Guia Referencial de Segurança da Informação da Justiça do Trabalho

- 2021 -

SUMÁRIO

1. SOBRE ESTE GUIA

Este Guia atua como parte complementar e subsidiária do disposto na Resolução CNJ nº 396/2021 e na Portaria CNJ nº 162/2021 que dispõem sobre a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e seus manuais e protocolos que devem ser aplicados no Poder Judiciário.

A atualização, publicação e divulgação deste Guia se dará por ato administrativo específico da Secretaria Geral do CSJT com a ciência e aprovação da Presidência.

O Guia foi criado com o intuito de orientar os diversos papéis que contribuem ou são impactados pelas atividades e deliberações no âmbito da segurança da informação na Justiça do Trabalho, com vistas a complementar a “Estratégia Nacional de Segurança Cibernética do Poder Judiciário”.

Qualquer instância que esteja envolvida na segurança da informação precisa estar ciente e considerar, naquilo que a diz respeito, as diretrizes e mecanismos constantes neste Guia.

2. COMO UTILIZAR E APLICAR ESTE GUIA

Este guia não substitui a Política de Segurança da Informação vigente em cada Regional e destina-se a dar orientações de cunho prático-operacional, visando maior agilidade e praticidade das diretrizes apresentadas na resolução que o originou e nos demais normativos complementares.

Estando dividido em seções para melhor compreensão, o leitor pode direcionar-se diretamente para o tema de seu interesse.

SEÇÃO I - Identidade e Acesso

1. Diretrizes para autenticação e senhas na Justiça do Trabalho

Espera-se que cada Regional, durante a elaboração de suas políticas e procedimentos, considere:

- A senha de acesso ao ambiente corporativo é de uso pessoal e intransferível, cabendo ao usuário mantê-la em sigilo. O titular é considerado responsável por qualquer ação realizada utilizando suas credenciais de acesso no ambiente computacional;

- É recomendável não reutilizar senhas de acesso corporativo em contas de sites de terceiros, sem relação com a rotina de trabalho, como por exemplo em plataformas de redes sociais, negócios/compras de interesse pessoal ou estabelecimentos físicos;

- Sempre que possível, a qualidade da senha deverá ser verificada no momento de sua definição. As senhas de acesso aos ativos de informação deverão conter, pelo menos, 11 caracteres, sendo ao menos 1 caractere alfabético e 1 caractere numérico. No caso de sistemas legados, admitir-se-á senhas com no mínimo 8 caracteres, sendo ao menos 1 caractere alfabético e 1 caractere numérico;

- A senha do usuário deve ser codificada por algoritmo de hash aberto (público) de, no mínimo, 160 bits. Quando tecnicamente viável, deverá ser utilizado mecanismo de “salt” para incrementar a segurança das senhas com relação a ataques de rainbow tables;

- As senhas deverão expirar depois de 365 dias contados à partir do seu cadastramento ou alteração. Senhas presentes em vazamentos de dados deverão ser revogadas imediatamente e os titulares comunicados;

- Deverão ser providenciadas soluções, tais como captcha, múltiplo fator de autenticação e bloqueio temporário após muitas tentativas pelo mesmo IP ou utilizando o mesmo nome de usuário, para coibir tentativas de descoberta de senha por força bruta;

- Sempre que possível, deverá ser implementado múltiplo fator de autenticação para soluções de acesso remoto, como VPN e Remote Desktop, e para privilégios administrativos, como acessos à redes de controle ou gerência, interfaces de administração de soluções, entre outros;

- Os processos de troca de senha deverão exigir que a nova senha do usuário seja diferente das anteriores. É desejável que as senhas não possam ser trocadas em período inferior a 3 dias.

2. Referências

- Portaria N° 162 de 10/06/2021 do Conselho Nacional de Justiça - CNJ - Que aprova Protocolos e Manuais criados pela Resolução CNJ n° 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

- Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, disponível em: http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2016_v4-2.pdf

SEÇÃO II – Cópias de segurança

1. Principais conceitos

- **Backup**: Cópia de um conjunto de dados de um dispositivo de armazenamento para outro, com a finalidade de proteger os dados e, eventualmente, restaurá-los em caso de perda;

- **Backup completo**: são copiados todos os arquivos do conjunto de dados existentes no momento do backup;

- **Backup diferencial**: somente os arquivos novos ou modificados desde o último backup completo são transmitidos.

