PODER JUDICIÁRIO
JUSTIÇA FEDERAL DE 1º GRAU DA 5ª REGIÃO
SEÇÃO JUDICIÁRIA DO CEARÁ

ANEXO II

Política de Controle de Acesso Lógico

1. Apresentação

Esta política norteará a implementação de medidas para regular o acesso lógico aos recursos de processamento, armazenamento e comutação de dados corporativos de Tecnologia da Informação (TI) da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará (SJCE) de forma a minimizar os riscos à segurança das informações corporativas.

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que a informação tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

As suas definições e orientações estão de acordo com as exigidas pelo item 9.3.1 – Política de Controle de Acesso Lógico – do Anexo I da Resolução Nº 6, de 7 de abril de 2008, do Conselho da Justiça Federal, que definiu a Política de Segurança da Informação no âmbito do Conselho e da Justiça Federal de Primeiro e Segundo Graus.

2. Escopo

O escopo deste documento integrante da Política de Segurança da Informação abrange a Justiça Federal de Primeira Instância – Seção Judiciária do Ceará.

3. Público Alvo

A presente Política aplica-se aos agentes públicos da Justiça Federal de Primeira Instância – Seção Judiciária do Ceará e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas.

4. Termos e Definições

Acesso remoto – Tipo de acesso que possibilita se conectar a um computador e assim controlar e trabalhar diretamente sobre o referido sistema tecnológico, independentemente da distância física.

Confidencialidade – Sigilo. Preservar a confidencialidade de uma informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-las.

Criptografia – Arte e ciência de esconder o significado de uma informação de receptores não desejados.

Disponibilidade – Uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que precisam.

Fator de Autenticação – Informação que um cliente/usuário sabe (ex: *senha*), tem (ex.: *smartcard*) ou é (ex: impressão digital) e é necessária para completar sua autenticação num sistema.

Integridade – A preservação da integridade envolve proteger as informações contra alterações, intencionais ou acidentais, em seu estado original.

Log – Registros de dados que armazenam informações de auditoria.

OTP – *One Time Password*. É uma senha que perde a validade após um processo de autenticação. Geralmente uma nova senha é gerada de forma aleatória e em intervalos de tempo regulares.

Privilégio Mínimo – Permissão para o usuário acessar apenas os recursos necessários para realizar a sua tarefa.

Recursos de TI – Recursos de Tecnologia da Informação. Softwares e hardwares que geram, processam, recebem ou transmitem informações como desktops, notebooks, sistemas operacionais, processadores de texto, *smartphone*, *pendrive*, etc.

Rede de dados institucional – Todos os segmentos de rede de dados disponibilizados pela SJCE.

Rede de dados institucional restrita– Todos os segmentos de rede de dados onde estão disponibilizados os serviços institucionais restritos aos agentes públicos da SJCE e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas. Todos os equipamentos utilizados nessa rede são de propriedade exclusiva da instituição ou por ela autorizados.

Rede de dados institucional sem fio – Todos os segmentos de rede de dados disponibilizados pela SJCE através da tecnologia sem fio.

Smartcard - é um cartão que geralmente assemelha-se em forma e tamanho a um cartão de crédito convencional. Muito utilizado para armazenar informações relativas a certificados digitais.

Smartphone – Telefone móvel, dotado de grande capacidade computacional, cumprindo funções de telefone celular, agenda e sistema informático de escritório elementar, com possibilidade de interconexão com um computador pessoal e redes de computação.

Usuários – agentes públicos, estagiários, aprendizes, parceiros e contratados.

VPN – *Virtual Private Network*. É uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, implementada em cima de uma rede de comunicações pública (como por exemplo, a Internet).

5. Identificação dos usuários

5.1 A gestão de credenciais de identificação de usuários, assim como de seus perfis de acesso aos recursos de rede e sistemas da SJCE, inclusive correio eletrônico, deve ser realizada pela unidade de Tecnologia da Informação (TI) por solicitação formal da autoridade competente.

5.2 O acesso aos recursos de tecnologia da informação somente deve ser permitido aos usuários previamente autorizados mediante identificação.

5.3 As autorizações devem ser definidas de acordo com a necessidade de condução das tarefas institucionais e considerando o princípio de privilégio mínimo.

5.4 Somente usuários que pertençam à unidade de Tecnologia da Informação (TI) poderão possuir privilégio de administrador de computadores/sistemas, ressalvando-se a possibilidade de se delegar tal privilégio em situações específicas e por tempo determinado, apenas e tão somente quando o acesso remoto não se mostrar suficiente para a solução do problema ou a adoção da providência necessária.

5.5 Os usuários da unidade de TI deverão possuir privilégio de administrador de computadores/sistemas apenas se necessário para o cumprimento de suas atividades, obedecido o princípio de privilégio mínimo.

5.6 Sempre que possível, o controle de acesso aos recursos de TI deverá possuir, pelo menos, dois fatores de autenticação.

