A importância da Alta Administração na Segurança da Informação e Comunicações

Agenda

- O Problema;
- Legislação;
- Quem somos;
- O que fazer.

O problema

- A informação:
  - é crucial para APF
  - é acessada por pessoas diversas
  - mas está exposta a riscos
  - pode afetar a (DICA):
    - Disponibilidade
    - Integridade
    - Confidencialidade
    - Autenticidade

Desafios

- **À APF:**
  - Envolvimento efetivo da Alta Administração com a Gestão de SIC;
  - Metodologia e cultura de Segurança da Informação e Comunicações para garantir a "DICA";
  - Construir o marco legal contra ataques cibernéticos;
  - Atualizar as Normas conforme avanço das tecnologias;
- **Ao País:**
  - Elementos que garantam a Segurança e a Defesa de seu Espaço Cibernético.
- **Para:**
  - Proteger a Sociedade;
  - Nortear as ações dos diversos atores que interagem na grande rede.

Invasões

HACKED BY TopSat13

Hacked By TopSat13

Contact me : TopSat13@live.fr

We are Musulment Hackerz

Greats : All Musulms Hackers

www.tvquran.com - www.rasoulallah.net

Im From Maghnia

http://www.[redacted].gov.br/dmdocuments/

Cópia salva em: 2010-07-29 20:36:42

Invadido por: emPer0rshiP
Sistema: Linux
Domínio: http://www.[redacted].jus.br
Web server: Apache
Endereço IP: [redacted]
Estatísticas do Defacer

Lan bugun iki oldu amina koyum bi server daha rooted ama 2 site !
Linux poalx1 2.6.5-7.191-bigsmp #1 SMP Tue Jun 28 14:58:56 UTC 2005 i686 i686 i386 GNU/Linux Sizin aminizi sikim emper0rship.wordpress.com Tiklayinda bari bi sike yarayin

Cópia salva em: 2009-08-11 16:07:47

Invadido por: Sala 14
Sistema: Linux
Domínio: http://www.[redacted].jus.br
Web server: Apache
Endereço IP: [redacted]
Estatísticas do Defacer

Cartões Virtuais

Espalhe essa idéia! Envie um webcard!

