Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

2. PRINCIPI, STANDARDI I NORMATIVI ZAŠTITE INFORMACIJA

Ciljevi

- **Razumeti i naučiti**:
  - Terminologiju
  - Strukturu i značaj **GAISP** *(Generaly Acepted Information Security Principles)* princima
  - Strukturu, značaj, vrste standarda zaštite **(**ISO/IEC 27001/2/..., NIST, BSI**)**
  - Standard kvaliteta sistema zaštite **(**ISO/IEC 21827**)**
  - Značaj i klasifikaciju dokumentacije zaštite

Koncept i značaj principa zaštite

- **Pincip zaštite** *(generička definicija):*
  - fundamentalna aksiomatska istina, "*zakonitost*"
  - osnova za izvršavanje racionalne aktivnosti u IS
  - gradivni blokovi standarda, procesa/projekata zaštite
  - u **širem smislu** uključuje:
    - generičke *principe (logičke,..), standarde, konvencije, mehanizme i protokole (zaštite)*

Sistemski principi zaštite IKTS

- **Preuzeti** iz procesa upravljanja IKTS
- **Administrativna i fizička** ograničenja
- **Obuhvataju** opšte prihvaćene i dokazane:
  - personalne, organizacione i operativne mere
- **Sprečavaju** sukob nadležnosti i zloupotrebu privilegija
- **Povećavaju** opštu pouzdanost resursa IKTS
- **Baza** za implementaciju GAISP principa
- **Obavezan okvir** u koji se ugrađuju specifični GAISP

Sistemski principi zaštite IKTS

- Standardni principi upravljanja IKTS:
  - *nikada sam*
  - *rotacija radnih mesta*
  - *razdvajanje dužnosti*
  - *dužna pažnja*
  - *minimum privilegija*
  - *prazan sto, čist ekran...*

Sistemski principi zaštite IKTS

- **Princip „nikada sam“**

- zahteva zapošljavanje **najmanje dva lica** za:
  - *autorizaciju prava pristupa*
  - *procesiranje osetljivih informacija*
  - *testiranje i prijem hardvera i softvera*
  - *modifikaciju hardvera, softvera i IKTS*
  - *projektovanje i implementaciju DB, programa ...*
  - *izmenu dokumentacije i procedura u IKTS*
  - *destrukciju važnih programa itd*.

Sistemski principi zaštite IKTS

- **Rotacija radnih mesta**

- Zahteva:
  - promenu pozicija na bezbednosno značajnom r/m
  - niko nesme pomisliti da je nezamenljiv
  - rotacija osoblja, zavisno od broja/kvalifikacije zaposlenih

Sistemski principi zaštite IKTS

Obavezno razdvajanje dužnosti u IKT sistemu	
operativni rad na računaru	programiranje
unos i priprema podataka za obradu	obrada podataka
obrada podataka	kontrola kvaliteta IKTS
operativni rad na računaru	čuvanje elektronskih medija
prijem osetljivih informacija	predaja osetljivih informacija
kopiranje, izdavanje/uništavanje osetljivih informacija	izdavanje ovlašćenja
programiranje aplikacija	sistemsko programiranje
programiranje aplikacija	administracija baza podataka
projektovanje, implementacija/ modifikacija sistema zaštite	bilo koji drugi posao
kontrola ovlašćenja za pristup	bilo koji drugi posao

Sistemski principi zaštite IKTS

- **Princip *minimuma privilegija***
  - davanje što je moguće manje privilegovanih naloga
- **Princip “*znati samo što je potrebno*”**
  - pristup samo informacijama, potrebnim za rad
- **Principi upravljanja IKTS**
  - obezbeđuje osnovni nivo upravljanja zaštitom:
    a. *postavljanje fizičkih prepreka i ograničenja i*
    b. *administrativno nametanje pravila ponašanja u radu sa IKTS*

GAISP

- **Opšte prihvaćeni principi zaštite** informacija
- **Promovišu** dobru praksu zaštite
- **Obezbeđuju**:
  - globalnu harmonizaciju principa zaštite
  - referentni nivo, konzistentnost i *merljivost* zaštite
  - ponovljivost procesa zaštite (manje troškove)
  - skup pravila/metrika/standarda za upravljanje S/Z
  - sertifikaciju S/Z i samostalnu izradu politika zaštite
  - brži razvoj metodologije i tehnologije zaštite itd.