5.7 As credenciais de identificação do usuário, a exemplo de dispositivos OTP, *login*/senhas e *smartcards*, são únicas, pessoais e intransferíveis, não devendo ser compartilhadas. Sua utilização ou conseqüências decorrentes do seu uso indevido são de responsabilidade do usuário. Nenhum usuário deve identificar-se como outro usuário.

5.8 Não haverá credencial de identificação de usuário genérica e de uso compartilhado para acesso aos recursos de TI, excetuando-se os casos de necessidade justificada. Nestes casos, a unidade de TI deverá ser consultada para emissão de parecer acerca dos riscos associados.

5.9 As senhas dos usuários devem ser escolhidas seguindo critérios a serem definidos pela unidade de TI. Tais critérios deverão considerar, entre outros:

5.9.1 Mecanismos para impedir a geração de senhas fracas ou óbvias;

5.9.2 Conjunto de caracteres permitidos;

5.9.3 Tamanho, vigência, forma de troca e restrições específicas para as senhas;

5.9.4 Segurança da distribuição de senhas (inicial ou não);

5.9.5 Bloqueio ou desativação de usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso malsucedidas.

5.10 Fica assegurado à Comissão Local de Resposta a Incidentes (CLRI), a qualquer tempo, decidir pela suspensão temporária do acesso de usuário ao recurso computacional da SJCE quando evidenciados os riscos à segurança da informação.

5.11 É proibida a utilização de senhas sem nenhum processo criptográfico aplicado, excetuando-se os casos em que não houver alternativa.

6. Processo de desligamento ou movimentação de usuário

6.1 Em regra, somente serão concedidas credenciais de acesso aos usuários que estejam em atividade na SJCE.

6.2 As credenciais, identificações, crachás, equipamentos, mecanismos e acessos lógicos devem ser revogados e/ou inutilizados quando do desligamento do usuário.

6.3 A unidade de gestão de pessoas será responsável pelo envio da informação de desligamento ou movimentação de magistrados, servidores, estagiários e aprendizes integrantes da SJCE à unidade de TI para os devidos ajustes das credenciais de acesso.

6.4 O desligamento ou movimentação de usuários não mencionados no item 6.3 deverá ser comunicado à unidade de TI pelo gestor ou responsável pelo respectivo contrato/convênio.

7. Acesso à rede institucional

7.1 É vedada a conexão de equipamento, ligado à rede institucional da SJCE, a outros sítios através da utilização de linha discada, rede sem fio, ou quaisquer outros meios, exceto em casos de comprovada necessidade, mediante autorização fundamentada em parecer técnico favorável da unidade de TI.

7.2 É vedada a utilização de microcomputadores ou dispositivos eletrônicos não pertencentes à SJCE, portáteis ou não, na rede institucional restrita, exceto em casos de comprovada necessidade, mediante autorização fundamentada em parecer técnico favorável da unidade de TI.

8. Acesso remoto à SJCE

8.1 É proibido o acesso remoto à rede institucional da SJCE por meios que não apliquem criptografia ao tráfego durante o acesso.

8.2 O acesso remoto à rede institucional da SJCE deverá ser precedido de solicitação formal explicitando os motivos de tais necessidades, o período de utilização e os serviços a

serem utilizados. A autorização ficará condicionada a parecer técnico favorável da unidade de TI.

8.3 As conexões de acesso remoto deverão ser precedidas da assinatura do Acordo de Requisitos a Acesso Remoto, documento a ser mantido e atualizado pela unidade de TI.

8.4 O usuário com privilégio de acesso remoto é responsável por garantir que nenhuma outra pessoa, com acesso físico ou lógico ao dispositivo que está efetuando a conexão, viole qualquer política da SJCE, execute atividades ilegais e/ou utilize o acesso para desenvolver atividades pessoais. Este usuário detém a responsabilidade pelas consequências do mau uso do acesso remoto.

8.5 A segurança do acesso remoto deve ser controlada. O controle deverá ser feito através de autenticação forte, de preferência com utilização de autenticação de no mínimo dois fatores e de regras de filtragem que reforcem o princípio do privilégio mínimo.

8.6 As credenciais de acesso remoto são pessoais e intransferíveis, sendo o usuário responsável pela segurança das informações.

8.7 Estações de trabalho ou dispositivos móveis que serão utilizados para o acesso remoto deverão ser disponibilizados preferencialmente pela unidade de TI e ter suas configurações por ela aprovadas.

8.8 As informações de controle dos acessos remotos (*logs*) deverão ser registradas e auditadas periodicamente pela unidade de TI para apuração de eventuais violações de segurança e contabilização do uso de recursos.

9. Utilização de sistema de mensageria institucional

9.1 O sistema de correio eletrônico da SJCE não deve ser utilizado para a criação ou distribuição de quaisquer mensagens que não sejam compatíveis com as atribuições dos usuários, incluindo, mas não se limitando a, ofensas e comentários sobre raça, idade, deficiência, orientação sexual, pornografia, crença e religião, política ou nacionalidade.

9.2 Cabe à Administração da SJCE, mediante solicitação formal e parecer técnico emitido pela unidade de TI, autorizar a criação de listas de endereços de *e-mail* para

veiculação de assunto dos juízes e servidores, inclusive para temas não compreendidos pelo item 9.1.