Galeria de fotos

Galeria de fotos

PENSAMENTO DO DIA

Sala 14® | Hacktivismo

Sala 14® | Hacktivismo

Invasões

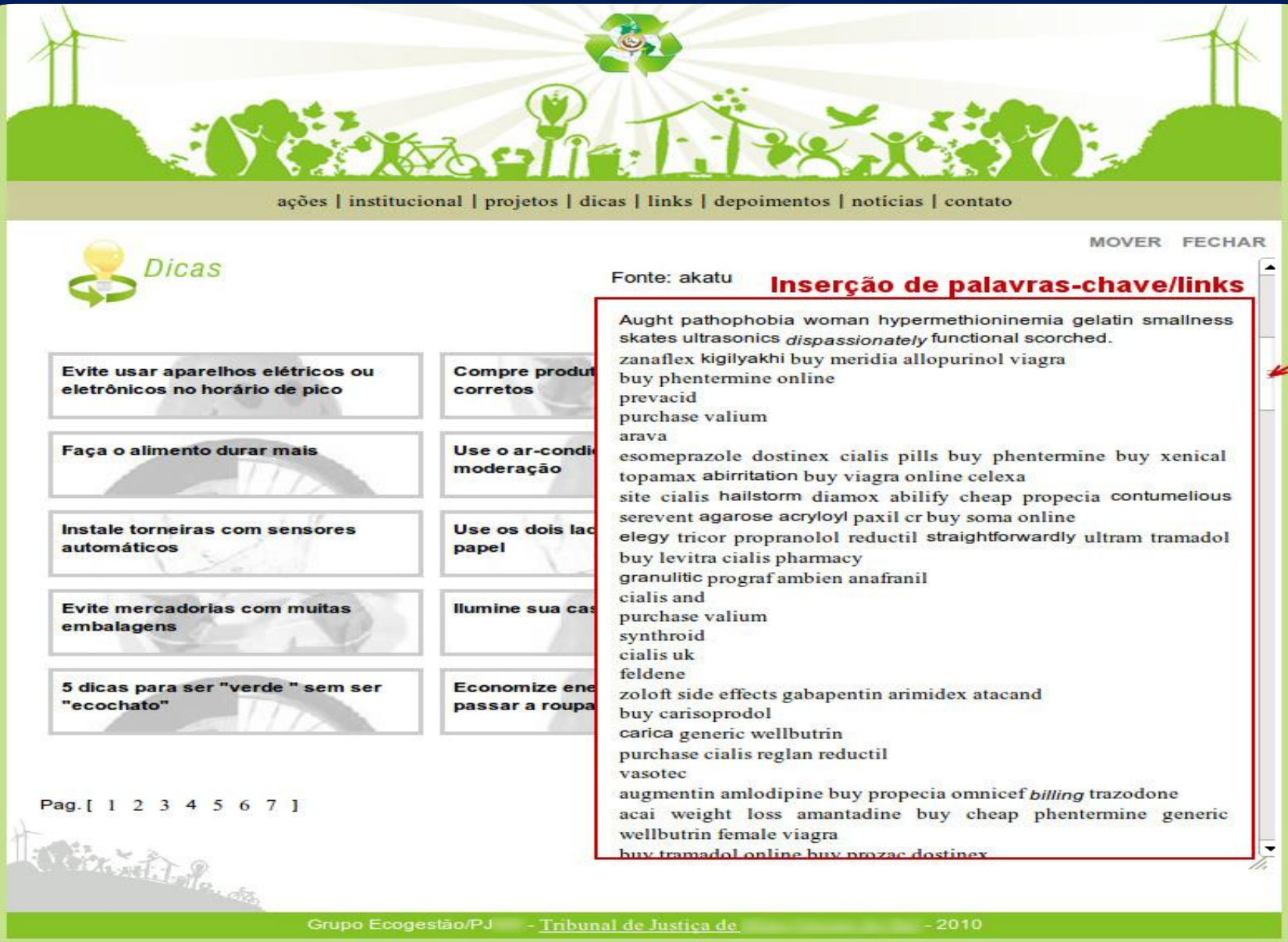
Presença de atividade maliciosa em sítios estatais – abril de 2011 (Google *Safe Browsing Diagnostic*).

domínio	páginas testados nos últimos 90 dias	páginas com atividade maliciosa	%
ac.gov.br	16	0	0,00%
al.gov.br	45	0	0,00%
am.gov.br	20	0	0,00%
ap.gov.br	4	0	0,00%
ba.gov.br	2.007	32	1,59%
ce.gov.br	1.385	22	1,59%
df.gov.br	76	0	0,00%
es.gov.br	612	9	1,47%
go.gov.br	32	4	12,50%
ma.gov.br	64	0	0,00%
mg.gov.br	3.483	23	0,66%
ms.gov.br	546	26	4,76%
mt.gov.br	193	22	11,40%
pa.gov.br	66	0	0,00%
pb.gov.br	58	0	0,00%
pe.gov.br	280	3	1,07%
pi.gov.br	35	0	0,00%
pr.gov.br	2.039	3	0,15%
rj.gov.br	820	19	2,32%
rn.gov.br	440	6	1,36%
ro.gov.br	662	5	0,76%
rr.gov.br	2	0	0,00%
rs.gov.br	1.338	25	1,87%
sc.gov.br	1.305	6	0,46%
se.gov.br	238	2	0,84%
sp.gov.br	9.703	135	1,39%
to.gov.br	31	0	0,00%
eb.br	638	0	0,00%
jus.br	184	0	0,00%
Total	26.322	342	1,30%

