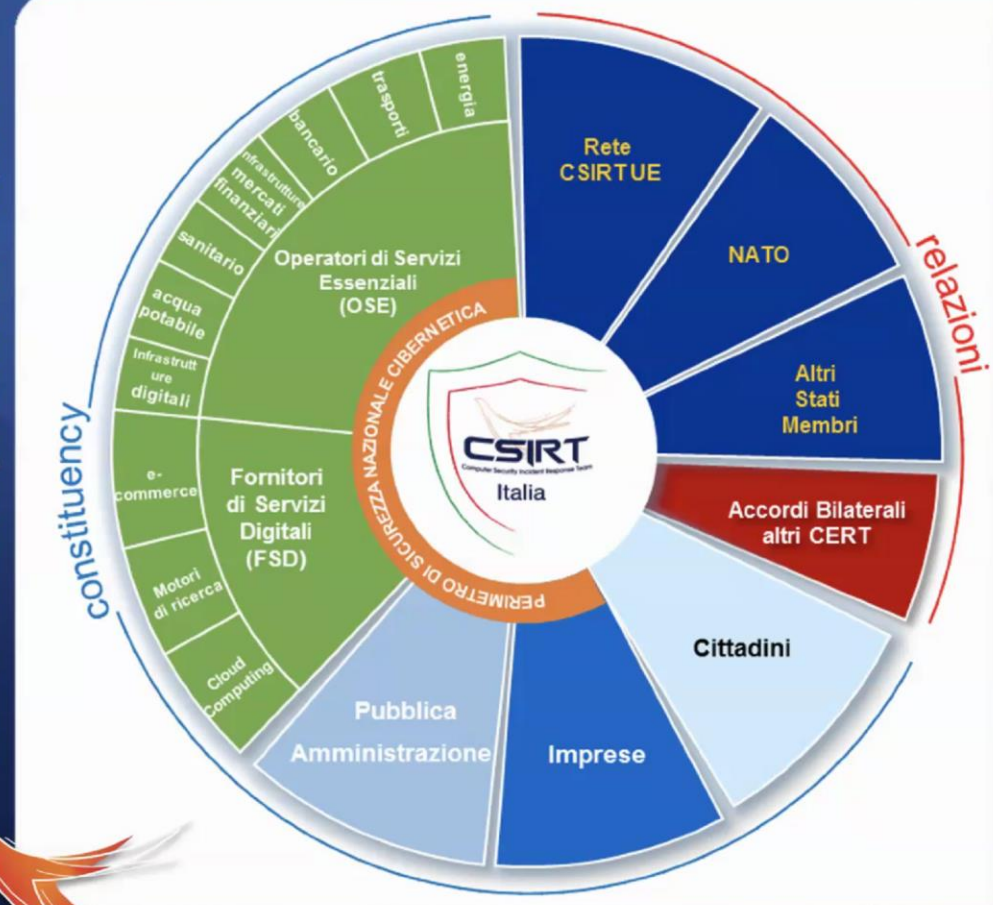
Orientata alla disponibilità, confidenzialità e integrità degli asset ICT selezionati

- Misure di sicurezza cyber (Sistema Ispezioni)
- Notifiche di incidenti (Sistema CSIRT)
- Procurement ICT sicuro (Sistema CVCN)

per amministrazioni pubbliche, enti e operatori nazionali, pubblici e privati che esercitano funzioni o servizi essenziali dello Stato

CONSTITUENCY DELLO CSIRT ITALIANO

Sistema di informazione per la sicurezza della Repubblica



PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

A CHI SI APPLICA → **Amministrazioni pubbliche**, **enti** e **operatori** nazionali, **pubblici** e **privati** che esercitano **funzioni/servizi essenziali dello Stato**

A COSA SI APPLICA → **Asset ICT** dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un **pregiudizio per la sicurezza nazionale**

COSA PREVEDE

Prevenzione di attacchi

- **Misure di sicurezza**
- Meccanismo per **procurement più sicuro (CVCN)**
- **Vigilanza** e **controllo + sanzioni**

Risposta ad attacchi

- **Notifica** di **incidenti obbligatoria e "tempestiva"**
- **Disattivazione apparati** o **prodotti** → **Rischio grave** e **imminente** per la sicurezza nazionale

ACCORDI SPECIFICI DI COLLABORAZIONE CON GLI ORGANI COSTITUZIONALI

«Gli Organi costituzionali, ove intendano adottare, per le proprie reti e i propri sistemi informativi e servizi informatici, misure di sicurezza analoghe a quelle previste dal decreto–legge, possono concludere per tali finalità appositi accordi con il Presidente del Consiglio dei Ministri» (Art. 2, comma 2, DPCM adottato ai sensi dell'art. 1, comma 2 del D.L. n. 105/2019)

Parte I
SGSeA
(alcuni esempi)

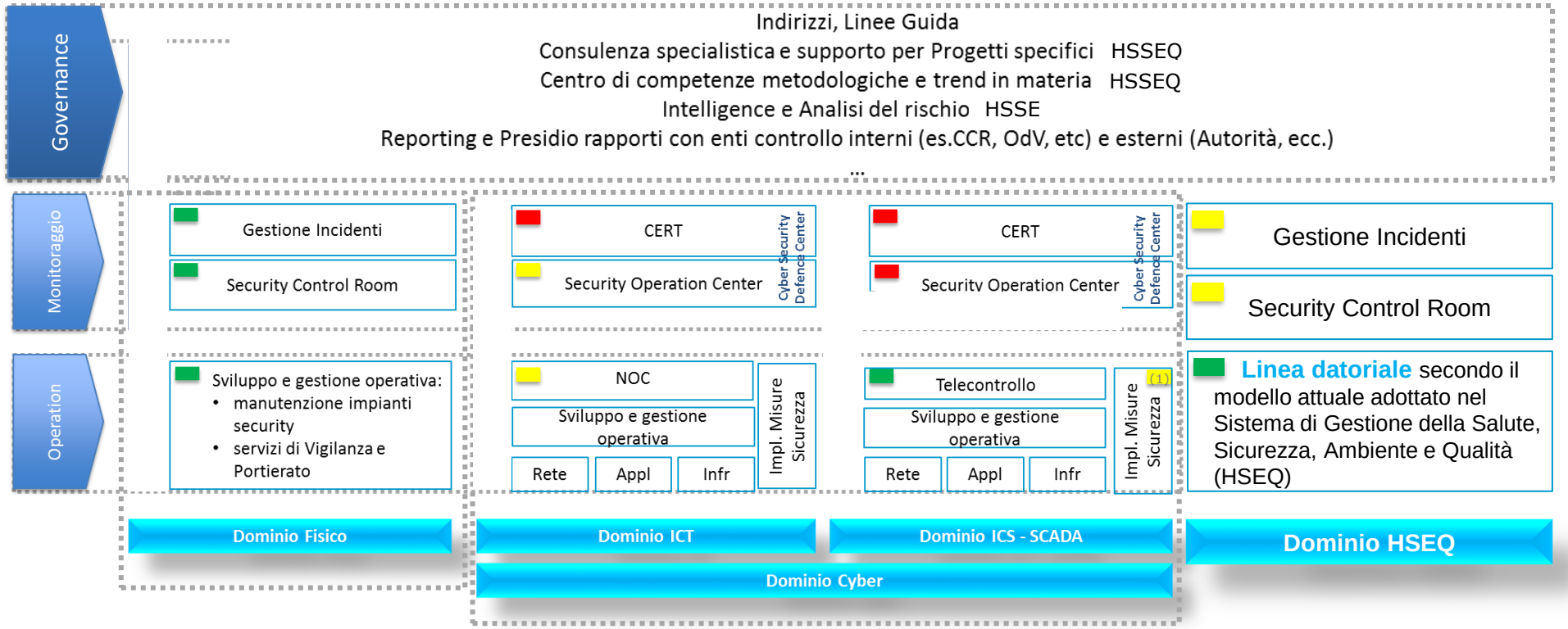
Framework Sicurezza

CeSIntES

Esempio di modello di gestione integrata HSSEQ

Health Safety Security Environment Quality

- **Valorizzazione** di un unico centro di competenza/governance in materie affini quali Salute, Sicurezza dei lavoratori, Security
- **Presidio unico** dei Sistemi di Gestione Aziendali (Safety, Security, Ambiente e Qualità)
- **Monitoraggio integrato** (audit tecnici) e gestione degli **incidenti** centralizzata
- **Reporting periodico** verso soggetti interessati
- **Sensibilizzazione** del business sui temi normativi di competenza



	SCOPO	
ORGANIGRAMMA	Sistema di Gestione della Sicurezza	PROGETTAZIONE NUOVI SERVIZI
RUOLI E RESPONSABILITA'	POLITICA DELLA SICUREZZA	VALUTAZIONE DEI RISCHI
REQUISITI PROFESSIONALI	PIANO INDICATORI	GESTIONE DOCUMENTALE
COINVOLGIMENTO RISORSE	PIANO ANNUALE SICUREZZA	GESTIONE PIANO SICUREZZA
REVISIONI	OBIETTIVI INIZIATIVE	
ACRONIMI	PIANO ANNUALE DI AUDIT	
DOCUMENTI DI RIFERIMENTO	PIANO ANNUALE FORMAZIONE	

Linea Guida

MANUALE DEL SISTEMA DI GESTIONE DELLA SECURITY AZIENDALE

	Elaborata da	Verificata da	Approvata da
Data			
Firma			

Data di entrata in vigore	01-III-2012

5.1 I PROCESSI DEL SGSeA

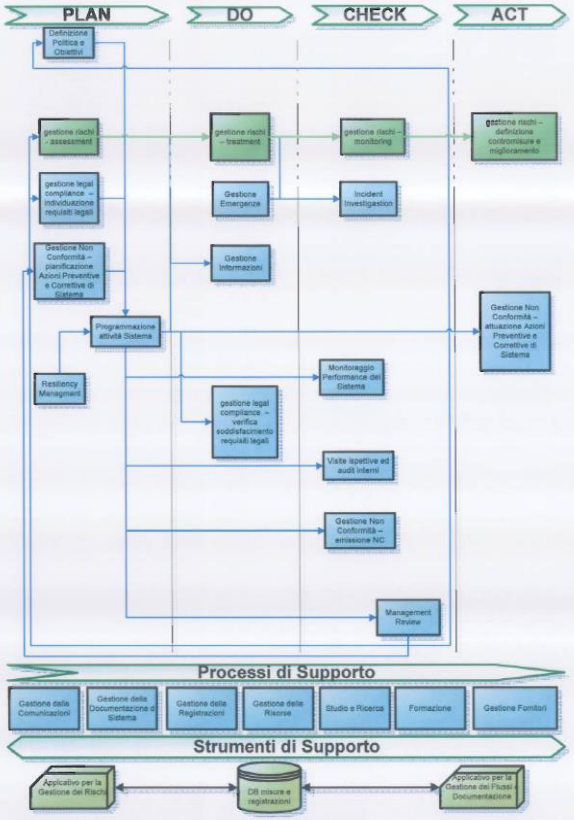


Figura 1: Processi del SGSeA

5.2 STRUTTURA DELLA DOCUMENTAZIONE DEL SGSeA

Al fine di garantire all'interno dei propri processi il rispetto di quanto riportato nel presente Manuale ha impostato tutta la documentazione a supporto del SGSeA come illustrato nella seguente figura:

Figura 2: Gerarchia della documentazione

- 1° livello è rappresentato dai documenti di rango Linea Guida e comprende:
  - Carta dei Valori;
  - Politica generale per la gestione della security aziendale (collegata al presente Manuale);
  - Politica generale per la gestione della sicurezza delle informazioni (collegata al presente Manuale);
  - Norme comportamentali per la gestione sicura delle risorse aziendali (collegata al presente Manuale).
- 2° livello è rappresentato dalle Procedure Aziendali.
- 3° livello è rappresentato dalle Procedure Operative.