GAISP- opšte karakteristike

- Precizno definisan, kompletan i konzistentan
- Usaglašen sa navedenim bezbednosnim ciljem
- Tehnički izvodljiv i prihvatljiv
- Prikladan za primenljive standarde i uputstva z.
- Dobro prezentovan (gramatika i sintaksa)
- **Prezentacija :**
  - *naziv,*
  - *definicija,*
  - *objašnjenje (opis) i*
  - *primer principa*

GAISP-struktura

1. **GAISP - Opšte prihvaćeni principi zaštite:**
   - za menadžment, strategiju i smernice u zaštiti
2. **Funkcionalni principi zaštite:**
   - gradivni blokovi GAISP za izgradnju arhitekture s/z
3. **Detaljni** (*potpuni, kompletni*) **principi zaštite:**
   - gradivni blokovi funkcionalnih principa
   - namenjeni za profesionalce u zaštiti

GAISP-Opšte prihvaćeni principi zaštite

- OECD + NIST = GAISP principi
- upravljanje S/Z na *konceptualnom* nivou
- retko se menjaju (2007) štite CIA informacija

1. **odgovornosti**
2. **preispitivanja i procene**
3. **svest o potrebi zaštite**
4. **etičnosti**
5. **demokratičnosti**
6. **integracije**
7. **multidisciplinarnosti**
8. **proporcionalnosti**
9. **blagovremenosti**

Primer GAISP principa

1. **Ime:** ***Princip odgovornosti***
2. **Definicija:** ovlašćenja i odgovornosti moraju biti jasno definisani, shvaćeni i prihvaćeni u s/z
3. **Objašnjenje**:
   - *Odgovornos*t - način kontrole akcija svih relevantnih učesnika u IKT sistemu
   - *Uloge* - jasno definišu, identifikuju i dodeljuju ovlašćenja za pristup osetljivim objektima IKTS
   - *Odnosi između učesnika, procesa i informacija* - jasno definisani, dokumentovani i prihvaćeni od svih učesnika
   - *Kontrolisane odgovornosti (lični nalozi)*- svi učesnici u s/z moraju prihvatiti odgovornost za ovlašćenja

Funkcionalni principi zaštite

- Gradivni blokovi opštih GAISP principa
- Definišu *taktiku* primene *kontrola* zaštite u praksi

Detaljni principi zaštite

- Gradivni blokovi funkcionalnih principa zaštite
- Definišu ih specijalisti zaštite za dnevno upravljanje R i s/z
- Elementi procedura zaštite
- Podržavaju jedan ili više funkcionalnih principa
- uključuju *tehnologije/okruženja/standarde/praksu*

Primer: detaljni principi

1. **Opšti GAISP:** ***Proporcionalnost***
2. **Funkcionalni**: *Kontrola pristupa*
3. **Detaljni***: Upravljanje lozinkom*

- **Ime**: *Jednokratna lozinka*
- **Objašnjenje:**
  - *Višekratni pasvordi* su zastareli, tradicionalni mehanizam za AC
  - *Jednokratni pasvord* – obezbeđuje ga tehnologija smart kartica

Primer: primena generatora jednokratnih pasvorda ili smart kriptokartice

Implementacija principa zaštite

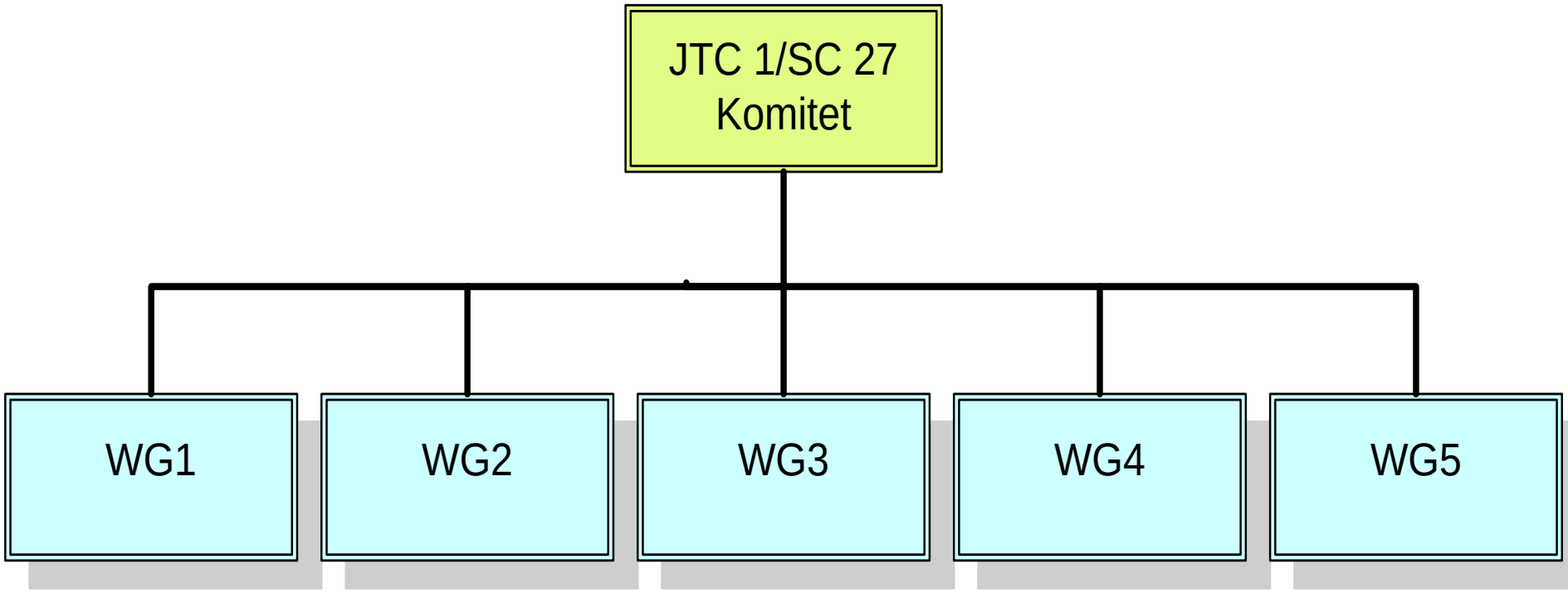
- **Kroz:**
  - razvoj programa (*programske politike*) zaštite(**NIST**)
  - *razvoj ISMS politike zaštite* (**ISO/IEC 27001**)
  - razvoj politika zaštite funkcionalnih komponenti SZ
  - obuku i podizanje svesti o potrebi zaštite
  - nametanje obaveza itd.