9.3 Todos os *e-mails* armazenados, transmitidos ou recebidos pelo sistema de correio eletrônico da SJCE são passíveis de auditoria, podendo ser rastreados por *softwares* específicos para a verificação e adequação às normas estabelecidas na Política de Segurança da Informação do Conselho e Justiça Federal de Primeiro e Segundo Graus e na legislação brasileira.

9.4 O envio de mensagens através de listas de endereços de *e-mail* deve restringir-se a assuntos referentes às suas respectivas temáticas.

9.5 É proibido o envio de *spam* ou mensagens que contenham *software* malicioso por parte dos usuários do sistema de correio eletrônico da SJCE.

9.6 A SJCE deverá prover mecanismos para a identificação de mensagens que possuam conteúdo infectado por *softwares* maliciosos ou que ofereçam risco à segurança da informação. Tais mensagens, quando detectadas, poderão ser excluídas automaticamente ou armazenadas em quarentena.

9.7 Cabe à Administração da SJCE, mediante parecer técnico emitido pela unidade de TI, estipular as regras de utilização do correio eletrônico que se façam necessárias para o bom funcionamento do serviço e à segurança das informações, tais como: quantidade máxima de destinatários, tamanho máximo das caixas postais, tipos e tamanho máximo de arquivos anexos permitidos, periodicidade de leitura obrigatória das mensagens recebidas e criação e exclusão de listas de endereços de *e-mail*.

10. Utilização de sistema de mensageria instantânea

10.1 A SJCE proverá sistemas de mensageria instantânea para a comunicação entre os seus usuários e outros órgãos.

10.2 Cabe à Administração da SJCE, mediante parecer técnico emitido pela unidade de TI, definir a solução de mensageria instantânea a ser utilizada pela SJCE.

10.3 A utilização ou conexão com sistemas de mensageria instantânea de uso não institucional deverá ser precedida de solicitação formal à Administração da SJCE, que decidirá mediante parecer técnico da unidade de TI.

10.4 O sistema de mensageria instantânea da SJCE não deve ser utilizado para a criação ou distribuição de quaisquer mensagens que não sejam compatíveis com as atribuições dos usuários, incluindo, mas não se limitando a, ofensas e comentários sobre raça, idade, deficiência, orientação sexual, pornografia, crença e religião, política ou nacionalidade.

11. Acesso à Internet

11.1 O acesso aos serviços disponibilizados na Internet será provido aos usuários conforme parâmetros estabelecidos pela SJCE, obedecendo ao princípio de privilégio mínimo.

11.2 O acesso a serviços que não se enquadrem na previsão do item anterior deverá ser precedido de solicitação formal à Administração da SJCE, que decidirá mediante parecer técnico da unidade de TI.

11.3 A unidade de TI utilizará *softwares* específicos que efetuarão o registro de todos os acessos aos serviços providos na Internet, assim como o bloqueio dos serviços não autorizados.

12. Conexão e Acesso para Terceiros

12.1 Toda conexão de rede de dados entre a SJCE e terceiros que necessitam de acesso remoto, independente da tecnologia de circuito de telecomunicação ou de VPN, deve ser autorizada pela Administração da SJCE mediante solicitação formal e parecer técnico emitido sob a perspectiva de segurança da informação pela unidade de TI. A análise deverá garantir que todos os acessos estejam de acordo com as necessidades do serviço da melhor maneira possível, e que o princípio do privilégio mínimo será seguido.

12.1.2 Toda nova requisição de conexão entre a SJCE e terceiros necessita que seus representantes concordem e assinem o Acordo de Conexão de Remota.

12.1.3 Cabe à Administração da SJCE, mediante parecer técnico emitido pela unidade de TI, estipular as regras para conexão e acesso remoto para terceiros.

13. Acesso à rede sem fio

13.1 As exigências que se seguem atingem todos os dispositivos de comunicação de dados conectados à rede institucional sem fio da SJCE.

13.1.1 Todos os pontos de acesso sem fio conectados à rede institucional da SJCE deverão ser submetidos ao controle da unidade de TI. Esses pontos de acesso serão objeto de periódicos testes de penetração e auditoria.

13.1.2 Todas as conexões à rede sem fio deverão ser aprovadas em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.

13.1.3 O acesso aos serviços disponibilizados na rede institucional restrita, a partir da rede sem fio, será provido aos usuários conforme parâmetros estabelecidos pela SJCE, obedecendo ao princípio de privilégio mínimo.

14. Periodicidade de Revisão

14.1 Esta política deverá ser revista anualmente pelo Comitê Local de Segurança da Informação com vistas a adequá-la às necessidades atuais.

14.2 O acontecimento de fatos supervenientes, relevantes para a segurança da informação, autorizam o Comitê Local de Segurança da Informação a rever esta política a qualquer tempo.

15. Penalidades

15.1 O descumprimento das regras contidas neste documento importará a aplicação das penalidades previstas na legislação vigente, mediante o devido processo legal.