6 MATRICE DEI CONTROLLI E SEGREGATION OF DUTIES

Matrice dei Controlli

Descrizione dei controlli indicati nel documento	Tipologia del controllo	Frequenza del controllo
(1) Riesame sistema	Manuale	Cambiamento organizzativo
(2) Riesame Politica	Manuale	Annuale
(3) Diffusione politica	Manuale	Ad hoc
(4) Diffusione Carta Valori	Manuale	Ad hoc
(5) Piano della Sicurezza	Manuale	Annuale
(6) Avanzamento Piano	Manuale	quadrimestrale

Matrice della Segregation of duties

Descrizione dei controlli indicati nel documento	Soggetto che svolge l'attività	Soggetto che verifica	Soggetto che approva
(1)	RSGSeA	RSIGE	Vertice aziendale
(2)	RSGSeA	RSIGE	Vertice aziendale
(3)	SIGE	RSGSeA	N.A.
(4)	PERS	RSIGE	N.A.
(5)	RSGSeA	RSIGE	Vertice aziendale
(6)	SIGE	RSGSeA	RSIGE

10 APPENDICE A

Elenco Linee Guida SGSeA

Codice	Titolo
Linea Guida SIGE 01	Manuale del Sistema di Gestione della Security Aziendale (presente documento)
Linea Guida SIGE 02	Politica Generale per la Gestione della Sicurezza delle Informazioni
Linea Guida SIGE 03	Norme Comportamentali per la Gestione Sicura delle Risorse Aziendali
Linea Guida SIGE 04	Politica per la Gestione della Security Aziendale

Elenco Procedure Aziendali

Codice	Titolo
PA SIGE 01	Gestione della Sicurezza delle Informazioni nei Rapporti con le Terze Parti
PA SIGE 02	Principi per la Classificazione e Gestione delle Informazioni
PA SIGE 03	Principi per la Classificazione e Gestione degli Asset
PA SIGE 04	Gestione della Compliance
PA SIGE 05	Gestione della Sicurezza delle Informazioni nei Rapporti con il Personale
PA SIGE 06	Gestione delle verifiche da parte dell'Internal Audit in ambito Sicurezza delle Informazioni
PA SIGE 07	Gestione della Sicurezza Fisica
PA SIGE 08	Monitoraggio, Tracciamento e Verifiche Tecniche
PA SIGE 09	Gestione Sicura degli Accessi Logici
PA SIGE 10	Ciclo di Vita dei Sistemi e dei Servizi
PA SIGE 11	Gestione e Manutenzione delle Reti
PA SIGE 12	Principi di Controllo Contro il Malware
PA SIGE 13	Principi per la Gestione del Back-Up e Restore
PA SIGE 14	Principi per la Gestione dei Log
PA SIGE 15	Cifratura e Controlli Crittografici
PA SIGE 16	Gestione degli Eventi Anomali e degli Incidenti

Elenco Istruzioni Operative

Codice	Titolo
PO SIGE 01	Regolamento Operativo di Gestione per gli Adempimenti Privacy
PO SIGE 02	Procedura di Gestione degli Accessi da Remoto
PO SIGE 03	Procedura per la Gestione degli Accessi Fisici
PO SIGE 04	Procedura per la Conduzione delle Verifiche Interne

Qualità e Ambiente

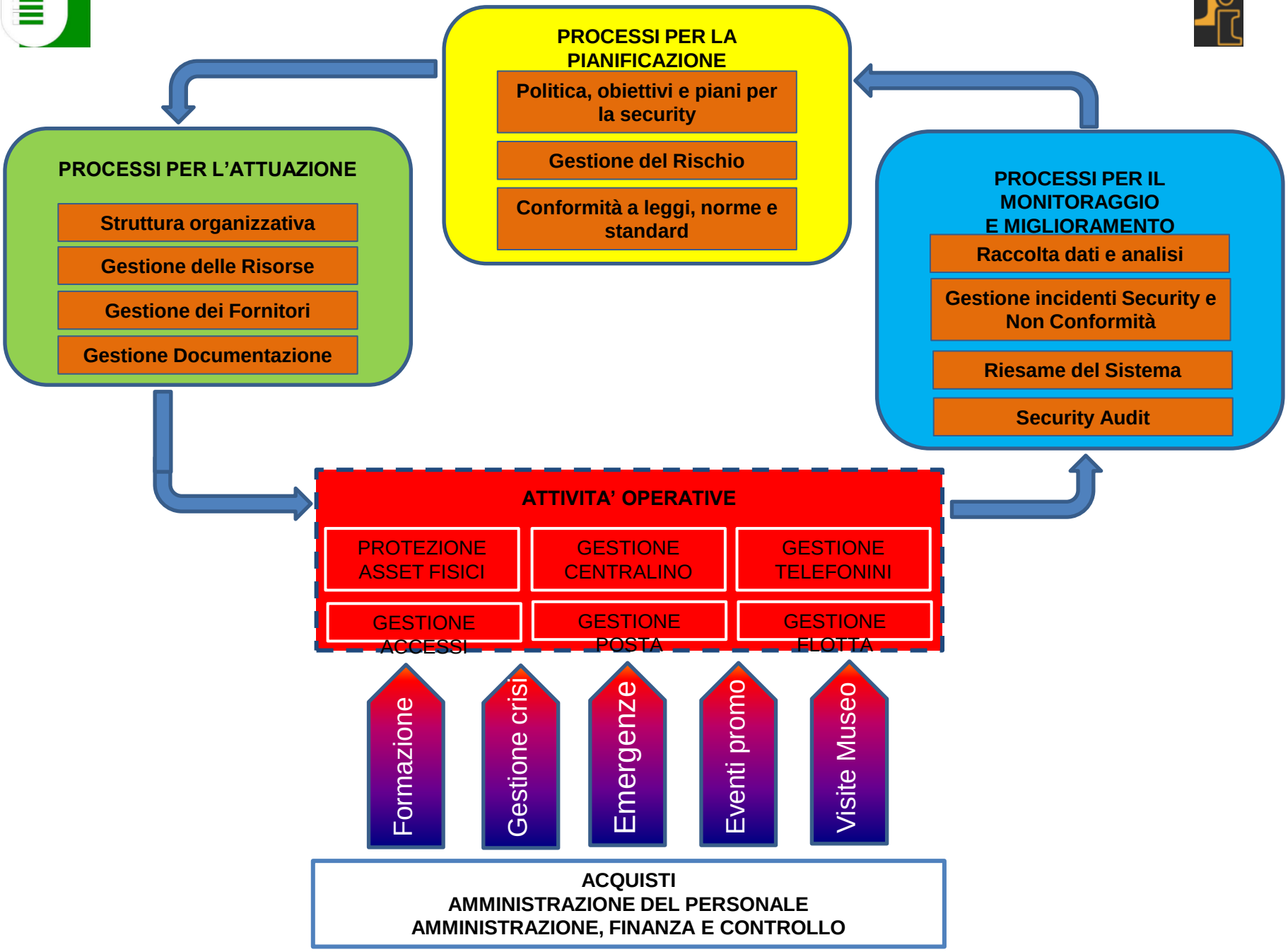
«Sistema di Gestione della Qualità e Ambiente»

La Società ha adottato un sistema di gestione della qualità conforme alla norma UNI EN ISO 9001:2008 e un sistema di gestione ambientale conforme allo standard ISO 14001:2004. Tali sistemi, entrambi certificati, contribuiscono a dare chiara evidenza ai **processi aziendali interessati** e a portare, anche attraverso gli audit e i controlli eseguiti con frequenza programmata, una **maggiore attenzione sul Modello Organizzativo ex D.Lgs. 231/2001** rispetto delle procedure e istruzioni relative. La **certificazione**, inoltre, permette la costante valutazione dello stato di applicazione e dell'efficacia del sistema procedurale, integrandosi quindi nel più ampio quadro dei controlli di cui al Decreto 231/2001.

Security Aziendale

Misure tecniche, organizzative e procedurali volte a tutelare la sicurezza delle informazioni, delle risorse informatiche e delle risorse umane e materiali aziendali. Tale ambito è anche regolamentato dal D.Lgs. 231/2001 s.m.i., D.Lgs. 196/2003 s.m.i., dai Provvedimenti del Garante della Privacy, dagli Standard ISO/IEC 27001:2005, ISO 28001 e C-TPAT.