Standardi zaštite

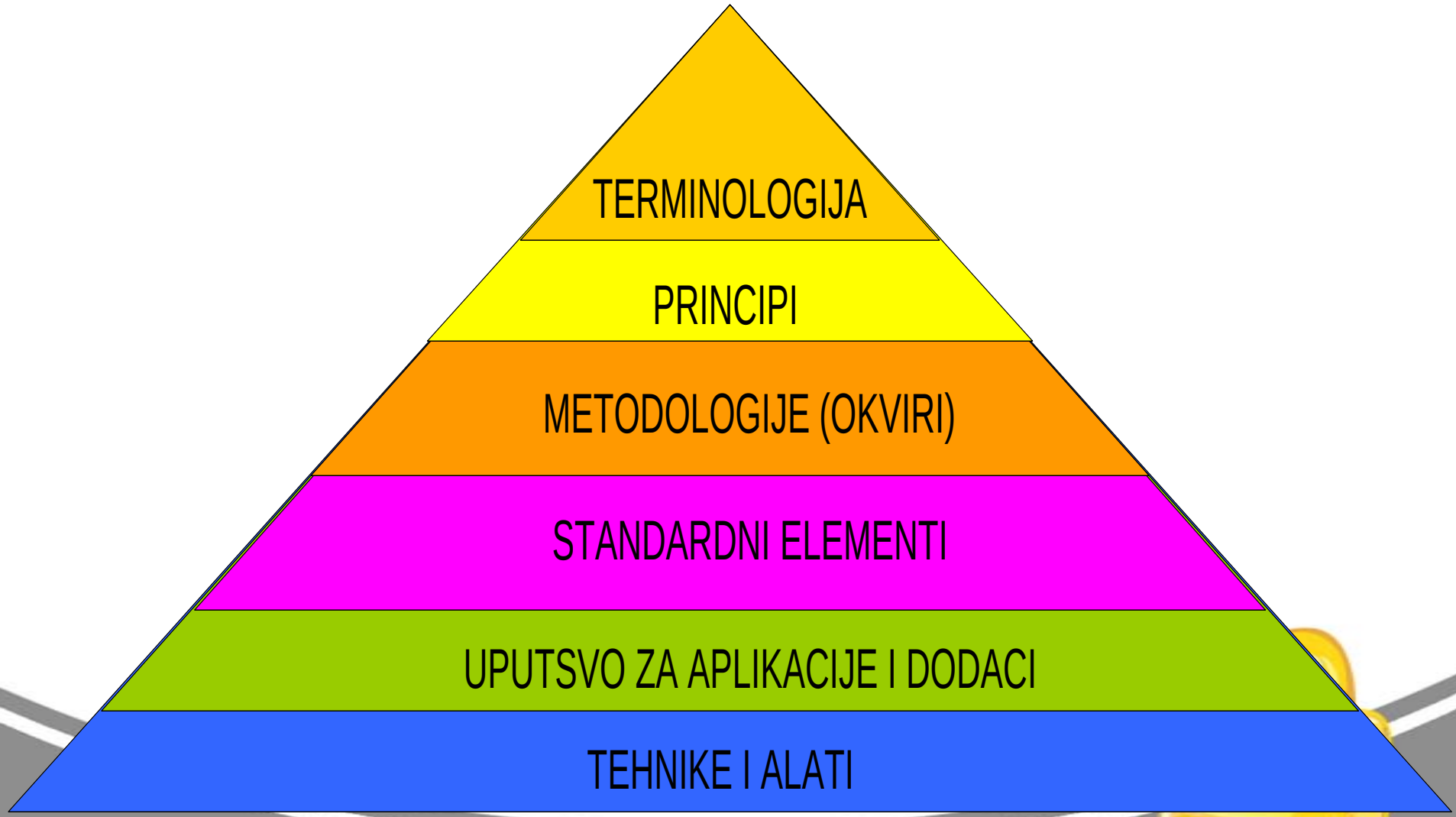
– **Međunarodni tehnički komitet za standardizaciju** *ISO/IEC JTC1/SC27*, formiran **1990**
– Ima organizovana tela za standarde, komponente...
– Obuhvataju sve aspekte zaštite informacija i privatnosti:
  • *metodologija, ISMS , kriptografski i drugi mehanizmi*
  • *dokumentacija i terminologija zaštite*
  • *upravljanja identitetom i zaštitom privatnosti*
  • *metodologija i kriterijumi za evaluaciju zaštite* itd.