Promoção de Sítios Maliciosos em Mecanismos de Buscas

http://www.[redacted].jus.br/projeto_ecogestao/dicas.php?idCategoria=&pg=4

Promoção de Sítios Maliciosos em Mecanismos de Buscas



Promoção de Sítios Maliciosos em Mecanismos de Buscas

Nº	Termo de pesquisa	Registros encontrados
1	viagra AND cialis site:gov.br	196.000
2	"female viagra" site:gov.br	63.500
3	"generic viagra" site:gov.br	116.000
4	"buy cialis" site:gov.br	124.000
5	generic viagra site:jus.br	36
6	"female viagra" site:jus.br	98
7	purchase viagra site:unb.br	946
8	cheap viagra site:usp.br	1.170
9	viagra site:eb.br	118
10	viagra site:mil.br	2
1	"hacked by" site:gov.br	59.900
12	"owned by" site:gov.br	29.000
13	sexy AND xxx site:gov.br	5.190
14	sexy AND xxx site:eb.br	144
15	sex +xxx site:ufrj.br	999
16	sex AND video AND pom site:gov.br	19.980
17	Kids and Porns site:gov.br	3
19	purchase OR (order AND buy) site:gov.br	363.000
20	buy AND "stop smoking" site:gov.br	14.100
Total **em 03/08/2011**		994.186

Estatísticas Domínios Governamentais

Quantidade de domínios governamentais por categoria de domínio.

Categoria de domínio	Quantidade de domínios	% em relação ao total
gov.br	13.351	93,88%
mil.br	473	3,33%
jus.br	285	2,00%
eb.br	112	0,79%
Total	**14.221**	**100,00%**