CORSI SECURITY MANAGEMENT A.A. 2020/2021



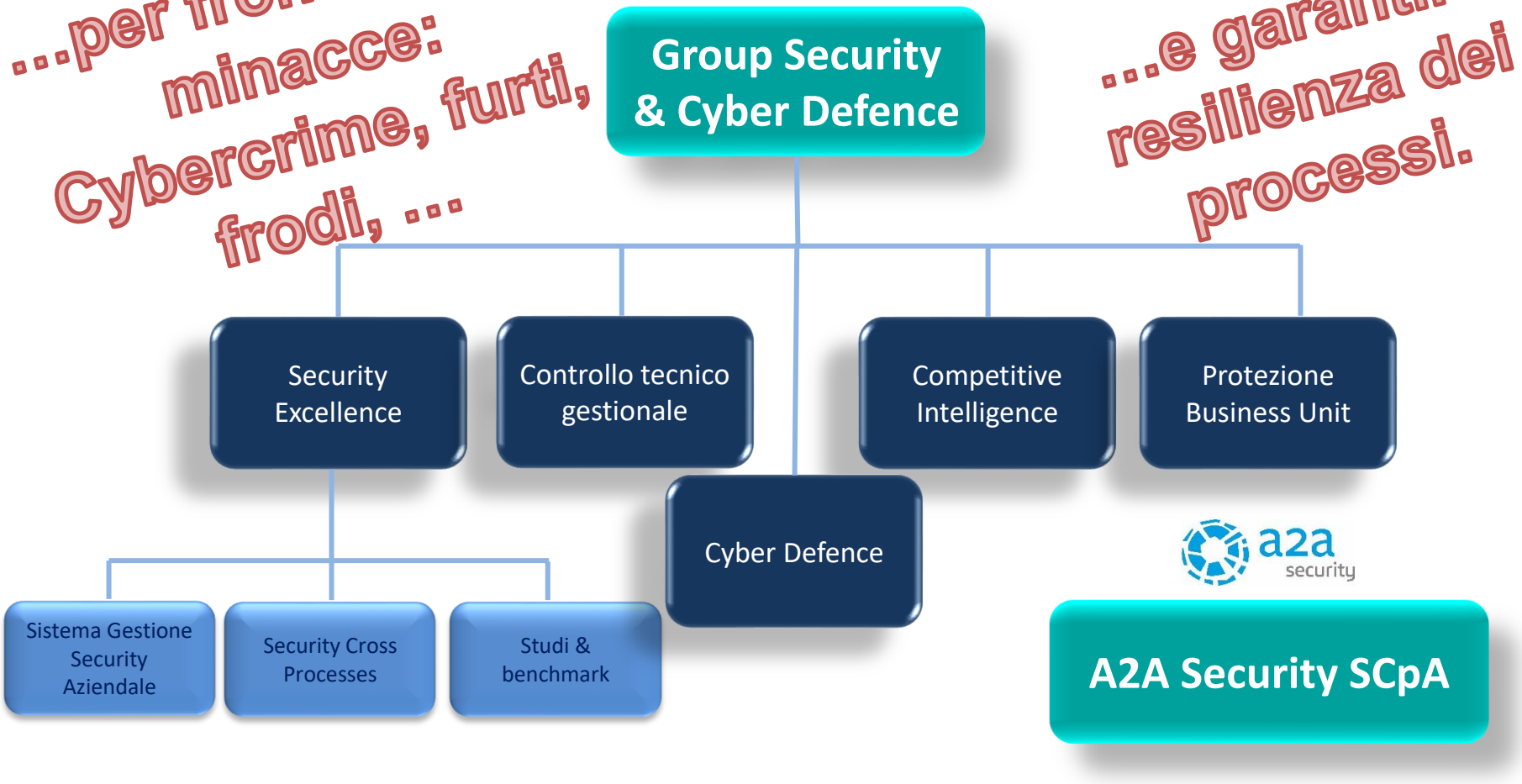
Descrizione delle fasi del processo

FASI	DESCRIZIONE
1 PLAN	Stabilire gli obiettivi del Sistema e i suoi processi, le risorse necessarie per fornire risultati conformi ai requisiti e alle politiche dell'organizzazione, indentificare e affrontare i rischi e le opportunità. Nel PLAN sono incluse, ad esempio, tutte le attività che identificano e definiscono i concetti base e la relativa terminologia, la normativa di settore, le metodologie di riferimento anche per quanto concerne la classificazione dei beni aziendali, l'individuazione di funzioni, ruoli e responsabilità, la previsione, stesura e revisione di procedure di sicurezza.
2 DO	Attuazione del PLAN
3 CHECK	Monitorare e, quando applicabile, misurare i processi, i prodotti e servizi risultanti a fronte delle politiche, degli obiettivi, dei requisiti e delle attività pianificate, e riferite ai risultati. In sostanza, per il controllo e la verifica del Sistema è necessario i) eseguire il monitoraggio continuo del sistema, sulla base delle procedure di misurazione e reporting definite, ii) eseguire periodicamente verifiche di autocontrollo (self-assessment), verifiche interne e audit esterni, iii) eseguire periodicamente o in presenza di cambiamenti significativi di contesto, la revisione dell'analisi del rischio
4 ACT	Intraprendere azioni al fine di individuare i miglioramenti (azioni correttive) da apportare al Sistema in funzione delle attività di verifica.

Organizzazione della Security

...per fronteggiare minacce: Cybercrime, furti, frodi, ...

...e garantire resilienza dei processi.



A2A Security Società Consortile per Azioni

Data di costituzione: *01 Ottobre 2017*

FINALITÀ

Garantire l'espletamento dei vari servizi di vigilanza svolti a beneficio dei beni mobili e immobili di proprietà delle Società consorziate, ai sensi dell'art. 133 co.2 **Testo Unico Leggi Pubblica Sicurezza** e del **D.M. 269/2010** emendato con il D.M. 56/2015 "Disciplina delle caratteristiche minime del progetto organizzativo e dei requisiti minimi di qualità degli istituti di vigilanza».
A tale scopo, la Security Control Room, sorta dall'unificazione delle sale controllo di Milano (A2A e AMSA) e di Brescia (A2A) eroga i servizi di:

- monitoraggio e controllo della tutela del patrimonio delle Società consorziate;
- videoronda dei siti collegati;
- gestione allarme e pronto intervento.

I vantaggi derivanti da tale iniziativa sono rappresentati da:

- creazione di un «Sistema di coordinamento/comando/controllo» che consenta una tempestiva, efficace ed efficiente gestione dello stesso;
- armonizzazione delle soluzioni tecnologiche installate a livello di Gruppo;
- presenza di una struttura operativa coerente con le esigenze del Gruppo A2A.

Società consorziate in A2A Security

A2A ENERGIA SPA
A2A ENERGY SOLUTIONS SRL
LD RETI S.R.L.
A2A RECYCLING SRL
A2A SMART CITY SPA
ACSM - AGAM SPA
APRICA SPA
AZIENDA SERVIZI VALTROMPIA SPA
LINEA AMBIENTE SRL
LINEA GREEN SPA
LINEA GROUP HOLDING SPA
LOMELLINA ENERGIA SRL
RETRAGAS SRL
LINEA GESTIONI

Servizi erogati

TELESORVEGLIANZA

Servizio di gestione a distanza di segnali, informazioni o allarmi provenienti ovvero diretti da o verso un obiettivo fermo o in movimento, finalizzato all'intervento diretto della guardia giurata.

TELEVIGILANZA

Servizio di controllo a distanza dei beni mobili o immobili dei soci con l'ausilio di apparecchiature che trasferiscono le immagini, allo scopo di promuovere l'intervento della guardia giurata.

SERVIZIO ISPETTIVO

Servizio di vigilanza ispettiva non programmato svolto dalla guardia giurata a seguito della ricezione di un segnale di allarme, attivato automaticamente ovvero dall'utente titolare del bene mobile o immobile.

CORSI SECURITY MANAGEMENT A.A. 2020/2021

A2A Security – Security Control Room

Attraverso la Security Control Room (SCR) vengono inoltre erogati i seguenti ulteriori **servizi**:

Monitoraggio stato efficienza impianti antintrusione e videosorveglianza

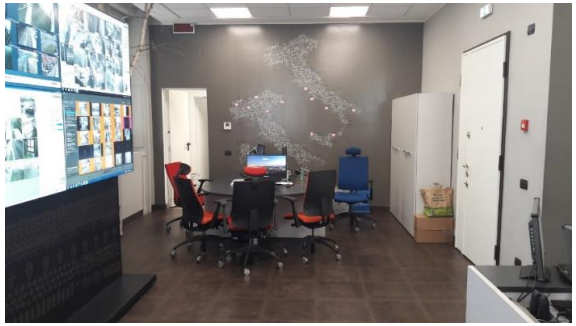
Lo stato di funzionamento degli impianti antintrusione e videosorveglianza viene costantemente monitorato allo scopo di mantenere questi ultimi in perfetto stato di efficienza

Travel Security

- Monitoraggio personale del Gruppo A2A in trasferta lavorativa
- Assistenza in caso di emergenza
- Analisi del Rischio Paese

Security Service Desk

La SCR riceve le segnalazioni di eventi emergenziali che coinvolgano persone e Società del Gruppo A2A, attivando quei flussi informativi per la gestione delle crisi aziendali



Gestione dei segnali di allarme

Tutti gli avvisi di allarme provenienti dagli impianti periferici vengono analizzati allo scopo di discriminare la natura e la causa della segnalazione stessa

Richiesta di intervento su allarme

Qualora la segnalazione di allarme pervenuta alla SCR fosse effettivamente causata da una reale intrusione, gli operatori di SCR richiedono intervento all'istituto di vigilanza, fornitore dei servizi di sicurezza ed eventualmente alle Forze dell'Ordine e di pronto intervento in generale (Vigili del Fuoco, Pronto Soccorso Sanitario, ecc.)

Registrazione delle informazioni

Tutte le azioni svolte dalla SCR vengono registrate in apposite piattaforme informatiche allo scopo di poter essere analizzate e valutate a posteriori

ALCUNI NUMERI

125 siti collegati

1900 telecamere gestite

2700 punti connessi

30000 telefonate annue gestite

2 operatori per turno

1 responsabile Certificato UNI 10459:2017

Tecnologie utilizzate

PSIM

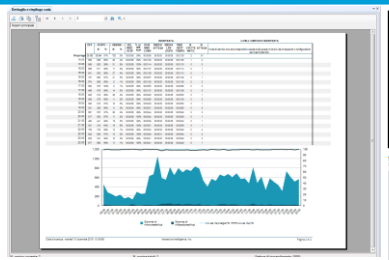
A2A dispone di una piattaforma PSIM (Physical Security Information Management) in grado di aggregare una molteplicità di informazioni provenienti da differenti sistemi di gestione di security. È in fase di realizzazione la migrazione di tutti i sistemi presenti sul sistema PSIM - Physical Security Information Management

VIDEOANALISI

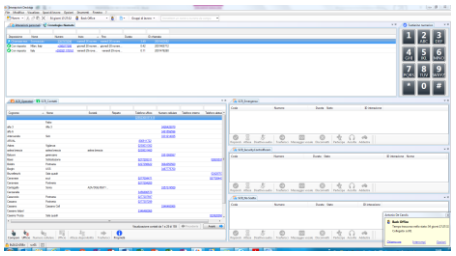
Si utilizzano moderne tecnologie di videoanalisi che associano telecamere ottiche a telecamere termiche in grado di definire "Cross Line" per segnalare eventuali intrusioni.

CENTRALINO IVR (Interactive Voice Response)

Le comunicazioni telefoniche sono gestite da un recente IVR Genesys (Interactive Voice Response) in grado di smistare automaticamente le chiamate in entrata e accompagnare il cliente verso l'operatore in modo più veloce, garantendo standard di qualità molto rigorosi.



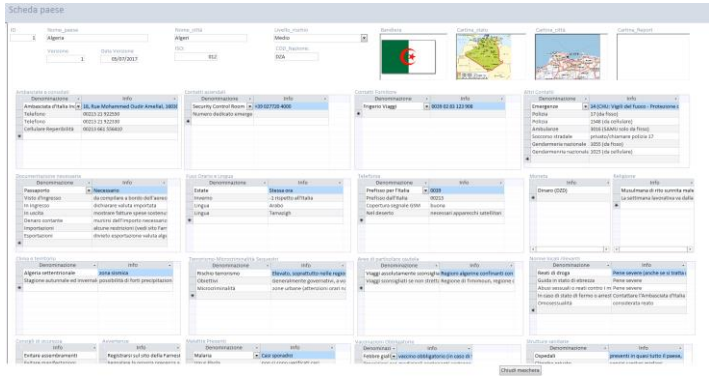
È inoltre possibile monitorare i livelli di servizio attraverso alcuni tool evoluti nell'ottica del miglioramento continuo.



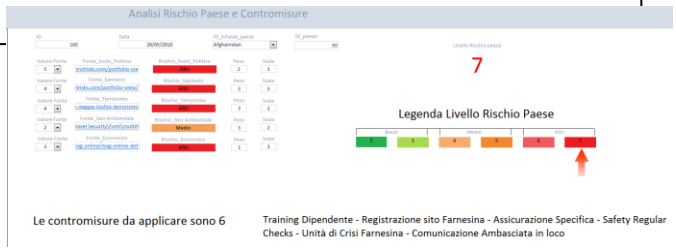
Travel Security

TRAVEL SECURITY

Applicativi di travel security in grado di monitorare la presenza di personale del Gruppo A2A in trasferta lavorativa e in grado di supportare il personale della SCR nella gestione di eventuali emergenze.



Database con cui catalogare tutte le informazioni reperite dalla fonti istituzionali e metterle a disposizione della popolazione aziendale in trasferta.



Avanzate metodologie di valutazione del rischio che permettono di assegnare un livello di rischio per ogni trasferta lavorativa suggerendo quante e quali contromisure adottare.