Standardi zaštite

Tehničkikomitet ISO/IEC JTC 1SC 27



Opšti model standarda zaštite



Standardi zaštite

- **Primarni cilj:**
- **NIJE** *sama standardizacija zaštite***???**
- **JESTE:**
  - *smanjenje kompleksnosti S/Z*
  - *standardizacija dokumentacije*
  - *obezbeđuje interoperabilnosti*
  - *formiranje baze znanja iz oblasti zaštite*
  - *obezbeđenje sertifikacije i akreditacije (**C&A**) S/Z*
  - *uvođenje promene* u *upravljački okvir zaštite (**SMF**)*

Standardi zaštite

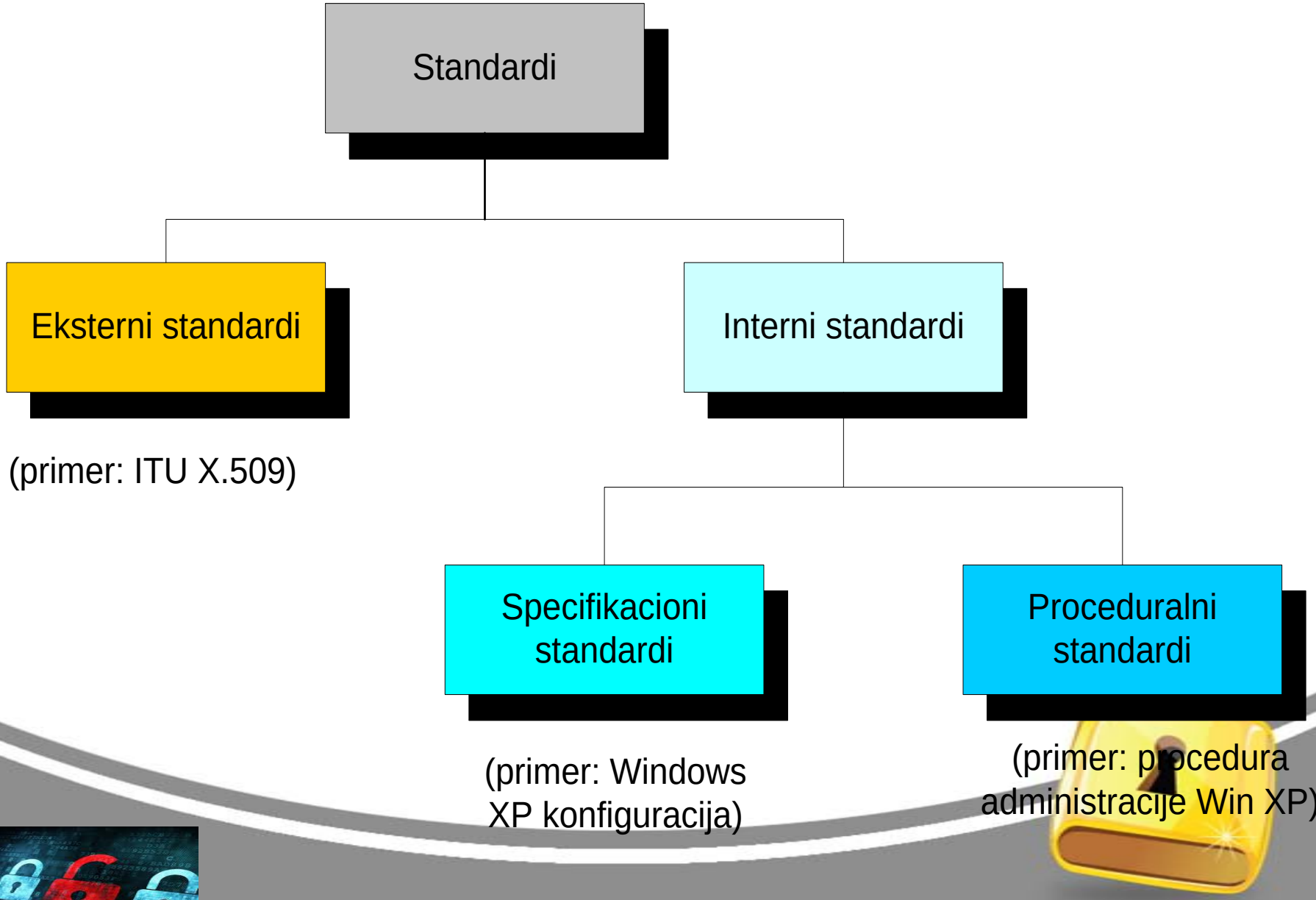
Opšta definicija:

