PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL
SECRETARIA DE COORDENAÇÃO DE SISTEMAS
DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

REQUISITOS MÍNIMOS DE SEGURANÇA DA INFORMAÇÃO AOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Brasília, DF

Julho, 2017

1. INTRODUÇÃO

Os presentes requisitos têm a finalidade de elevar e aprimorar a segurança da informação no âmbito da Administração Pública Federal (APF), sendo constituídos por uma coletânea dos principais procedimentos extraídos dos normativos exarados pelo Departamento de Segurança da Informação e Comunicações do GSI/PR, com alguns complementos e atualizações.

Os itens aqui descritos foram influenciados em substantiva proporção pela crescente incidência de ataques cibernéticos, e por constantes ameaças à segurança da informação, que passaram a requerer dos gestores do tema atenção, dedicação e estudo muito maiores e abrangentes.

Tais requisitos, entretanto, não são exaustivos, estando sujeitos a sugestões de melhoria e alterações de forma e conteúdo, caso necessário. Com o fim de facilitar a leitura, estão divididos em dois tópicos, sendo um de orientações gerenciais, voltadas aos gestores de equipes, de sistemas e coordenadores, e outro de orientações técnicas, dirigidas aos quadros eminentemente técnicos dos órgãos da APF.

Faz-se, ainda, necessário ressaltar que a consolidação dos presentes requisitos mínimos não exime o agente público de conhecer e cumprir as instruções normativas e suas respectivas normas complementares, expedidas pelo DSIC/GSI/PR.

2. ORIENTAÇÕES DE SEGURANÇA DA INFORMAÇÃO NOS AMBIENTES FÍSICO E VIRTUAL

2.1. Orientações Gerenciais

- Todos os funcionários, contratados, terceirizados e outros agentes que utilizam os recursos de rede são responsáveis pela segurança, zelo e bom uso das informações às quais têm acesso, sejam elas do próprio governo, do cidadão ou de outro órgão.

- As informações e os recursos de TI para acesso à rede de órgão da APF e seus recursos agregados devem ser disponibilizados, única e exclusivamente àqueles que necessitem deles para o exercício de suas funções, devendo ser disponibilizados e utilizados apenas para o exercício profissional.

- Todas as instalações e equipamentos devem ser protegidos contra acessos não autorizados. Os órgãos devem implementar mecanismos de proteção que impeçam acesso indevido aos ativos de informação e às áreas em que se encontram, como por exemplo, estações de trabalho com identificação de usuário e senha, os quais são pessoais e intransferíveis.

- Os usuários devem manter em absoluto sigilo as suas senhas, de forma que somente eles possam reproduzi-las. Os órgãos deverão orientar os usuários na escolha de senhas de elevado grau de segurança, que mesclem caracteres alfanuméricos e especiais, podendo haver letras maiúsculas e minúsculas.

- Os acessos aos dados e informações devem ser registrados, de modo que a qualquer momento estejam disponíveis as informações sobre acesso ou tentativas de acesso, frustradas ou não.

- Os órgãos devem estabelecer mecanismos de limites ao número de tentativas frustradas, que levem ao bloqueio da estação de trabalho.

- É recomendado que os órgãos tenham suas próprias políticas e normas de segurança claras e objetivas, revistas e divulgadas regularmente, com base nas diretrizes estabelecidas nos normativos do DSIC/GSI/PR, para orientar a correta utilização dos recursos computacionais em suas redes.

- Os órgãos devem exigir a assinatura de Termos de Responsabilidade (ou outro documento semelhante) em que o usuário dê ciência sobre os regulamentos a que está sujeito. No caso de terceirizados, os órgãos devem colocar cláusulas de segurança da informação em seus contratos.

- Toda informação deve ser protegida para que não seja alterada, acessada ou eliminada indevidamente.

- Toda informação não mais necessária deve ser seguramente descartada, de maneira que impeça a recuperação não autorizada.

- Toda informação custodiada pelos órgãos deve possuir cópia de segurança (backup) e ser guardada em local protegido, compatível com o grau de segurança necessário. Processos regulares de testes de *restore* são recomendados.