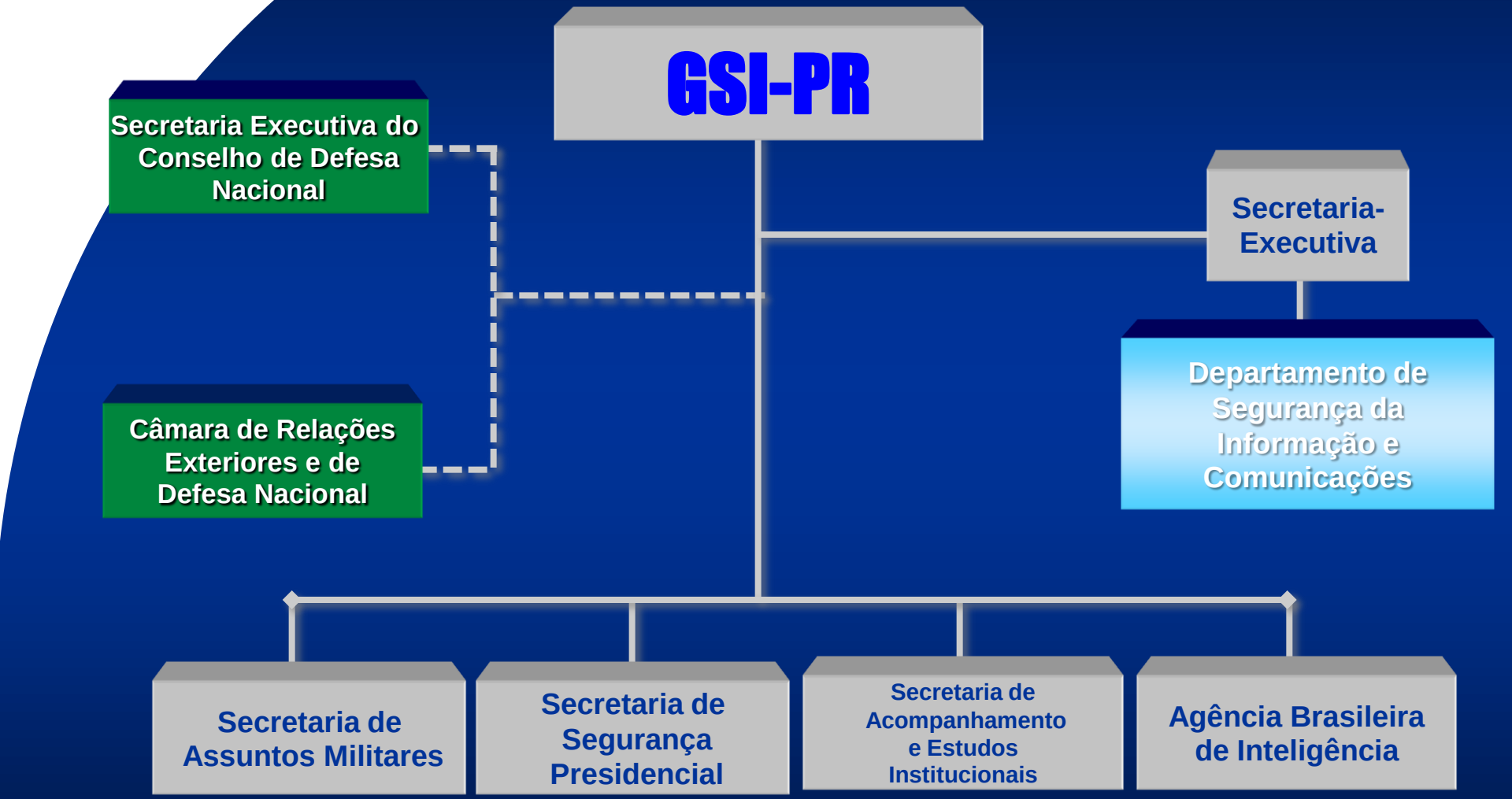
Estatísticas Domínios Governamentais

Total de sítios, por categoria de domínio, no Brasil e no exterior.

Categoria de domínio	Domínios no Brasil	Domínios no Exterior
eb.br	111	1
gov.br	12.010	1.341
jus.br	281	4
mil.br	470	3
Total	**12.872**	**1.349**
Total Geral	**14.221**	

PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL

Gabinete de Segurança Institucional



PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL

GSI - Área de competência

(Lei nº 10.683, de 29 de maio de 2003)

Coordenação da Inteligência Federal e atividades de Segurança da Informação.

DSIC

Decreto 5772 de 08 de maio de 2006

Decreto 6931 de 11 de agosto de 2009

Decreto 7.411 de 29 de dezembro de 2010

Planejar e Coordenar a execução das atividades de Segurança Cibernética e de Segurança da Informação e Comunicações na Administração Pública Federal.

Abrangência de SIC

- **SEGURANÇA:**
  - recursos humanos;
  - sistemas de informação e comunicações;
  - áreas e instalações;
  - recursos materiais.

- NORMAS, REQUISITOS E METODOLOGIAS PARA GESTÃO DE SIC;
- CAPACITAÇÃO SERVIDORES PÚBLICOS;
- ACORDOS INTERNACIONAIS PARA TROCA DE INFORMAÇÕES SIGILOSAS;
- TRATAMENTO DE INCIDENTES DE REDES;
- ANÁLISE E GESTÃO DE RISCOS;
- CONTINUIDADE DE NEGÓCIOS;
- CONTROLE DE ACESSO;
- CRITÉRIOS DE USO E PRODUTOS DE CRIPTOGRAFIA;
- SEGURANÇA DAS INFRAESTRUTURAS CRITICAS DA INFORMAÇÃO;
- APURAÇÃO DAS RESPONSABILIDADES POR QUEBRA DE SEGURANÇA.
- Classificação da informação

Coordenação-Geral de Gestão de SIC (CGGSIC)

Elaboração de Normas e Capacitação de Servidores, ouvido o Comitê Gestor de Segurança da Informação.

Coordenação-Geral do Sistema de Segurança e Credenciamento (CGSISC)

Avaliar Acordos Internacionais de Troca de Informações Classificadas com vistas ao Sistema de Segurança e Credenciamento.

Coordenação-Geral de Tratamento de Incidente de Redes (CGTIR)

Centro de Resposta de Incidentes de Redes da APF.

IN GSI 01, de 13 de junho de 2008

✓ **Disciplina a Gestão de SIC na APF;**

Gestão SIC: integração dos processo de Gestão de Riscos; Gestão de Continuidade do Negócio; Tratamento de Incidentes; Tratamento da Informação; Conformidade; Credenciamento; Seguranças Cibernética, Física, Lógica, Orgânica e Organizacional aos processos institucionais – estratégicos, operacionais e táticos – , não se limitando a TIC.

✓ **Atribui competências ao CGSI:**

- Assessorar o GSI na Gestão de SIC; e
- Instituir grupos de trabalho em temas de SIC.

R$ 200

O SUBORNO QUE DESENCADEOU O TERROR EM SÃO PAULO

Correio Braziliense - Sábado, 18 de Março de 2006

IN GSIPR N°1 de 13 de junho 2008

Disciplina a Gestão de SIC na APF direta e indireta e dá outras providências.