- *usvojen i objavljen dokument, uspostavlja specifikaciju i procedure koje obezbeđuju da:*
  - *dokumenta, materijal, proizvod, metod ili servis zaštite odgovara nameni i konzistentno izvršava svoje funkcije*.
- *pokriva sve zahteve za održavanje prihvatljivog rizika-Rpn*
- *obezbeđuju objektivne mere za razvoj/implementaciju S/Z*
- *usaglašen sa zakonima i međunarodnim ugovorima*
  - *adekvatan, rentabilan, dobrovoljno prihvaćen*
  - *izdat od nacionalnog tela za standardizaciju ...*

Standardi zaštite

- **Glavni nedostatak** :
- Ne postoji *jedinstven model najbolje prakse zaštite:*
  - različiti uticaji nacionalnih zakona i pravnih okvira
  - različite i brojne definicije *najbolje prakse zaštite*
  - *veliki broj sertifikacionih tela* i dr.
- **Da li je dobro imati jedinstven standard zaštite???**
- Model najbolje prakse zaštite - „*Hierarchy of Security*”
- Standardi ISO/IEC 27K serije daju **ŠTA** treba uraditi

Klasifikacija standarda zaštite



Eksterni (industrijski) standardi

- **Obuhvataju**:
  - *ISMS, menadžment rizika, obuku, evaluaciju,* ***C&A***
- **Obezbeđuju:**
  - *više testiranja u praksi, razmenu iskustava i rešenja*
- **Zahtevaju**:
  - *periodično usaglašavanje sa uspostavljenim kriterijumima*
- **Standardi *najbolje* prakse zaštite***:*
  - ***ISO/IEC 27001, 2, 3, 5,...;***
  - ***NIST SP 800 serije;***
  - ***ISF v.4.0, 2006...***

Interni standardi

- Specifični za organizaciju koja ih proizvodi i kontekst
- Jezgro *upravljačkog okvira zaštite* (**SMF**)
- Dodaju novu vrednost pomažu interpretaciju politike z.

Specifikacioni interni standardi:

– definišu sistem osnovnih kontrola zaštite **(k/z)**

Proceduralni interni standard:

– za opis procedura zaštite bez tehničkih detalja

– generički su i nisu specifični za IS

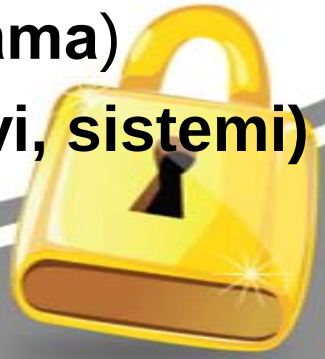
Standard *najbolje prakse zaštite*

***Definicija*:**

- *Dokumentovan, dostupan, efikasan, odgovarajući*
- *Sadrži široko prihvaćene strategije, pristupe, planove, taktike, procese, metodologije i aktivnosti zaštite*
- *Razvijen od strane kompetentnih entiteta i izvršen sa adekvatno obučenim personalom*
- *Uaglašen sa zakonima i regulativama*
- *Potvrđen kroz istraživanje, evaluaciju i praksu kao efikasan za zaštitu informacija na prihvatljivom nivou rizika*
- *Neprekidno se proverava i poboljšava u skladu sa promenama okruženja, tehnologija, pretnji, org. i sl*

Program *sistema najbolje prakse zaštite*

- *dokumentovan* i *pristupačan* (**dostupan**)
- *standardan* (**strategijski, taktički, na procesu i metodu**)
- *neprekidno poboljšavan* (**obuka, edukacija i sertifikacija**)
- *ponovljiv*, *efikasan i rentabilan* (**korisnost >troškova**)
- *efektivan* (**vodi do željenog cilja**)
- *skalabilan* (**adaptivan i fleksibilan, obuhvata plan VD**)
- *praćen i kontrolisan* (**monitorisan, obezbeđuje metriku**)
- *usaglašen* (**sa postojećim zakonima i regulativama**)
- *sveobuhvatan* (**kadrovi, procesi, politike, planovi, sistemi)**



Implementacija standarda zaštite

- **Obezbeđuje:**
  - *Interoperabilnost*
  - *upravljanje rizikom*
  - *izgradnju poverenja*
  - *smanjenje incidenata*
  - *borbu protiv kompjuterskog kriminala*
  - *usklađivanje prakse sa normativnim zahtevima*
  - *održavanje kontinuiteta poslovanja* i dr.

Relevantni standarda zaštite

- ***ISO/IEC*** i drugi:
  - **ISO/IEC 27001**, *ISMS*
  - **ISO/IEC 27002**, kontrole z.
  - **ISO/IEC 27005**, upravljanje R
  - **ISO/IEC 27006**, C&A
  - **ISO/IEC 15443**, tehnike zaštite
  - **ISO/IEC 21827** sazrevanja procesa zaštite
  - **ISO/IEC 15408**, („*Common Criteria*“) *Evaluation Criteria for IT Security (praktično* povučen 2005.*)*
  - *.....*

Standard ISO/IEC 27001:2013 (ISMS)