- Ambientes críticos devem ter planos de contingência ou continuidade de negócios definidos, revisados e testados periodicamente.

- Nenhuma informação crítica pode sair dos ambientes dos órgãos sem a expressa autorização do proprietário da informação. As formas de transporte dessas saídas de informação, sejam elas eletrônicas ou não, devem considerar proteção proporcional à criticidade da informação, como por exemplo, utilizando criptografia ou transporte seguro.

- Todos os dispositivos utilizados para a proteção, manutenção da integridade, disponibilidade e confidencialidade das informações devem ser considerados de absoluto sigilo, sendo, portanto, proibida a sua divulgação a pessoas não autorizadas ou a terceiros.

- Todo e qualquer programa de computador utilizado deve ser de propriedade do órgão, ou deve estar devidamente licenciado pelo proprietário, devendo estar sempre atualizado, e atender aos padrões de segurança e homologação, bem como à compatibilidade e conectividade com a arquitetura existente na Rede de órgão da APF.

- É de responsabilidade do órgão promover a filtragem de acessos indevidos provenientes de suas redes, com destino a outra(s) rede(s) de outros órgãos, ou para a Internet. Esses acessos indevidos podem ser gerados por ataques direcionados, códigos maliciosos (*malware*) e ataques de negação de serviço (DDoS), dentre outros.

- Todos os agentes públicos têm a responsabilidade de contribuir para a melhoria dos níveis de segurança da informação.

- É obrigação dos agentes públicos notificar imediatamente à administração da rede qualquer ponto de vulnerabilidade, irregularidade ou descumprimento dos requisitos de segurança estabelecidos pelo órgão.

- O órgão deve possuir uma Política de Segurança da Informação institucionalizada.

- O órgão deve possuir um Comitê de Segurança da Informação formalmente constituído.

- O órgão deve possuir um Gestor de Segurança da Informação nomeado.

- O órgão deve possuir uma Equipe de Tratamento e Respostas de Incidentes de Redes Computacionais em conformidade com os normativos do DSIC/GSI/PR.

- O órgão deve possuir uma Política de Controle de Acesso físico e lógico.

- O órgão deve possuir uma Política de Cópias de Segurança das Informações do órgão (backup).

- O órgão deve possuir um mapeamento e inventário de ativos de informação.

- O órgão deve realizar a gestão dos riscos que possam impactar a segurança da informação.

- O órgão deve notificar ao Centro de Tratamento de Incidentes de Redes de Governo (CTIR Gov) todos os incidentes de segurança computacionais nele ocorridos, de acordo com as Normas Complementares do DISC/GSI/PR.

- O órgão deve prever, nos processos de elaboração dos termos de referência para contratação de serviços de TI, cláusulas que levem à máxima proteção das informações a cargo da Administração Pública Federal, que a resguardem de comprometimentos em termos de segurança da informação e que reduzam o risco contratual.

- O órgão deve fortalecer internamente a cultura de segurança da informação, por meio de campanhas e ações regulares de sensibilização e disseminação de boas práticas, como palestras e worshops.

2.2. Orientações Técnicas

- Em sítios dos órgãos, todas as páginas que lidem com dados sensíveis devem trafegar em páginas conhecidas como "conexão segura", ou seja, as que usam o protocolo HTTPS – SSL (*Secure Sockets Layer*).

- Manter os desenvolvedores sempre atualizados com relação às novas vulnerabilidades e formas de proteção.

- Nunca armazenar usuários e senhas ou chaves criptográficas de sua aplicação no código fonte. Procurar utilizar serviços de autenticação, como o RADIUS, ou criptografar estes dados.

- Nunca permitir que a sua aplicação receba dados de usuários e senhas em texto claro. Utilize sempre o protocolo SSL.

- Estabelecer uma política de senhas para a sua aplicação de acordo com as seguintes regras mínimas:
  - comprimento mínimo de 8 caracteres.
  - obrigatoriedade de que a senha seja composta de letras, números e caracteres especiais.
  - obrigatoriedade de que o usuário, ao compor uma nova senha, não utilize nenhuma das quatro senhas anteriores.
  - número máximo de três tentativas frustradas.