Offerta servizi

Gestione dei segnali di allarme

- ✓ Vigilare e custodire la proprietà mobiliare e immobiliare aziendale
- ✓ Gestire a distanza segnali, informazioni o allarmi provenienti ovvero diretti da o verso un obiettivo fermo o in movimento, finalizzato all'intervento diretto della guardia giurata
- ✓ Verificare che gli impianti antintrusione, videosorveglianza e controllo accessi siano in stato di efficienza
- ✓ Gestire gli avvisi d'allarme provenienti dagli impianti periferici discriminando la natura della segnalazione
- ✓ Richiedere interventi all'Istituto di Vigilanza fornitore dei servizi di Sicurezza e quello eventuale delle Forze di Polizia o di Pronto Intervento in generale (VV.F., Pronto Soccorso Sanitario, ecc.)
- ✓ Redigere rapporti/relazioni di servizio

Security service desk

- ✓ Monitorare le trasferte lavorative del personale del Gruppo A2A utilizzando evolute piattaforme informatiche
- ✓ Fornire assistenza telefonica in caso di emergenza fungendo da tramite con gli uffici istituzionalmente preposti.
- ✓ Predisporre Safety Regular Checks per il personale in trasferta nei paesi a medio alto rischio
- ✓ Partecipare fattivamente alle Gestione delle emergenza collaborando con i Responsabili dei Piani Emergenza delle varie sedi
- ✓ Svolgere attività di Security Desk per tutto il Gruppo A2A
- ✓ Redigere rapporti/relazioni di servizio

Videoronda

- ✓ Effettuare ronde virtuali sui vari siti connessi utilizzando gli impianti di videosorveglianza, rispettando una precisa pianificazione
- ✓ Controllare a distanza i beni mobili o immobili delle Società consorziate con l'ausilio di apparecchiature che trasferiscono le immagini, allo scopo di promuovere l'intervento della guardia giurata
- ✓ Redigere rapporti/relazioni di servizio

Altri servizi

- ✓ Servizi di vigilanza a presidio delle sedi
- ✓ Servizi fiduciari (portierato/reception)
- ✓ Servizi di monitoraggio e risposta agli incidenti informatici (cyber defence)
- ✓ Analisi forensi post incident
- ✓ Penetration test e vulnerability assessment

- ✓ Progetti di security fisica e logica

Un approccio per «processi»

Organizzazione basata sul ciclo di Deming
ispirata a ISO 9001

Plan
- Direttore Group Security & Cyber Defence

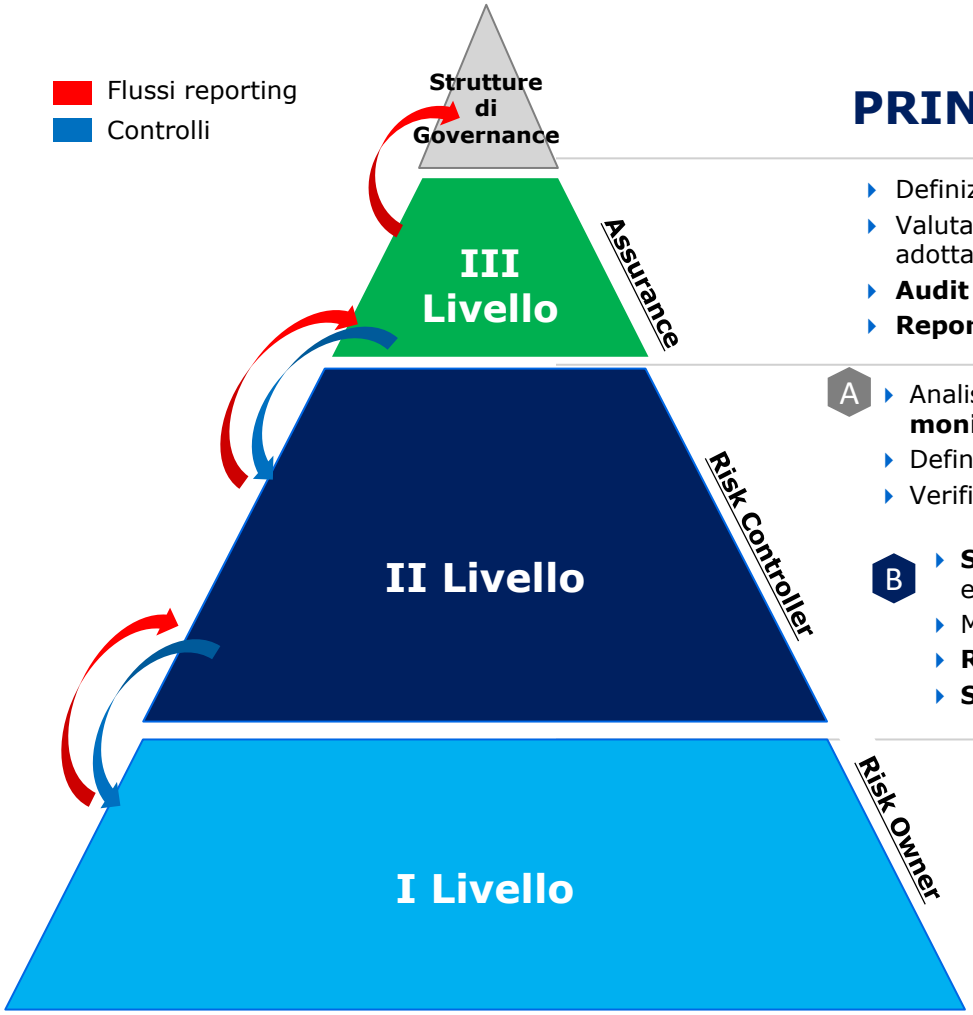
Do
- Competitive Intelligence
- Protezione BU
- Security Cross Processes
- Cyber Defence

Check
- Sistema di Gestione della Security
- Controllo tecnico gestionale

Act
- Competitive Intelligence
- Protezione BU
- Security Cross Processes
- Cyber Defence

La nostra organizzazione si è strutturata per passare dai Progetti ai Servizi

Il Sistema di Controlli Interni in A2A



PRINCIPALI ATTIVITA' SVOLTE …

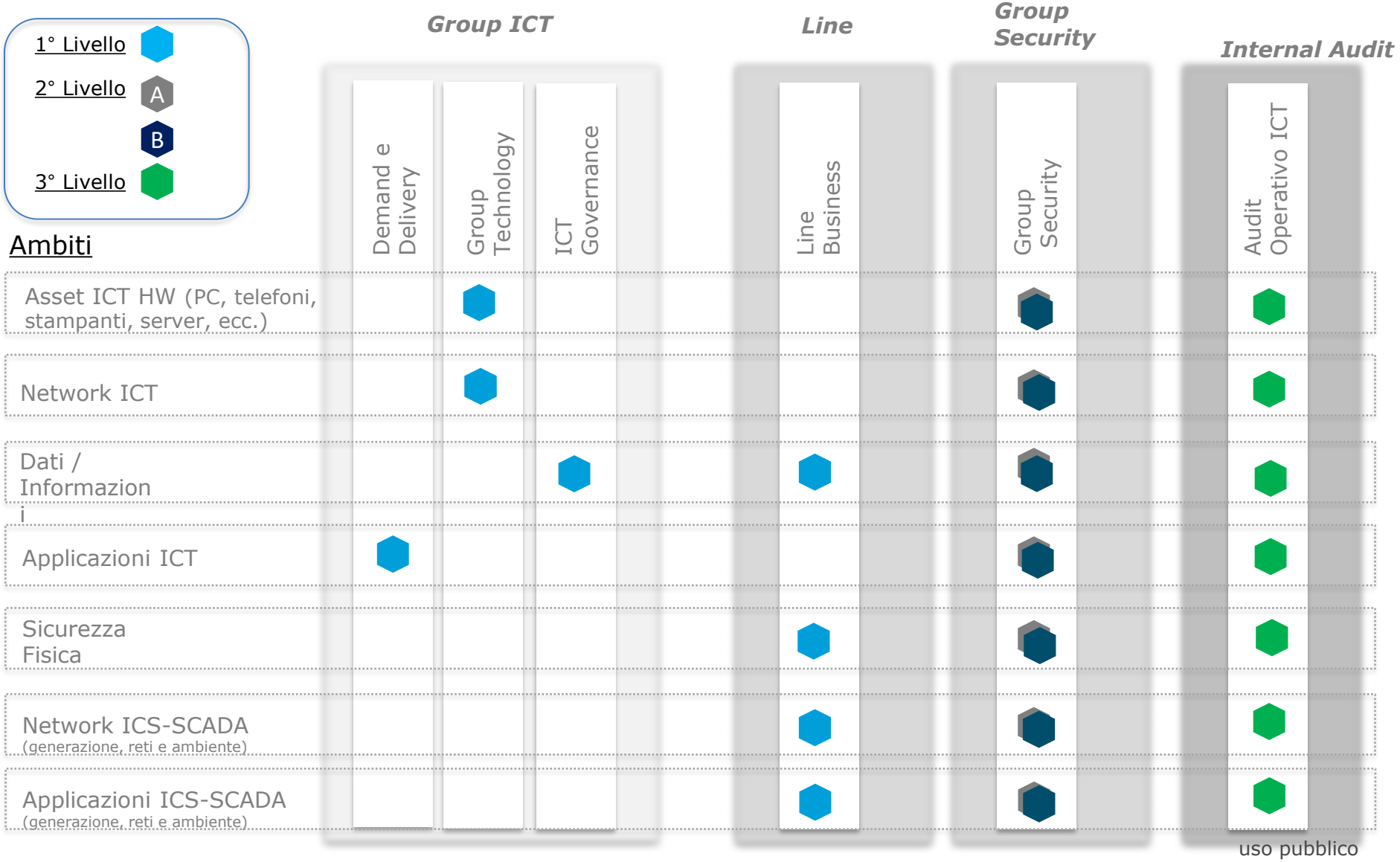
- Definizione e esecuzione **piano di audit**
- Valutazione **adeguatezza Funzioni di II Livello** e dei modelli da esse adottati
- **Audit speciali** su base esigenze strutture di governance
- **Reporting periodico** verso organi consiliari / soggetti apicali

A
- Analisi normative esterne rilevanti, elaborazione **Linee Guida e monitoraggio del recepimento da parte di Livello II B**
- Definizione **modelli di valutazione rischi** / approccio metodologico
- Verifiche di conformità e monitoraggio sui controlli svolti da Risk Owner

B
- **Supporto** a strutture I Livello per valutazione rischi, definizione controlli e elaborazione procedure tecniche specifiche per recepire Linee Guida
- Monitoraggio, anche preventivo, analisi log e segnalazione **incident**
- **Reporting periodico** verso soggetti interessati
- **Sensibilizzazione** del business sui temi normativi di competenza