- **Obavezuje i usmerava pažnju na upravljanje s/z*:***
  - odgovornost i usaglašvanje prakse sa ISMS politikom
  - izbor k/z na osnovu procene rizika
  - zaštitu kritične **informacione imovine** organizacije …
  - *ISMS politiku* (**šta** treba da sadrži)
- **Ne obezbeđuje:**
  - izbor metodologije za procenu rizika
  - metriku zaštite
  - uputstvo za kreiranje i čuvanje podataka *za DF istragu*
  - *kako* se razvija i izrađuje politika zaštite

Standardi ISO/IEC 27002:2005 (2013)

- **Katalog U, O, T** *kontrola zaštite*
  - sadrži **11** (14) kategorija, **39** (**18**) sekcija i ukupno **133** **(114)** kontrole zaštite
  - svaka K/Z sadrži *cilj kontrole* i samu *kontrolu*
  - sugeriše **koje** K/Z treba uključiti za ublažavanja rizika
  - ne specificira **kako** ih implementirati i administrirati
  - *nije tehnički standard niti zavisi od tehnologije*

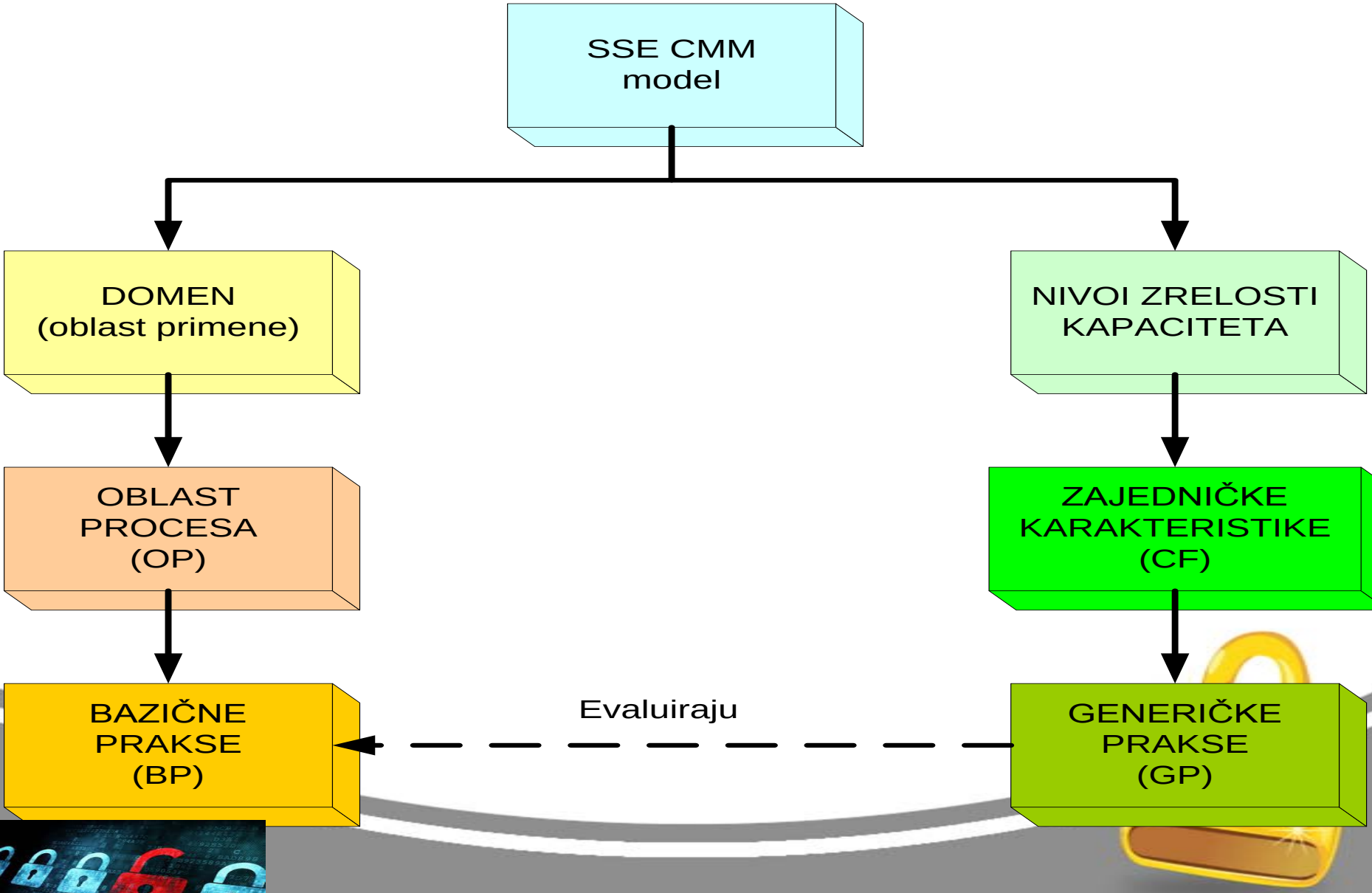
Relevantni standardi za evaluaciju S/Z

- **ISO/IEC 15443,** sve metode i sredstva za sistem kvaliteta, baziran na **pristupu**:
  - **kvalitetu procesa:**
    - *SSE-CMM, ISO 9000-3, ISO 9001, ISO/IEC 15504* itd.
  - **kvalitetu proizvoda/sistema:**
    - *CC/CEM, ITSEC/ITSEM, TCSEC/, ISO/IEC 9646*, *ISO/IEC 14598* itd.
  - **kvalitetu okruženja:**
    - *TCMM, ISO 13407* i dr.