- Não enviar a senha por e-mail nos casos em que o usuário execute a função "esqueci minha senha". Procurar usar mecanismos como o de pergunta secreta.

- Não armazenar cookies com o usuário e a senha, mesmo que criptografados, na estação do usuário.
- Certificar-se de que a função de "*logout*" de sua aplicação realmente encerra completamente a sessão.
- Inserir um botão de "*logout*" em cada uma das páginas de seu site.
- Conceder ao usuário de serviço de sua aplicação somente os acessos mínimos para o seu funcionamento. Nunca o definir como "*root*", "administrador" ou "sa".
- Desenvolver permissões de acesso de acordo com cada funcionalidade da aplicação e não por menus.
- Implementar mecanismos de validação da entrada de dados em sua aplicação impedindo, que seja possível, a inserção de dados de um tamanho ou tipo (numérico, alfanumérico, data/hora, etc.) que contrarie a regra de negócio estabelecida no sistema.
- Implementar mecanismos de geração de logs, sobretudo para as transações críticas.
- Armazenar os logs em arquivos ou bancos de dados com acesso disponível somente às equipes de infraestrutura.
- Realizar o tratamento de erros impedindo a ocorrência de mensagens de erro com origem no sistema de banco de dados ou no *webserver*.
- Não armazenar informações de produção nos ambientes de desenvolvimento e homologação.
- Remover todas as informações e contas de usuário de testes ao migrar o sistema para o ambiente de produção.
- Estabelecer procedimentos, com periodicidade no mínimo anual, de teste de intrusão com foco na tentativa de exploração de vulnerabilidades em aplicações web.
- Eliminar as vulnerabilidades reportadas em, pelo menos, um mês após a detecção.
- Utilizar firewalls para segregar as redes do ambiente. Evite usar roteadores para realizar esta função.
- Procurar utilizar firewalls com a função de "*stateful inspection*".
- Analisar o desenho de sua rede criticando se os dispositivos (servidores, *switches*, etc,) estão devidamente agrupados em redes específicas de acordo com a sua importância para o negócio. Caso estes ativos não estejam segregados desta maneira, considerar separá-los. Essa atividade cria zonas de segurança por função, o que limita o alcance de um possível ataque.
- Implementar uma DMZ com o objetivo de abrigar todos os dispositivos expostos à internet. Limitar todo o tráfego de entrada somente para a DMZ.
- Concentrar os servidores de banco de dados em uma rede segregada, nunca os deixar expostos à internet.
- Segregar, por meio de firewalls, os ambientes de desenvolvimento, homologação e produção.

- Estabelecer quais são as portas permitidas para a comunicação entre seus dispositivos e as documentar. Essa atividade aumenta o controle e torna formal qual tipo de comunicação é permitida em seu ambiente.

- Evitar o uso de portas de comunicação reconhecidamente consideradas como vulneráveis, como TELNET e FTP.

- Preferir soluções com criptografia como SFTP e SSH.

- Definir um processo formal para a manutenção e alteração de regras nos firewalls. Esse processo deve contemplar uma solicitação de mudança para cada regra com a aprovação de pelo menos um gestor.

- Caso possua redes sem fio em seu ambiente, segrega-las por meio de firewall concedendo somente os acessos necessários para os equipamentos com origem nestas redes.

- Configurar os pontos de acesso wireless para usar somente o padrão de criptografia de autenticação WPA2 com chaves longas.

- Nunca utilizar o padrão de criptografia de autenticação WEP.

- Proibir qualquer acesso originado na Internet que tenha como destino algum equipamento da rede interna.

- Utilizar o mascaramento de IP (*Network Address Translation* - NAT) para todo o tráfego de saída para Internet.

- Não utilizar senhas padrão de fábrica em nenhum dos equipamentos.

- Configurar os dispositivos de rede para gerar logs de todos os eventos realizados com privilégios administrativos.

- Configurar os dispositivos de rede para gerar logs de todos os eventos cuja tentativa de acesso resultou em falha.

- Configurar os logs para manter os dados de data/hora do evento, identificação do usuário, tipo de evento, indicação de sucesso ou falha e a indicação de qual componente foi alterado ou sofreu uma tentativa de alteração.