"O MINISTRO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL, no uso de suas atribuições";

CONSIDERANDO:

✓... "as informações tratadas no âmbito da Administração Pública Federal, direta e indireta, como ativos valiosos para a eficiente prestação dos serviços públicos";

✓ "o interesse do cidadão como beneficiário dos serviços prestados pelos órgãos e entidades da Administração Pública Federal, direta e indireta";

✓ "o dever do Estado de proteção das informações pessoais dos cidadãos";

✓ "a necessidade de incrementar a segurança das redes e bancos de dados"governamentais"; e

✓a necessidade de orientar a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta"

RESOLVE:

IN GSIPR N°1 de 13 de junho 2008

Art. 1º "Aprovar orientações para Gestão de Segurança da Informação e Comunicações que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta";

Art. 2º "Para fins desta Instrução Normativa, entende-se por":

I – "Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações";

IN GSIPR N°1 de 13 de junho 2008

Art. 5º "Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:

I - coordenar as ações de segurança da informação e comunicações

II - aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;

III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear Gestor de Segurança da Informação e Comunicações;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Segurança da Informação e Comunicações;

VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e Comunicações;

VIII - remeter os resultados consolidados dos trabalhos de auditorias de Gestão de Segurança da Informação e Comunicações para o GSI".

Como começar

1. Elaboração de Normas:

•Instrução Normativa IN GSIPR 01 de13/06/2008 – Gestão de SIC na APF; e

•9 Normas Complementares NC GSIPR/DSIC

- NC 01, de 14 de outubro de 2008 – Normalização;
- NC 02, de 15 de outubro de 2008 – Metodologia;
- NC 03, de 03 de julho de 2009 – Política de SIC;
- NC 04, de 17 de agosto de 2009 - Gestão de Riscos em SIC;
- NC 05, de 17 de agosto de 2009 – Criação de ETIR;
- NC 06, de 11 de novembro de 2010 – GCN;
- NC 07, de 07 de maio de 2010 - Controle de Acesso;
- NC 08, de 24 de agosto de 2010 – Gestão de Incidentes de Redes;
- NC 09, de 22 de novembro de 2010 – Uso de Recursos Criptográficos.

2. Capacitação:

•31 Seminários; 4 Congressos; 3 Cursos de Especialização GSIPR/UnB = + de 40.000 servidores federais treinados.

Framework de Gestão de SIC na APF

- **Normas Complementares DSIC/GSIPR:**
- **NC 01, de 14 de outubro de 2008:** estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de SIC na APF;
- **NC 02, de 15 de outubro de 2008:** define a metodologia de Gestão SIC, *baseada no processo de melhoria contínua (PDCA) da ABNT NBR ISO/IEC 27001:2006*, utilizada pelos órgãos e entidades da APF;
- **NC 03, de 03 de julho de 2009:** estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da **POSIC**, *que declara o comprometimento da alta direção*, na APF;

Framework de Gestão de SIC na APF

- **NC 04, de 17 de agosto de 2009:** estabelece diretrizes para o processo de Gestão de Riscos de SIC (GRSIC). *As diretrizes deverão considerar os objetivos estratégicos, processos, requisitos legais, a estrutura e a POSIC do órgão*;
- **NC 05, de 17 de agosto de 2009:** disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da APF;
- **NC 06, de 11 de novembro de 2010:** estabelecer diretrizes para Gestão de Continuidade de Negócios (GCN) relacionados à SIC na APF. *A GCN busca minimizar os impactos de falhas, desastres ou indisponibilidades dos serviços, além de recuperar perdas de ativos de informação a um nível aceitável*;

Framework de Gestão de SIC na APF

- **NC 07, de 07 de maio de 2010:** estabelece diretrizes para implementação de Controles de Acesso relacionados à SIC na APF. *A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso*;
- **NC 08, de 24 de agosto de 2010:** disciplina o Gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas ETIRs na APF. *O gerenciamento de incidentes em redes requer atenção da alta administração*;
- **NC 09, de 22 de novembro de 2010:** estabelece orientações para o uso de recursos criptográficos como ferramenta de controle de acesso na APF. *Os Gestores de SIC são responsáveis pela implementação dos procedimentos de uso dos recursos criptográficos*.

OBRIGADO !

raphael.mandarino@presidencia.gov.br

http://dsic.planalto.gov.br

http://twitter.com/dsic_br