ISO/IEC 21827 (2002.) (SSE - CMM)

- **Razvio SEI** (*SoftwareEngeneeringInstitute*), SAD, NSA (1996)
- **SSE-CMM v. 3 model/metod (objavljen 2007**):
  - **OP**: *SE, organizacione i projektne*
  - meri zrelost i kapacitete org. za izvršavanje OP zaštite
  - pretpostavlja: *zreli procesi i kapaciteti-dobar proizvod/SZ*
  - ima *sistemski* i *procesno* orijentisanu metriku
  - zreo proces postaje stabilan i predvidljiv
  - koristi se za evaluaciju i poboljšavanje procesa zaštite IS

Struktura SSE CMM



Standard ISO/IEC 15504

- Kompatibilan sa **CMM** koristi dimenzije procesa i kapaciteta
- Podržava sve procese i ima metriku zrelosti:
  - ***L0****: nekompletan proces*
  - ***L1****: izvršen proces*
  - ***L2:*** *upravljan proces*
  - ***L3****: uspostavljen proces (odgovara* ***ISO 9000*** *sertifikatu)*
  - ***L4****: predvidljiv proces*
  - ***L5:*** *optimizovan proces*
- Primenljiv za: *samo-, nezavisnu, neprekidnu i diskretnu procenu*
- Koristi se za **evaluaciju kriptografskih modula**

Primer: ostali standardi zaštite

1. ***Cobit*** (*Control Objectives for Information and Related Technology*) - opisuje metod nadzora i kontrole rizika,
2. ***ISO/IEC TR 13335*** standard za upravljanje zaštitom inf. i komunikacija
3. ***ITU*** (*International Telecommunications Union*) -za kom. podataka: X.25 X.400**,** X.500, X.800 i X.509 (DS u PKI)
4. ***ANSI*** - Nacionalna organizacija za standardizaciju SAD
5. ***NIST*** (*National Institute for Standards and Technologies*), *FIPS* za potrebe federalne vlade i industrije SAD
6. ***IETF i IEEE*** proizvele su standarde za specifične interesne zajednice, RFC (*Request for Comment*) koju objavljuje IETF

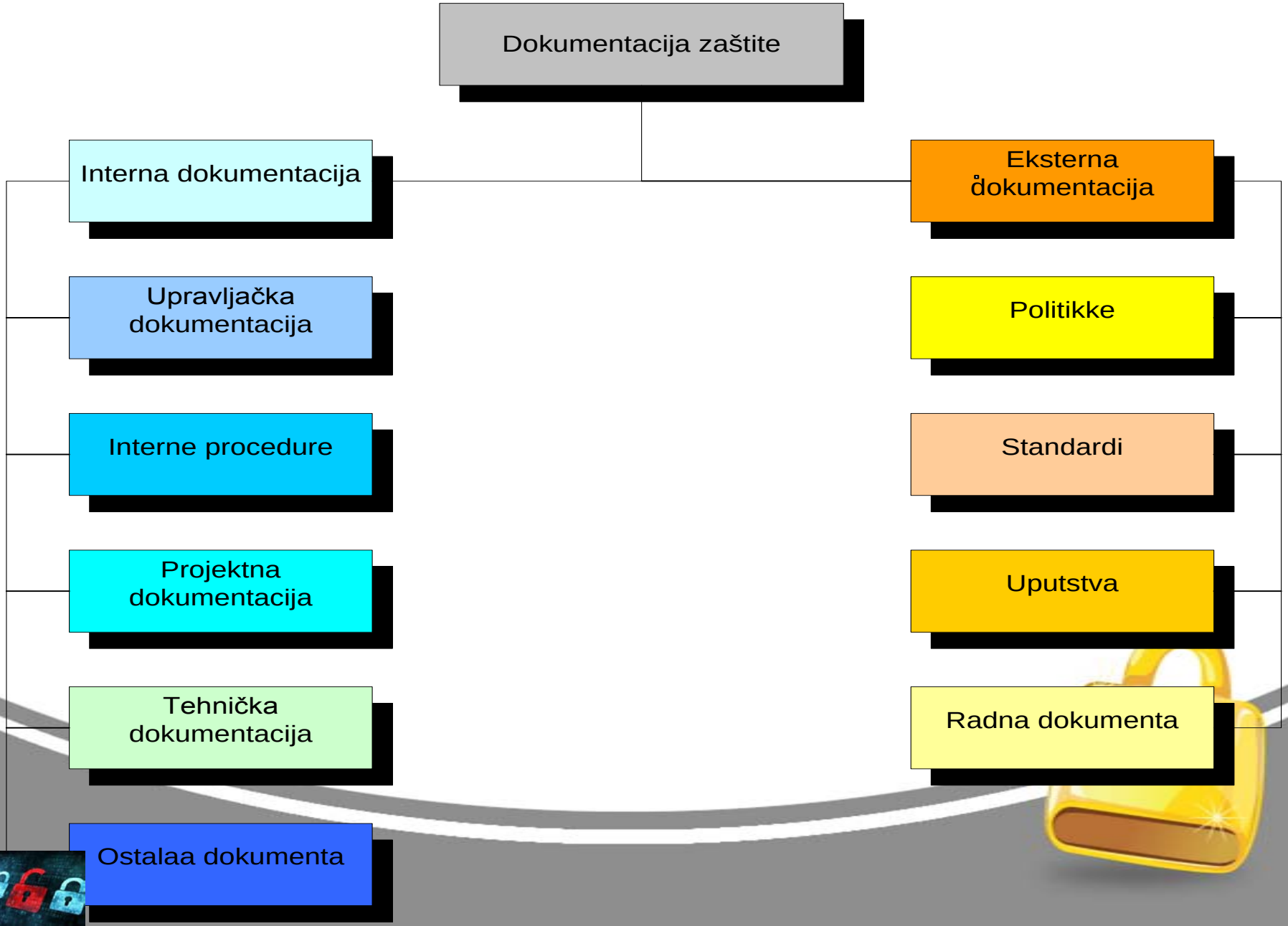
- Ključni dokument **RFC 1539** - uvod i reference u RFC dokumenta ostalih RFC sa detaljnijim informacijama