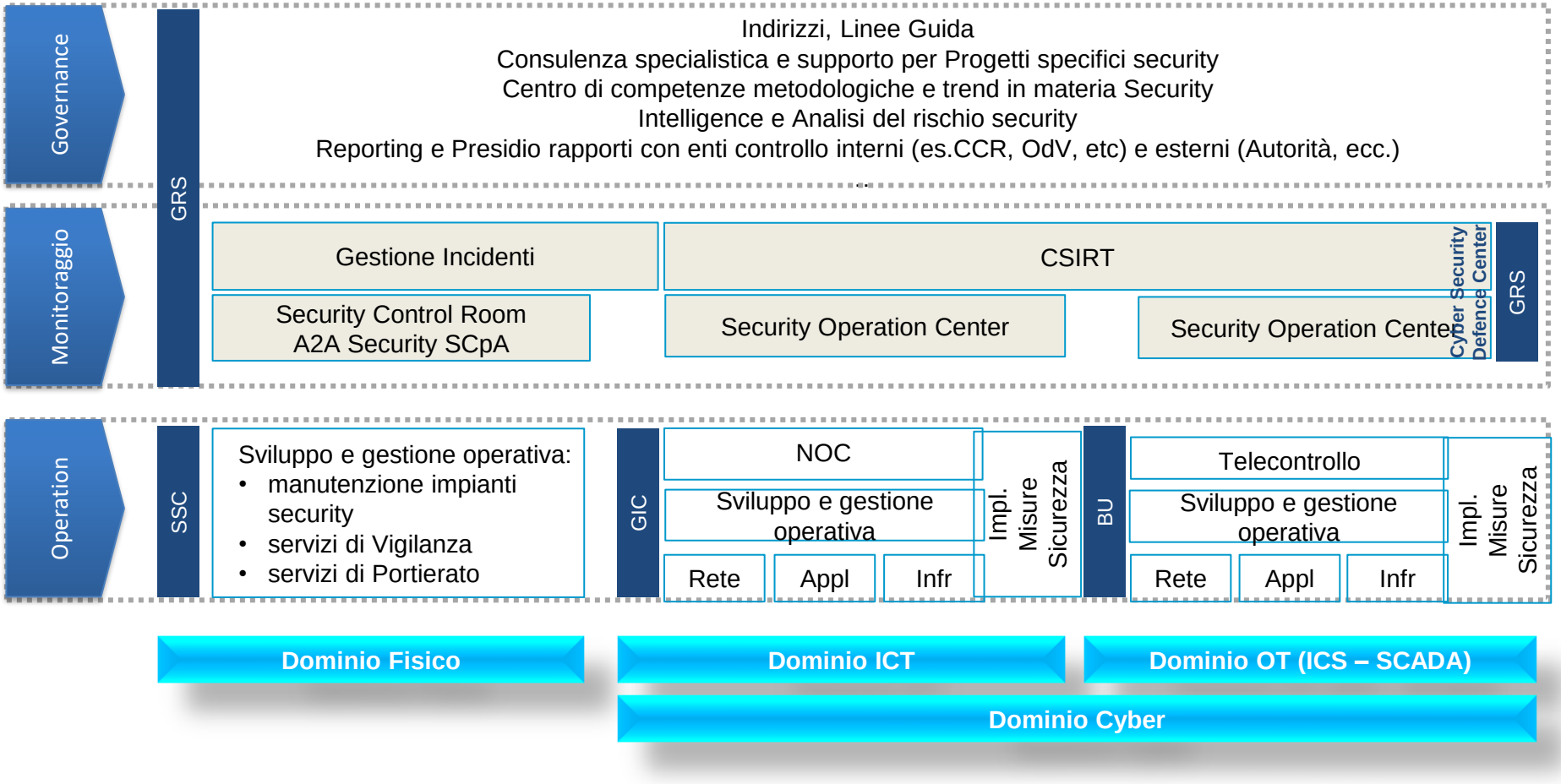
- **Declinazione** Linee Guida in procedure tecniche e definizione relativi strumenti / tecnologie di **security**
- **Supporto all'implementazione** / manutenzione di applicativi /infrastrutture per adozione procedure tecniche e relativi strumenti /tecnologie di **security**
- Invio log e gestione **Incident**
- **Identificazione** e **valutazione rischi**
- **Esecuzione controlli** per mitigazione **rischi**
- **Reporting periodico** verso Funzioni di II Livello

Ambiti Security – Responsabilità target per area



Framework Security aziendale

Modello di gestione integrata Security A2A



Modello di Governance

2015 Italian Cyber Security Report – *Un Framework Nazionale per la Cyber Security*

Il Rischio Cyber

(…) Top Management deve affrontare il tema della Cyber Security come un problema di gestione generale del rischio (Enterprise Risk Management) e non esclusivamente come un problema dell'"Information Technology".

Governance

(…) affiancare le funzioni di sicurezza all'interno dell'ICT, con funzioni di Sicurezza Logica collocate al di fuori dell'ICT (solitamente a riporto del Chief Security Officer o del Chief Risk Officer, oppure in alcuni casi a riporto diretto del Direttore Generale, del Chief Operating Officer o dell'Amministratore Delegato). Questa funzione di Sicurezza Logica è guidata dal CISO - Chief Information Security Officer. Questa impostazione garantisce i principi di segregazione delle responsabilità, nonché consente di poter differenziare i controlli di sicurezza di primo livello (a carico dell'ICT o delle funzioni di business/produzione) dai controlli di secondo livello (a carico del CISO e/o della funzione di sicurezza logica).

Sinergie tra Security e HSE-Quality

Governance

Modello integrato di indirizzo e controllo, presidio di compliance, sviluppo centro di competenze tecniche, intelligence, **analisi del rischio**, gestione rapporti con Autorità locali e nazionali

Controllo di 2° livello

Monitoraggio, audit tecnici e **gestione degli incidenti/crisi**

A2A Security SCpA

Sala Controllo unificata per security e antincendio

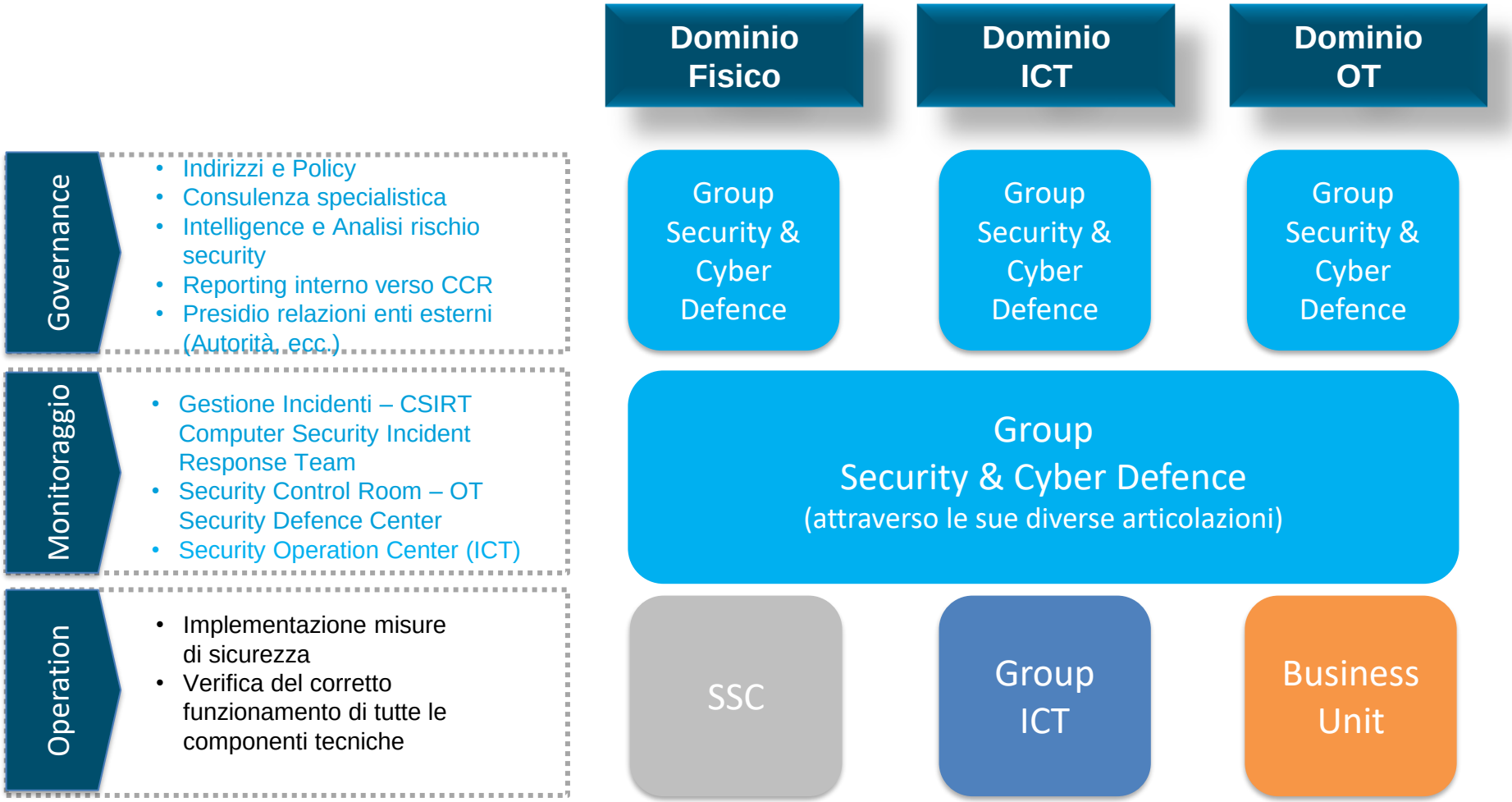
Sistemi di gestione già certificati in A2A

- Salute lavoratori
- Sicurezza nei luoghi di lavoro — OHSAS 18001 — ISO 45001
- Sicurezza dei beni — S.G.Se.A. di A2A
- Sicurezza delle informazioni — ISO 27001
- Ambiente — ISO 14001 — EMAS
- Qualità — ISO 9001
- Etica — SA 8000
- Sistema di Corporate Social Responsability

Sistemi di gestione

Presidio integrato dei sistemi di gestione

Modello organizzativo security nel Gruppo A2A



Evoluzione degli scenari tecnologici

- In questi ultimi anni è maturata l'attenzione alle tematiche di sicurezza cibernetica, dovute alla convergenza tecnologica tra sistemi industriali e informatici, nonché **l'interconnessione** tra sistemi che ha fatto aumentare la lista di incidenti in cui i sistemi IT connessi all'OT hanno propagato la minaccia.
- In tutto il mondo aumenta l'attenzione, che storicamente era stata dedicata alla tradizionale sicurezza informatica, sulla sicurezza dei **sistemi industriali** (Industrial Control System – ICS) e degli SCADA (Supervisory Control And Data Acquisition):viene coniato il termine **Cyber-Physical Security**.
- Il 2003 è il primo anno noto per la diffusione di diversi virus/worm sulla rete, che ha comportato diversi problemi anche nell'ambito industriale:
  - la centrale nucleare David-Besse (Ohio – USA) è infettata dal virus Slammer nonostante fosse protetta da firewall. Il virus è infatti portato da un PC di un fornitore connesso via modem che – di fatto – bypassa il firewall perimetrale;
  - l'U.S. Railway Company è costretta a bloccare il sistema ferroviario per diverse ore a causa dell'infezione del virus Blaster;
  - il Virus Nachi / Welchia comporta il rallentamento di una società chimica Francese;
  - in Iran attraverso il virus/worm Stuxnet, si è stati in grado di alterare il normale funzionamento delle centrifughe di arricchimento dell'uranio.
- Cambiano le priorità della sicurezza stessa: lato IT si ci si focalizza sulla confidenzialità del dato, mentre nell'OT si è soliti focalizzarsi sulla **safety** e sulla **disponibilità**.