2. Diretrizes para a geração e testes de cópias de segurança

Espera-se que cada Regional, durante a elaboração de suas políticas e procedimentos, considere:

- As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização;

- Todos os dados dos sistemas críticos da organização devem ter cópias de segurança (backups) realizadas automaticamente de forma regular;

- Os sistemas críticos da organização devem ter suas cópias de segurança (backups) realizadas como um sistema completo, por meio de processos como a geração de imagem, de forma a permitir uma rápida recuperação de todo o sistema;

- As cópias de segurança (backups) devem estar apropriadamente protegidas por meio de segurança física ou criptografia quando forem armazenadas, assim como quando são movimentadas através da rede;

- Os testes de recuperação do backup completo das bases de dados dos sistemas nacionais devem ser realizados ao menos uma vez por ano e, os resultados, divulgados;

- A frequência, tipo e tempo de retenção dos backups gerados serão definidos pela unidade gestora de TIC do Tribunal em conjunto com a área negocial, considerando os requisitos legais e a criticidade dos

dados envolvidos com relação às atividades da instituição e à disponibilidade de recursos de infraestrutura de TIC;

  - É recomendada a utilização de backup diferencial diário com retenção mínima de 30 dias corridos, como modelo padrão de backup na Infraestrutura de TIC;
  - Em caso de necessidade, poderá ser adotado modelo de backup diferente do padrão constante no item anterior.

- As mídias de backup de dados de sistemas críticos ao funcionamento da organização devem ser testadas periodicamente através de procedimento de cópia do backup ou testes de recuperação, de acordo com a disponibilidade de recursos de infraestrutura de TIC;

- As cópias do backup de dados de sistemas críticos devem ser armazenadas em uma localidade remota, a uma distância suficiente para evitar danos ocasionados por um eventual desastre no local principal e deve possuir um nível apropriado de proteção física e ambiental;

- As cópias de segurança dos sistemas críticos da organização devem conter ao menos uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.

3. Referências

- Portaria Nº 162 de 10/06/2021 do Conselho Nacional de Justiça - CNJ - Que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

- O Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

- Norma ABNT NBR ISO/IEC Série 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

- Norma ABNT NBR ISO/IEC 17799:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

- Publicação ISACA COBIT 4.1:2007 - Controls Objectives for Information and Related Technology;

- A Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD).

SEÇÃO III – Uso de recursos de TIC

1. Diretrizes para o uso de recursos nas redes corporativas da Justiça do Trabalho

Espera-se que cada Regional, durante a elaboração de suas políticas e procedimentos, considere:

- O acesso à rede corporativa e aos ativos deverá acontecer somente pelos meios disponibilizados pelo Tribunal, com a utilização de procedimentos e mecanismos definidos pela área de Tecnologia da Informação e Comunicação;

- Sempre que possível, deverá haver procedimentos auditáveis para credenciamento, bloqueio e exclusão de contas de acesso dos usuários de sistemas informatizados, inclusive para ambientes de homologação.

- Os acessos à rede corporativa deverão ser registrados de forma a permitir a rastreabilidade e a identificação dos usuários que o fizeram por um período mínimo de 6 meses.

- Os acessos remotos para uso da rede corporativa realizados por prestadores de serviço devem ser, preferencialmente, supervisionados, controlados e monitorados.

- A comunicação entre a rede corporativa dos Tribunais e a Internet priorizará a prestação jurisdicional acima de outras necessidades.

- A utilização da Internet para acesso de informações e serviços de caráter pessoal é permitida desde que a frequência do uso e a quantidade de dados transmitidos considerem a disponibilidade dos canais de acesso.

- Toda conexão à Internet deverá passar por equipamentos de segurança que garantam o controle de acesso e a aplicação de mecanismos de filtragem de tráfego, identificação de ameaças, entre outros.

- Os equipamentos que hospedam serviços e aplicações devem ter acesso restrito à internet, sendo liberado apenas o acesso a sites e serviços necessários ao seu pleno funcionamento.

- É recomendado que os dispositivos com acesso à Internet providos pela instituição, como estações de trabalho, notebooks, servidores e outros, devem possuir sistema de proteção instalado, ativado e atualizado contra vírus ou contra qualquer outro software malicioso. Isso inclui os dispositivos utilizados em teletrabalho ou trabalho remoto.

- O acesso remoto a serviços críticos de monitoração e gerenciamento administrativo deve ser realizado, preferencialmente, via VPN.

2. Referências

- Portaria Nº 162 de 10/06/2021 do Conselho Nacional de Justiça - CNJ - Que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)

- O Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

- Norma ABNT NBR ISO/IEC Série 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

- Norma ABNT NBR ISO/IEC 17799:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

- Publicação ISACA COBIT 4.1:2007 - Controls Objectives for Information and Related Technology;

- A Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD).

Histórico de Versões

Versão	Descrição	Responsável	Data
1.0	Versão inicial do Guia	NUGOV/CTSEG	Setembro/2021