- Centralizar os logs dos dispositivos de rede e servidores em um servidor com esta função.

- Desabilitar a função PROXY-ARP em roteadores, evitando a possibilidade obtenção não autorizada de informações do dispositivo.

- Desabilitar a função *SOURCE-Routing* em roteadores, evitando a possibilidade de inserção não autorizada de rotas nos dispositivos.

- Utilizar obrigatoriamente a criptografia SSL V3, impedindo a conexão por meio do uso de versões antigas do SSL. Isso é aplicado por meio da alteração da configuração de seu *Webserver*.

- Somente utilizar certificados digitais de autoridades certificadoras válidas.

- Monitorar a validade do certificado digital e buscar adquirir um novo com antecedência à expiração do certificado instalado.

- Somente administrar dispositivos utilizando protocolos com criptografia como SSH.

- Somente realizar a troca de arquivos entre dispositivos utilizando protocolos com criptografia como SFTP.

3. ORIENTAÇÕES DE SEGURANÇA DA INFORMAÇÃO RELATIVAS AO CREDENCIAMENTO DE SEGURANÇA

Credenciamento de Segurança é o processo utilizado para habilitar órgão ou entidade pública ou privada ou para credenciar pessoa, para o tratamento de informação classificada, conforme dita o inciso IV do art. 2º da Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013. (Disponível em: <http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr2.pdf>).

3.1. Definição de Habilitação de Segurança de Órgão e Entidade Privada

Habilitação de Segurança é a condição atribuída a um Ministério ou Órgão Público, de nível equivalente, ou a uma entidade pública ou privada, que lhe confere a aptidão para tratar a Informação Classificada em determinado grau de sigilo.

Tratamento da Informação Classificada é o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

Isso posto, seguem os requisitos mínimos para Habilitação de Segurança de Órgão Público ou Entidade Privada para o Tratamento da Informação Classificada.

3.1.1. Requisitos Mínimos para Órgão de Registro Nível 1 (ORN 1)

Somente os Ministérios, ou Órgãos Públicos de nível equivalente, que identificarem a necessidade de Tratamento de Informações Classificadas, em qualquer grau de sigilo, deverão habilitar-se como ORN 1, devendo seguir o previsto no item 6 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013. (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >).

- Ser um Ministério, ou Órgão Público de nível equivalente;

- Ter necessidade em seus processos internos de tratar Informações Classificadas, em qualquer grau de sigilo, produzidas por ele próprio ou recebidas de outro ente público ou privado que mantenha vínculo;

- Ter Habilitação de Segurança como Órgão de Registro Nível 1 (ORN 1), na forma do item 6 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013. (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >);

- Possuir um Gestor de Segurança e Credenciamento (GSC) Titular e um Suplente, conforme itens 6.2 e 6.4.1 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em:

<http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >) e inciso VII do art. 2º e 17 da Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013. (Disponível em: <http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr2.pdf>);

- Ter o primeiro Posto de Controle (PC) do ORN 1 habilitado, na forma do item 8 da NC01/IN02/NSC/GSI/PR, de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >);

- Realizar Processo de Segurança para concessão de Credencial de Segurança de pessoas naturais, na forma do item 5 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >);

- Possuir servidor público ocupante de cargo efetivo ou militar de carreira, com competência profissional comprovada para atuar na área de inteligência, ou policial ou por perito criminal, ou ainda, conforme o caso, profissionais de saúde, a fim de emitirem pareceres técnicos específicos desta área, a critério do responsável pelo relatório da investigação, na forma do item 5.5.2.5 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >) ou do Parágrafo único do art. 8º do Decreto 7.845, de 14 de novembro de 2012 (disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>);

- Habilitar ORN 2 para o Tratamento da Informação Classificada, na forma do item 7 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >);

- Habilitar entidade privada para o Tratamento da Informação Classificada; e

- Habilitar os demais PC, do ORN 1 e do ORN 2 e de entidades privadas, após sua habilitação de Segurança, na forma do item 8 da NC01/IN02/NSC/GSI/PR, de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >).

