Processo de Trabalho: **IDENTIFICAR E TRATAR VULNERABILIDADES NOS ATIVOS DE TIC**	PAT 01	Revisão 00
Atividade: **GERIR AS VULNERABILIDADES**		

Descrição das Tarefas, em Sequência	
1	O Serviço de Controle de Incidentes e Gestão de Vulnerabilidade do Gabinete da Presidência (GABPRES/SECIS) recebe a lista das vulnerabilidades identificadas e encaminha ao Serviço de Riscos e Compliance do Gabinete da Presidência (GABPRES/SERIC).
2	O SERIC faz a classificação e a priorização das vulnerabilidades com base na avaliação de severidade fornecida pelas ferramentas, quando disponível, ou por meio de uma matriz de riscos, considerando o impacto potencial e a probabilidade de exploração, definindo assim o SLA.
3	O SERIC avalia as vulnerabilidades e identifica tanto as novas ocorrências quanto as que já estão em tratamento. No caso de novas, encaminha-as para o SECIS. As que já estão em tratamento são acompanhadas conforme o SLA.
4	**Para Novas Vulnerabilidades:**
5	As vulnerabilidades são analisadas pelo SECIS e endereçadas com a descrição do CVE (Common Vulnerabilities and Exposures) - sistema mundial de identificação e catalogação de vulnerabilidades de segurança em softwares e hardwares, a fim de facilitar a identificação e permitir que os departamentos e as fábricas tenham acesso às recomendações de correção.
6	Todas as informações geram um plano de ação com o SLA definido.
7	O SECIS solicita ao SERIC o cadastro da vulnerabilidade na ferramenta de Gestão de Riscos (GRC) anexando o plano de ação, para acompanhamento.
8	O SECIS encaminha à área responsável, a vulnerabilidade para tratamento.
9	A área responsável pela vulnerabilidade analisa se a vulnerabilidade pode ser tratada.
10	Se for possível o tratamento da vulnerabilidade, a área responsável implementa as ações para correção e informa ao SECIS.

Processo de Trabalho: **IDENTIFICAR E TRATAR VULNERABILIDADES NOS ATIVOS DE TIC**	PAT 01	Revisão 00
Atividade: **GERIR AS VULNERABILIDADES**		

11	Se não for possível o tratamento da vulnerabilidade, a área responsável deverá informar ao SECIS, para que seja criado um Plano de Mitigação.
12	O SECIS acompanha o tratamento de vulnerabilidades junto às áreas responsáveis, auxiliando nas tratativas sempre que necessário.
13	O SERIC monitora o SLA de cada vulnerabilidade e entra em contato com a área para negociação de novo prazo, caso o prazo do SLA não seja cumprido.
14	Quando o tratamento é implementado, o SECIS realiza uma verificação para validação.
15	Caso seja confirmada a correção, o SERIC fecha o risco na ferramenta de GRC.
16	**Para Vulnerabilidades já encaminhadas para tratamento:**
17	O SERIC verifica o prazo de atendimento (SLA) para a correção da vulnerabilidade
18	Se o SLA está dentro do prazo, o SERIC mantém o acompanhamento do tratamento.
19	Se o SLA não foi cumprido e a vulnerabilidade ainda não foi corrigida, o SERIC realiza o contato com a área responsável para entender o motivo e renegociar novo prazo.
20	Caso seja possível tratar a vulnerabilidade, o motivo do atraso é registrado na ferramenta de GRC pelo SERIC e um novo SLA é estabelecido.
21	SECIS altera o plano de ação, incluindo o novo SLA acordado e encaminha novamente à área responsável para tratamento.
22	Se a área responsável informar que não será possível a correção da vulnerabilidade, será necessária a implementação de um Plano de Mitigação.
23	**Elaborar e Implementar Plano de Mitigação:**
24	O SECIS cria um Plano de Mitigação com a área responsável para as vulnerabilidades que não podem ser tratadas.

Processo de Trabalho: **IDENTIFICAR E TRATAR VULNERABILIDADES NOS ATIVOS DE TIC**	PAT 01	Revisão 00
Atividade: **GERIR AS VULNERABILIDADES**		

25	O Plano de Mitigação é incluído na ferramenta de GRC pelo SERIC e definido um SLA.
26	O SERIC acompanha o prazo do SLA e ao vencer o prazo, verifica com a área responsável o motivo do atraso.
27	Caso o Plano de Mitigação não tenha sido implementado, o SECIS verifica a necessidade de ajuste do Plano de Mitigação e atribui um novo SLA.
28	A área responsável implementa as ações do Plano de Mitigação e informa ao SECIS.
29	O SERIC atualiza a ferramenta de GRC e o risco é mitigado.