7. **ISF** (*Information Security Forum*) – standard najbolje prakse zaštite….

Normativni okvir zaštite informacija

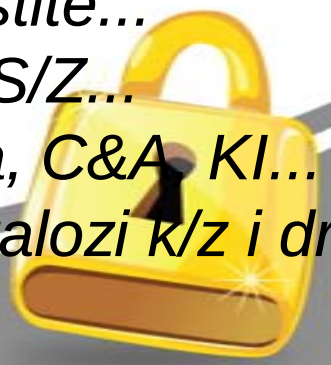
- **Normativni okvir (**zakoni, podzakonska akta...)
- **Nacionalni zakon za zaštitu informacija:**
  - obezbeđuje značajne funkcije osnovnog sloja zaštite:
    - *ističe značaj zaštite i strateškog istraživanja*
    - *zahteva obuku i obrazovanje i sankcioniše zloupotrebe itd*
  - podzakonski *pravni akti:*
    - *pravilnici* za PKI (*Public Key Infrastructure*), CA i DS itd.
- **ENISA** (*European Network and Information Security Agency):*
  - *ekspertsko telo EU za zaštitu informacija (od 2005.)*
  - *za razmenu informacija, znanja, najbolje prakse zaštite*
  - uključuje *zakon, podzakonska akta* i standarde zaštite

Klasifikacija dokumenata zaštite



Dokumentacija zaštite informacija ISO/IEC

- **Kriterijumi dobre dokumentacije zaštite**
  - *laka* za upotrebu/održavanje,*odgovarajuća* za ciljne korisnike
  - sadrži *tačne, bitne i ažurne* informacije
- **Interna:**
  - ***Upravljačka dokumentacija**: ugovor, plan, izveštaj, NDA*
  - ***Projektna dokumentacija**: npr. konfigurisanje firewall-a*
  - ***Interne procedure**: izveštavanja, adm. zaštite itd.*
  - ***Tehnička dokumentacija**: za uređaje zaštite, testove i sl.*
  - ***Ostala dokumenta**: materijal za obuku, instrukcije isl*.
- **Eksterna:**
  - ***Politika zaštite**: programska, ISMS, komp. Zaštite...*
  - ***Industrijski standardi**: ISMS, obuka, provera S/Z...*
  - ***Uputstva za zaštitu**: za upravljanje S/Z, obuka, C&A KI...*
  - ***Radna dokumenta**: kontrolne liste , uzorci, katalozi k/z i dr.*



Ključnu dokumenta zaštite

- **ISO/IEC 27K serija standarda*:***
  - *Politika zaštite informacija (ISMS politika)*
  - *Politike zaštite funkcionalnih komponenti*
  - *Procedure zaštite*
  - *Uputstva zaštite*
  - *Plan tretmana rizika ili Plan zaštite ...*

Osnovna ISMS dokumentacija

Uputstva za zaštitu

1. Za administratore i menadžere zaštite:

– pomoć u projektovanju i upravljanju S/Z

– sveobuhvatan i dovoljno detaljan

– sadrži uzorke, nstrukcije, upitnike, tabele i dijagrame

2. Za korisnike:

– orijentisan na određene grupe korisnika

– obrađuje određene komponente zaštite u delokrugu odgovornosti grupe/pojedinaca

Pregled i ažuriranje dokumenata zaštite

- **Od kritičnog značaja** su regularne provere:
  - *nezavisna provera 1 put/godišnje i češće*
  - *interna provera za korekciju i poboljšanje zaštite*
- **Provera promena** u IS/*SZ:*
  - *zahtevaju značajne promene u planu zaštite*
  - *zahtevaju promene u politici i procedurama zaštite*

Pitanja