3.1.2. Requisitos Mínimos para Habilitação Órgão de Registro Nível 2 (ORN 2)

Somente os Órgãos e entidades públicas (ORN 2) vinculadas a um Ministério, ou Órgão Público de nível equivalente (ORN 1), que identificarem ou que seja identificada pelo ORN 1, com a qual esteja vinculada, a necessidade de Tratamento de Informações Classificadas, em qualquer grau de sigilo, deverão habilitar-se como ORN 2, devendo seguir o previsto no item 7 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013. (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >).

- Ser um Órgão ou entidade pública vinculada a um Ministério, ou Órgão Público de nível equivalente habilitado como ORN 1;

- Ter necessidade em seus processos internos de tratar Informações Classificadas, em qualquer grau de sigilo, produzida por ele próprio ou recebida de outro ente público ou privado;

- Ter Habilitação de Segurança como Órgão de Registro Nível 2 (ORN 2), na forma do item 7 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >);

- Possuir um Gestor de Segurança e Credenciamento (GSC) Titular e um Suplente, conforme itens 7.2 e 7.4.1 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >) e inciso VII do art. 2º e 17 da Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013 (Disponível em: <http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr2.pdf>);

- Ter, no mínimo, 1 (um) Posto de Controle (PC) do ORN 2 habilitado pelo ORN 1 com o qual mantenha vinculo, na forma do item 8 da NC01/IN02/NSC/GSI/PR, de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >);

- Realizar Processo de Credenciamento de Segurança de pessoas naturais sob sua responsabilidade, na forma do item 5 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >); e

- Possuir servidor público ocupante de cargo efetivo ou militar de carreira, com competência profissional comprovada para atuar na área de inteligência, ou policial ou por perito criminal, ou ainda, conforme o caso, profissionais de saúde, a fim de emitirem pareceres técnicos específicos desta área, a critério do responsável pelo relatório da investigação, na forma do item 5.5.2.5 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >) ou do Parágrafo único do art. 8º do Decreto 7.845, de 14 de novembro de 2012 (disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>).

3.1.3. Requisitos Mínimos para Habilitação de Segurança de Entidade Privada

A entidade privada será habilitada por um ORN 1, a fim de tratar informações classificadas com a própria ORN 1 ou com os seus Órgãos e entidades públicas vinculadas (ORN 2), seguindo o previsto no item 9 da NC01/IN02/NSC/GSI/PR, de 2013. (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >).

- Possuir um Gestor de Segurança e Credenciamento (GSC) Titular e um Suplente, conforme itens 9.3 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >) e inciso VII do art. 2º e 17 da Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013 (Disponível em: <http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr2.pdf>);

- Ter, no mínimo, 1 (um) Posto de Controle (PC) habilitado pelo ORN 1 com o qual mantenha vinculo, na forma do item 8 da NC01/IN02/NSC/GSI/PR, de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >);

- Apresentar prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ) atualizado;

- Possuir ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

- Ter o organograma atualizado ou documento que identifique os reais controladores da empresa;

- Apresentar Certidão Negativa de Débitos de Tributos e Contribuições Federais (Receita Federal);

- Apresentar certidão quanto à Dívida Ativa da União (Procuradoria-Geral da Fazenda Nacional);

- Apresentar Certidão Negativa de Débitos (INSS);

- Apresentar certidão de regularidade do FGTS (Caixa Econômica Federal);

- Provar sua inscrição no cadastro de contribuintes estadual e municipal, se houver, relativo ao domicílio ou sede da empresa;

- Provar sua regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede da empresa;

- Possuir protocolo ou carta de intenções, contendo o objeto do contrato, duração e grau de sigilo envolvido; e

- Informar a natureza da Informação Classificada, bem como a necessidade do seu tratamento.

Obs: Todos os requisitos mínimos estão em conformidade com o item 9 da NC01/IN02/NSC/GSI/PR, de 2013. (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >).

3.1.4. Requisitos Mínimos para Habilitação de Posto de Controle (PC)

A Habilitação de Segurança de Posto de Controle (PC) será sempre feita por um Órgão de Registro Nível 1 (ORN 1) habilitado, com exceção do primeiro PC do ORN 1 que será habilitado sempre pelo Núcleo de Segurança e Credenciamento (NSC), a fim tratarem Informações Classificadas, em qualquer grau de sigilo, na forma do item 8 da NC01/IN02/NSC/GSI/PR, de 2013. (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >).