Presidi Cyber Defence nel Gruppo A2A

Il Gruppo A2A ha deciso di gestire il rischio cyber presidiando, tramite la funzione **Group Security & Cyber Defence**, le seguenti attività:

Iniziative Cyber Security nel Gruppo A2A

Gruppo di Lavoro «OT Security»

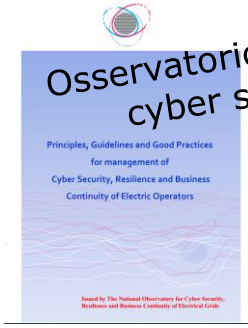
Networking

Campagna phishing 2019

ITSAR ISTITUTO TECNICO SUPERIORE ANGELO RIZZOLI

Corso di formazione per analista cyber

Osservatorio nazionale cyber security



Workshop 18 settembre 2019

Security Excellence

Security Excellence

Sistema Gestione Security Aziendale

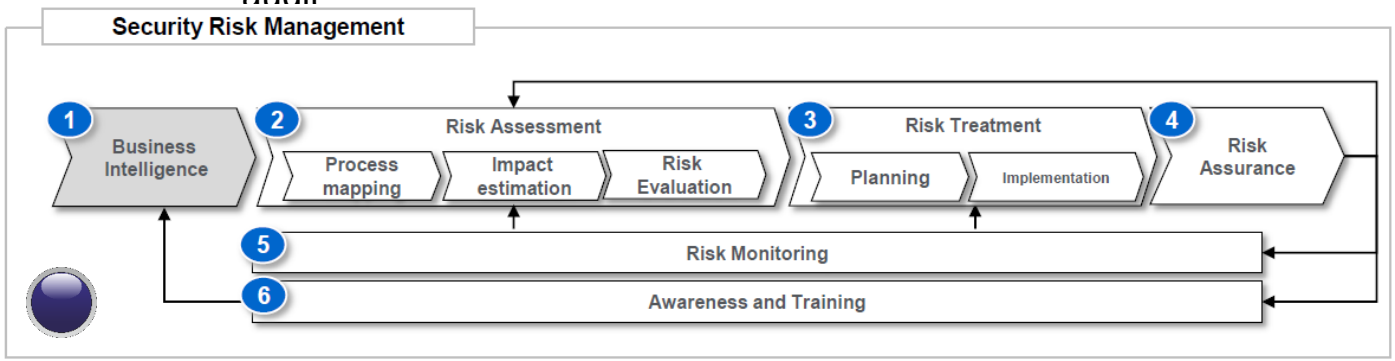
- Progettazione piano documentale della security aziendale
- Predisposizione documenti
- Predisposizione e attuazione piano di audit

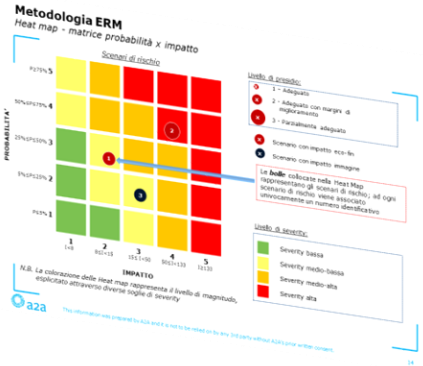
Security Cross Process

- Progettazione processi di gestione della sicurezza trasversali a varie funzioni aziendali (es. Risk Management,...)

Studi & benchmark

- Processo di analisi e studio di normative, nuovi scenari, modelli di rischio, ecc. ecc.
- Progetti speciali interfunzionali





Rischi gestiti da A2A Group Security & Cyber Defence

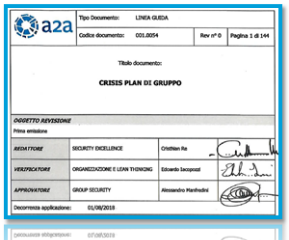
	1	2	3	4	5	6	7
Rischi	Travel Risk	Rischio accessi non autorizzati (danneggiamenti / furti /sabotaggi/ attacchi terroristici)	Cyber Risk	Rischio reputazionale	Rischio privacy Cyber risk	Rischio Infrastrutture critiche	Rischio interruzione del business
Processi	Travel Risk Management	Gestione servizi ispettivi/di vigilanza, controllo accessi fisici e logici	Implementare misure tecniche ed organizzative proporzionate ai rischi esistenti	Reputational Due Diligence	Assessment TVCC di Gruppo Sistemi ICT-ICS	Sviluppo metodologia MIDA (Ciclo Idrico)	Business Continuity management
Funzioni	Security Cross Process	Protezione BU Cyber Defence	Cyber Defence	Competitive Intelligence	Security Excellence Cyber Defence	Security Excellence	Security Excellence

CORSI SECURITY MANAGEMENT A.A. 2020/2021

Sistema di Gestione delle Crisi

1 GESTIONE DELLA CRISI IN A2A

Agosto 2018
Pubblicazione del **CRISIS PLAN** di Gruppo emesso da *Group Security*



Identifica il sistema organizzativo, le attività e le procedure necessarie per far fronte agli eventi che hanno portato alla dichiarazione di crisi e al ripristino in tempi rapidi le normali condizioni di operatività

Team Gestione Crisi Corporate

Componenti in relazione al tipo di crisi

Responsabili di:
- Group Security (**coordinatore crisi**)
- Affari Legali e Compliance
- Comunicazione Esterna e Media Relations
- Risorse Umane, HSE, Organizzazione e Change Management
- Group ICT
- Rapporti Istituzionali e Territoriali
- Responsabile della BU coinvolta (o delle BU coinvolte)
- Gestore Indipendente per società soggette a separazione funzionale

Riferiscono a...
- Amministratore Delegato e Direttore Generale di A2A SpA
- Presidente di A2A SpA

Sistema di Gestione dell'Emergenza COVID-19

2 RISPOSTA DI A2A

Venerdì 21 Febbraio 2020
Ore 14:00
Riunione tra Group Security e HSE

Attivazione

- COMITATO DI GRUPPO A2A
- COMITATO GESTIONE CONTINUITÀ OPERATIVA
- COMITATO ZONA ROSSA

Società impattate:
- Linea Gestione
- Linea Ambiente
- LD Reti

Presidio attivo 24/7, in presenza e tramite chat

Da Venerdì 21 Febbraio 2020
A2A è presente, in modo permanente, al Tavolo di crisi della sala operativa **dell'Unità di Crisi della Prefettura di Milano**

Da Martedì 25 Febbraio 2020
A2A partecipa ai tavoli tecnici dei servizi essenziali della **Prefettura di Brescia**

Comitato di Gruppo A2A
- Presieduto e coordinato dal Responsabile Group Security & Cyber Defence
- Si è riunito tutti i giorni dal 24 Febbraio al 9 aprile 2020
- Dal 9 aprile è iniziata la fase di «normale gestione dell'emergenza»
- Dal 14 aprile si è riunito 2 volte a settimana, salvo particolari criticità o necessità

Indirizzamento alla «nuova normalità»

3 LA FASE 2

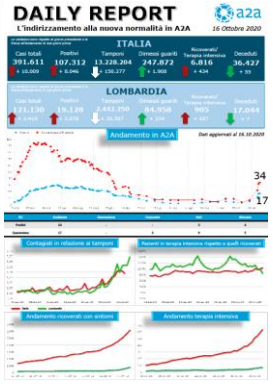
Nel caso di A2A non si tratta di Ripresa, ma di un ulteriore cambiamento nella gestione dei processi, perché il Gruppo e le sue attività essenziali non si sono mai interrotte

Istituzione di un gruppo di lavoro per la fase 2

Questo gruppo di lavoro ha coordinato tutte le **misure** necessarie (stabilite dalla normativa nazionale e da norme tecniche) per far rientrare il personale alla «nuova normalità»

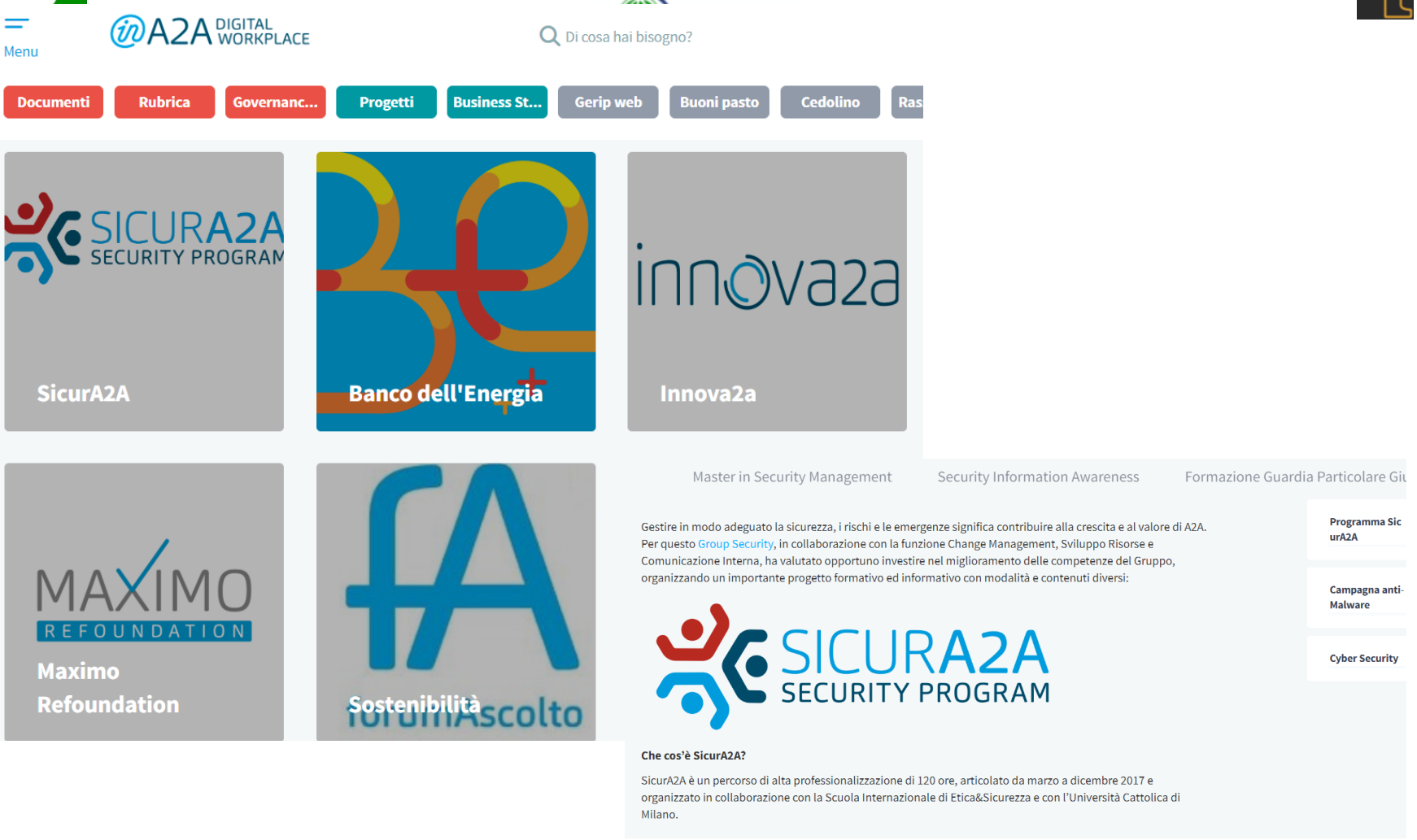
Redazione delle **Linee Guida per la gestione del rientro – fase 2**

- Sanificazione degli ambienti prima del rientro
- Predisposizione di un KIT per tutti i dipendenti
- Rilevazione della temperatura all'ingresso
- Buone prassi di comportamento
- Riorganizzazione degli spazi (uffici, aree comuni ecc.)
- Gestione degli esterni (fornitori e clienti)



uso pubblico

CORSI SECURITY MANAGEMENT A.A. 2020/2021



CORSI SECURITY MANAGEMENT A.A. 2020/2021

Formazione

SICURA2A SECURITY PROGRAM

Corso di alta formazione *Security & Safety Management*

120 h

ISPS Code

Corso sul ***Port Facility Security Officer***

16 h

Corso ***Focus sul Terrorismo*** costituito dai seguenti moduli:

- Fenomeno terroristico
- Prevenzione e gestione evento
- Stabbing

24 h

Corso sul ***Monitoraggio delle vulnerabilità***

8 h

Rischi gestiti

Rischi	Travel Risk	Rischio accessi non autorizzati (danneggiamenti/ furti /sabotaggi/ attacchi terroristici)	Crisi/Emergenze	Rischio reputazionale	Rischio privacy Cyber risk
Processi	Travel Risk Management	Gestione servizi ispettivi/di vigilanza, controllo accessi fisici e logici	Master Crisis Plan	Reputational Due Diligence	Assessment TVCC di Gruppo Sistemi ICT-ICS
Funzioni	Security Cross Process	Protezione Corporate/ Protezione BU Cyber Defence	Security Cross Process Cyber Defence	Competitive Intelligence	Security Excellence Cyber Defence

Travel risk

Rischi	Travel Risk	Rischi socio-politici, sanitari, terroristici, geo-ambientali ed economici per i dipendenti in trasferta.
Processi	Travel Risk Management	Processo di analisi del rischio dei Paesi in cui i dipendenti si recano in trasferta, predisposizione di contromisure e predisposizione di un centralino per le emergenze che è in grado di monitorare i dipendenti in trasferta.
Funzioni	Security Cross Process	Funzione che si occupa della progettazione processi di gestione della sicurezza trasversali a varie funzioni aziendali.

Rischio accessi non autorizzati

Rischi	Accessi non autorizzati	Rischio di accessi non autorizzati/danneggiamenti/furti/sabotaggi/attacchi terroristici che possono causare danno al patrimonio aziendale.
Processi	Controllo accessi	Processo di valutazione degli strumenti tecnologici più idonei a garantire il controllo degli accessi fisici e logici (in collaborazione con ICT Security) alle sedi del Gruppo.
	Vigilanza e servizi ispettivi	Processo di costante custodia e presidio dei beni mobili e immobili del Gruppo.
Funzioni	Security Excellence	Funzione che si occupa della pianificazione del servizio di sicurezza in oggetto e del suo monitoraggio costante.
	Protezione BU	Funzione che si occupa di attuare i processi di security pianificati da «Security Cross Processes&Projects».
	A2A Security ScpA	Funzione che si occupa di vigilare sulla sicurezza dei beni mobili e immobili dei Soci.
	Cyber Defence	Presidio di intelligence e di gestione dei rischi cyber (dominio ICT e OT)

Crisis & Incident management

Rischi	Crisi/Emergenze	Rischi in grado di compromettere l'integrità delle risorse umane e degli asset aziendali nonché la continuità operativa del business.
Processi	Crisis & Incident Management e Master Crisis Plan	Processo costante di monitoraggio delle vulnerabilità e di analisi e gestione dei rischi di security e di contrasto e prevenzione delle frodi, con conseguente produzione documentale relativa alla gestione di crisi ed incidenti.
Funzioni	Security Cross Process	Funzione che si occupa della progettazione processi di gestione della sicurezza trasversali a varie funzioni aziendali.
	Cyber Defence	Presidio di intelligence e di gestione dei rischi cyber (dominio ICT e OT)

Rischio reputazionale

Rischi	Rischio reputazionale	Rischi in grado di compromettere la reputazione aziendale.
Processi	Due Diligence	Processo costante di monitoraggio dell'affidabilità di tutti i soggetti (persone fisiche e giuridiche) che entrano in contatto con l'azienda (es. fornitori).
Funzioni	Competitive Intelligence	Funzione che si occupa della pianificazione delle strategie di verifica dell'affidabilità dei soggetti terzi che entrano in contatto con l'azienda e del loro monitoraggio.

Rischio privacy e Cyber risk

Rischi	Rischio privacy Cyber Risk	Rischi in grado di compromettere la protezione dei dati delle persone fisiche presenti in azienda (dipendenti, consulenti, esterni, ecc.) .
Processi	Assessment impianti videosorveglianza	Processo di valutazione ed analisi della compliance dei sistemi di videosorveglianza del Gruppo al nuovo Regolamento EU 679/2016.
	Creazione Registro dei Trattamenti	Creazione di un Registro dei trattamenti di dati personali effettuati dal titolare del trattamento relativi a: controllo accessi, videosorveglianza e analisi reputazionali.
	Cyber Defence	Presidio di intelligence e di gestione dei rischi cyber (dominio ICT e OT)
Funzioni	Security Cross Processes & Projects	Funzione che si occupa della pianificazione delle strategie di sicurezza in oggetto e del loro costante monitoraggio.
	Cyber Defence	Presidio di intelligence e di gestione dei rischi cyber (dominio ICT e OT)

Infrastrutture Critiche

Direttiva 2008/114/CE Infrastrutture Critiche

8 dicembre **2008**: **Direttiva** 114 del Consiglio relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione

Da recepire entro 12/1/2011

In Italia D.Lgs **11 aprile 2011:** Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione.

Entrato in vigore **5/5/2011**

L'art. 211 bis Decreto Legge 19.05.2020, n. 34

Infrastrutture Critiche

L'art. 211 bis del D.L. 19.05.2020, n. 34 (il così detto **DL Rilancio**) impone agli operatori di infrastrutture critiche di adottare, ovvero aggiornare, i proprio **piani di sicurezza** con specifiche misure atte a garantire una migliore gestione di crisi derivanti da **emergenze sanitaria**.

Tali aggiornamenti devono essere redatti d'intesa con le amministrazioni competenti e, per quel che concerne la gestione dell'emergenza Covid-19, tener conto delle linee guida emanate dai Ministeri competenti per materia e dei "Principi Precauzionali" emanati dalla **Segreteria Infrastrutture Critiche** della **Presidenza del Consiglio dei Ministri**.

Parte II
Piano Annuale della Security

•**Il Piano Annuale della Security contiene i progetti e le attività per eliminare o ridurre le aree di criticità frutto di:**

- valutazione del rischio e delle non conformità di Sistema;
- indicazioni del Top Management o di enti/organizzazioni esterne all'azienda;
- analisi delle prestazioni di security dell'anno precedente.

Le relative azioni riguardano attività:

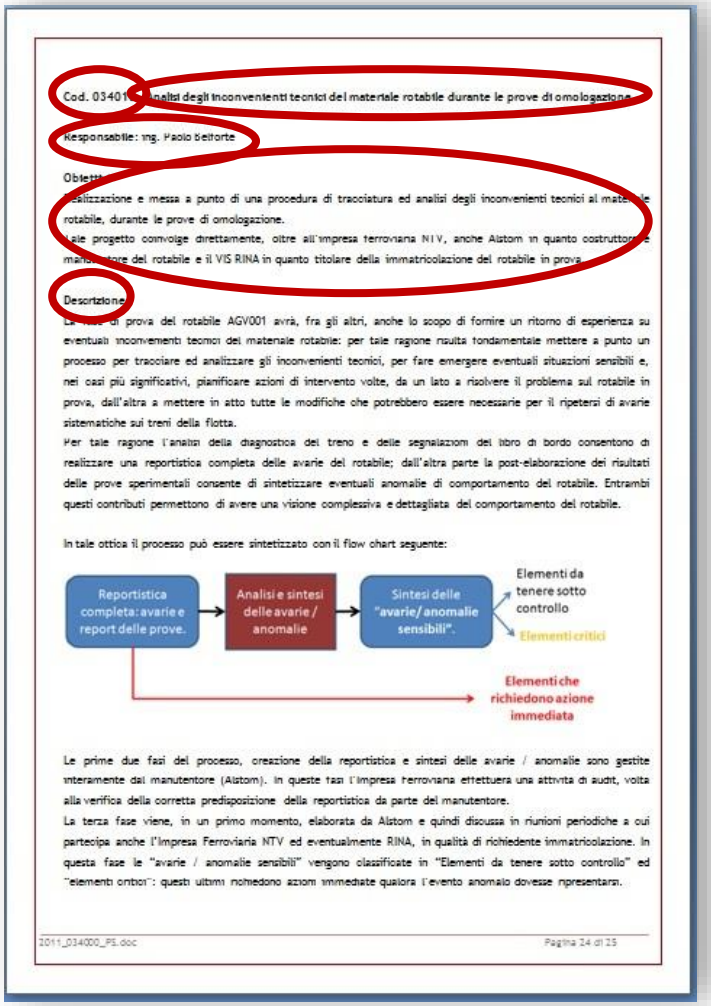
- per la piena attuazione o eventuali adeguamenti e miglioramenti dell'SGSeA;
- finalizzate al mantenimento o al miglioramento delle prestazioni di sicurezza;
- di verifica ed ispezione da condurre nel campo della sicurezza;
- finalizzate all'adozione di sistemi e tecnologie per la sicurezza, nelle fasi di ideazione, progettazione, realizzazione o acquisto e messa in servizio.

Piano annuale della Security

L'elaborazione del Piano è affidata al funzione Security che, con le sue linee guida, introduce i singoli **progetti** elaborati dai relativi Responsabili

L'Amministratore Delegato o il Vertice Aziendale approva il Piano ogni anno a seguito del riesame del sistema svolto con il supporto anche di un Gruppo di Lavoro Security appositamente da lui costituito

Struttura dei singoli progetti 1/3



Cod. 03401 Analisi degli inconvenienti tecnici del materiale rotabile durante le prove di omologazione

Responsabile: Ing. Paolo Belforte

Obiettivo

Realizzazione e messa a punto di una procedura di tracciatura ed analisi degli inconvenienti tecnici al materiale rotabile, durante le prove di omologazione.

Tale progetto coinvolge direttamente, oltre all'impresa ferroviaria NTV, anche Alstom in quanto costruttore e manutentore del rotabile e il VIS RINA in quanto titolare della immatricolazione del rotabile in prova.

Descrizione

La fase di prova del rotabile AGV001 avrà, fra gli altri, anche lo scopo di fornire un ritorno di esperienza su eventuali inconvenienti tecnici del materiale rotabile: per tale ragione risulta fondamentale mettere a punto un processo per tracciare ed analizzare gli inconvenienti tecnici, per fare emergere eventuali situazioni sensibili e, nei casi più significativi, pianificare azioni di intervento volte, da un lato a risolvere il problema sul rotabile in prova, dall'altra a mettere in atto tutte le modifiche che potrebbero essere necessarie per il ripetersi di avarie sistematiche sui treni della flotta.