- Estar localizado em área de acesso restrito, conforme disposto nos artigos 42, 43, 44 e 45 do Decreto nº 7.845, de 2012 (disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>);

- Possuir meios de armazenamento de documentos físicos e eletrônicos com nível de segurança compatível com os graus de sigilo e volume;

- Possuir estrutura física adequada para o armazenamento e preservação dos documentos físicos e eletrônicos;

- Possuir planos e procedimentos de contingência de forma a assegurar a continuidade dos processos essenciais no caso de falhas ou sinistros;

- Possuir meios de comunicação segura compatível com os graus de sigilo;

- Possuir suas redes de dados e seus sistemas de tecnologia da informação adequadamente protegidos de ataques eletrônicos;

- Possuir sistemas alternativos de proteção da infraestrutura crítica relacionada com os ativos de informação e materiais de acesso restrito sob sua responsabilidade de armazenamento e controle;

- Atender aos princípios de disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação e materiais de acesso restrito sob sua responsabilidade;

- Possuir protocolo exclusivo para documentos classificados, e quando necessário, de Documentos Controlados;

- Possuir restrição ao uso de máquinas fotográficas, gravadores de vídeo e áudio, ou similares, tais como câmeras de dispositivos móveis no interior das instalações do PC;

- Possuir meios de armazenamento de documentos físicos que permitam sua disponibilidade, integridade, confidencialidade e autenticidade bem como ter nível de segurança compatível com o volume de dados a ser armazenado;

- Possuir capacidade de fazer o Tratamento da Informação Classificada dos documentos físicos ou eletrônicos que estejam sob sua guarda na forma do Capítulo III do Decreto nº 7.845, de 14 de novembro de 2012 (disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>);

- Possuir um Gestor Responsável pelo PC;

- Possuir quadro de pessoal capacitado para o Tratamento de Informação Classificada; e

- Possuir recurso criptográfico para armazenamento e transmissão da informação classificada em conformidade com a Instrução Normativa GSI/PR nº 3, de 6 de março 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr3.pdf>).

Obs: Todos os requisitos mínimos estão em conformidade com o item 8.5 da NC01/IN02/NSC/GSI/PR, de 2013. (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >).

3.2. Requisitos Mínimos para Credenciamento de Segurança de Pessoas Naturais

O Credenciamento de Segurança de pessoas naturais é um processo que deverá sempre ser feito pelos Órgãos de Registro Nível 1 e 2 (ORN 1 e ORN 2) devidamente habilitado, e será concedida a uma pessoa natural somente nos casos em que houver a **necessidade de conhecer informações classificadas**, em qualquer grau de sigilo, conforme estabelecido em normatização interna do órgão ou entidade do Poder Executivo federal ao qual a pessoa a ser credenciada estiver vinculada, devendo esta concessão seguir o estabelecido no item 5 da NC01/IN02/NSC/GSI/PR, de 2013. (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >).

- Ser um ORN 1 ou ORN 2 com Habilitação de Segurança;

- Ser um Órgão ou entidade pública competente para realizar o Credenciamento de Segurança de pessoas naturais, integrante ou não da própria estrutura organizacional do Órgão de Registro solicitante, observado o disposto no Parágrafo único do art. 8º Decreto nº 7.845, de 2012. (disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>);

- Possuir um Gestor de Segurança e Credenciamento devidamente credenciado e nomeado; e

- Possuir servidor público ocupante de cargo efetivo ou militar de carreira, com competência profissional comprovada para atuar na área de inteligência, ou policial ou por perito criminal, ou ainda, conforme o caso, profissionais de saúde, a fim de emitirem pareceres técnicos específicos desta área, a critério do responsável pelo relatório da investigação, na forma do item 5.5.2.5 da NC01/IN02/NSC/GSI/PR, de 27 de junho de 2013 (disponível em: <http://dsic.planalto.gov.br/documentos/NSC/NC01_IN02_GSI.pdf >) ou do Parágrafo único do art. 8º do Decreto 7.845, de 14 de novembro de 2012. (disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>).