Per tale ragione l'analisi della diagnostica del treno e delle segnalazioni del libro di bordo consentono di realizzare una reportistica completa delle avarie del rotabile; dall'altra parte la post-elaborazione dei risultati delle prove sperimentali consente di sintetizzare eventuali anomalie di comportamento del rotabile. Entrambi questi contributi permettono di avere una visione complessiva e dettagliata del comportamento del rotabile.

In tale ottica il processo può essere sintetizzato con il flow chart seguente:

Le prime due fasi del processo, creazione della reportistica e sintesi delle avarie / anomalie sono gestite interamente dal manutentore (Alstom). In queste fasi l'impresa ferroviaria effettuerà una attività di audit, volta alla verifica della corretta predisposizione della reportistica da parte del manutentore.

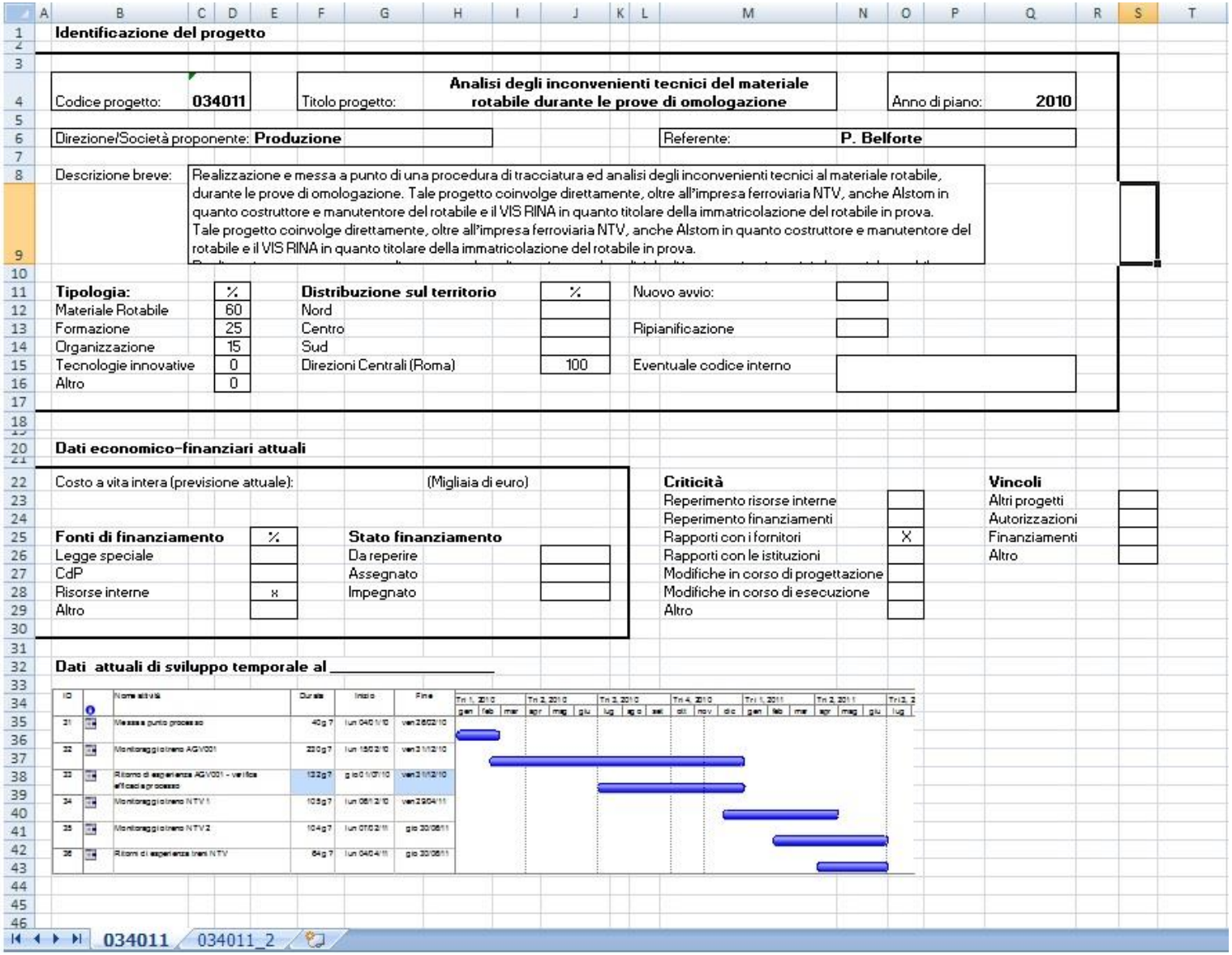
La terza fase viene, in un primo momento, elaborata da Alstom e quindi discussa in riunioni periodiche a cui partecipa anche l'Impresa Ferroviaria NTV ed eventualmente RINA, in qualità di richiedente immatricolazione. In questa fase le "avarie / anomalie sensibili" vengono classificate in "Elementi da tenere sotto controllo" ed "elementi critici": questi ultimi richiedono azioni immediate qualora l'evento anomalo dovesse ripresentarsi.

2011_034000_PS.doc Pagina 24 di 25

Per ogni Progetto è elaborata una scheda che contiene:

- codice identificativo XXX 034000;
- titolo del progetto
- indicazione Responsabile
- obiettivo
- breve descrizione generale
- breve descrizione stato avanzamento trimestrale

- foglio Excel con puntuale descrizione di alcuni indicatori



Identificazione del progetto

Codice progetto:	034011	Titolo progetto:	Analisi degli inconvenienti tecnici del materiale rotabile durante le prove di omologazione	Anno di piano:	2010

Direzione/Società proponente: **Produzione** — Referente: **P. Belforte**

Descrizione breve: Realizzazione e messa a punto di una procedura di tracciatura ed analisi degli inconvenienti tecnici al materiale rotabile, durante le prove di omologazione. Tale progetto coinvolge direttamente, oltre all'impresa ferroviaria NTV, anche Alstom in quanto costruttore e manutentore del rotabile e il VIS RINA in quanto titolare della immatricolazione del rotabile in prova.
Tale progetto coinvolge direttamente, oltre all'impresa ferroviaria NTV, anche Alstom in quanto costruttore e manutentore del rotabile e il VIS RINA in quanto titolare della immatricolazione del rotabile in prova.

Tipologia:	%	**Distribuzione sul territorio**	%	Nuovo avvio:	
Materiale Rotabile	60	Nord			
Formazione	25	Centro		Ripianificazione	
Organizzazione	15	Sud			
Tecnologie innovative	0	Direzioni Centrali (Roma)	100	Eventuale codice interno	
Altro	0				

Dati economico-finanziari attuali

Costo a vita intera (previsione attuale): (Migliaia di euro)

Fonti di finanziamento	%	**Stato finanziamento**	
Legge speciale		Da reperire	
CdP		Assegnato	
Risorse interne	x	Impegnato	
Altro			

Criticità		**Vincoli**	
Reperimento risorse interne		Altri progetti	
Reperimento finanziamenti		Autorizzazioni	
Rapporti con i fornitori	X	Finanziamenti	
Rapporti con le istituzioni		Altro	
Modifiche in corso di progettazione			
Modifiche in corso di esecuzione			
Altro			

Dati attuali di sviluppo temporale al _____

ID	Nome attività	Durata	Inizio	Fine
31	Messa a punto processo	40g 7	lun 04/01/10	ven 26/02/10
32	Monitoraggio treno AGV001	220g 7	lun 15/02/10	ven 31/12/10
33	Ritorno di esperienza AGV001 - verifica efficacia processo	132g 7	gio 01/07/10	ven 31/12/10
34	Monitoraggio treno NTV1	105g 7	lun 08/12/10	ven 29/04/11
35	Monitoraggio treno NTV2	104g 7	lun 07/02/11	gio 30/06/11
36	Ritorni di esperienza treni NTV	64g 7	lun 04/04/11	gio 30/06/11

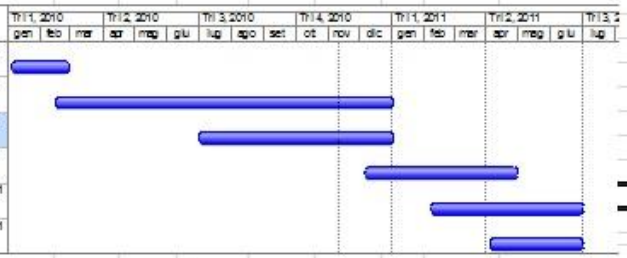
Identificazione del progetto

Codice progetto:	034011	Titolo progetto:	Analisi degli inconvenienti tecnici del materiale rotabile durante le prove di omologazione	Referente:	P. Belforte

Direzione/Società proponente:	NTV/Produzione	Anno di avvio:	2010	Anno di piano	2011

Sviluppo temporale completo (attuale)

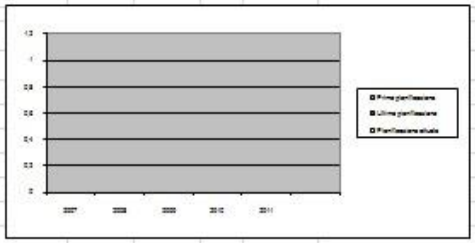
ID	Nome attività	Durata	Inizio	Fine
31	Messa a punto processo	40 g?	lun 04/01/10	ven 26/02/10
32	Monitoraggio treno AGV001	230 g?	lun 15/02/10	ven 31/12/10
33	Ritorno di esperienza AGV001 - verifica efficacia processo	132 g?	gio 01/07/10	ven 31/12/10
34	Monitoraggio treno NTV 1	105 g?	lun 06/12/10	ven 29/04/11
35	Monitoraggio treno NTV 2	104 g?	lun 07/02/11	gio 30/06/11
36	Ritorno di esperienza treni NTV	64 g?	lun 04/04/11	gio 30/06/11



Storico economico-finanziario

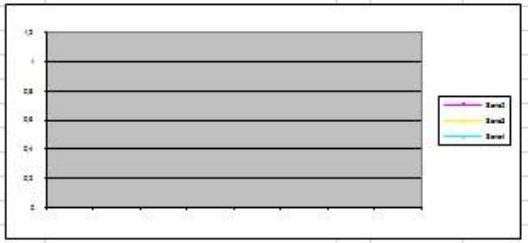
Costo a vita intera

	2007	2008	2009	2010	2011
Prima pianificazione					
Ultima pianificazione					
Pianificazione attuale					



Stato di avanzamento del progetto

	2007	2008			2009				2010	oltre
Prima pianificazione										
Contabilizzazioni										
Valore del realizzato										



I contenuti di un Piano della Security

CORSI SECURITY MANAGEMENT A.A. 2020/2021

INDICE

Obiettivi:

- Stabilire ruoli e responsabilità tra le parti;
- Assicurare la tempestiva e puntuale raccolta di informazioni;
- Fornire una metodologia omogenea per i Risk assessment e per i Security Plan;
- Assicurare la fiducia, tra le parti, che ognuno abbia implementato le misure minime previste

Requisiti funzionali:

- Raccogliere e valutare informazioni rispetto alle minacce di sicurezza;
- Assicurare il mantenimento di protocolli di comunicazioni tra le diverse funzioni
- Prevenire accessi non autorizzati nelle aree riservate;

Requisiti funzionali:

- Fornire mezzi di contrasto e procedure di reazione adeguati ;
- Garantire formazione, prove, esercitazioni ed aggiornamenti dei Risk Assessment e dei Security Plan