Guia Referencial de Segurança da Informação da Justiça do Trabalho

- Versão 2.0 - fevereiro de 2022 -

SUMÁRIO

Histórico de Versões

Versão	Descrição	Responsável	Data
1.0	Versão inicial do Guia	NUGOV/CTSEG	Setembro/2021
2.0	Inclusão da Seção IV - Desenvolvimento de sistemas	NUGOV/CTSEG	Fevereiro/2022

SOBRE ESTE GUIA

Este Guia é parte complementar e subsidiária ao 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), seus manuais e protocolos que devem ser aplicados no Poder Judiciário.

A atualização, a publicação e a divulgação deste Guia dar-se-ão 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 deve estar ciente e considerar, no que lhe diz respeito, as diretrizes e os mecanismos constantes neste Guia.

1. COMO UTILIZAR E APLICAR ESTE GUIA

Este guia não substitui a Política de Segurança da Informação vigente em cada Tribunal Regional do Trabalho e se destina 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.

SEÇÃO I - Identidade e Acesso

1. Diretrizes para autenticação e senhas na Justiça do Trabalho

Espera-se que cada Tribunal 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 ao ambiente computacional;

- É recomendável não reutilizar senhas de acesso corporativo em contas de sítios de terceiros sem relação com a rotina de trabalho, como 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-ão 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 do 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 a 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 Nº 162 de 10/6/2021 do Conselho Nacional de Justiça - CNJ – Aprova Protocolos e Manuais criados pela Resolução CNJ nº 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**: Cópia de todos os arquivos do conjunto de dados existentes no momento do backup.

- **Backup diferencial**: Cópia dos arquivos novos ou modificados desde o último backup completo.

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

Espera-se que cada Tribunal 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 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, o tipo e o 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 para o funcionamento da organização devem ser testadas periodicamente por meio 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 localidade remota, a distância suficiente para evitar danos ocasionados por eventual desastre no local principal e devem possuir nível apropriado de proteção física e ambiental;

- As cópias de segurança dos sistemas críticos para a 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 10/6/2021 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).

- Decreto nº 3.505, de 13 de junho de 2000 – 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.

- 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 Tribunal 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 por um período mínimo de 6 meses.

- Os acessos remotos para uso da rede corporativa realizados por prestadores de serviço deverão 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 deverão ter acesso restrito à internet, sendo liberado apenas o acesso a sítios 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, possuam 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 10/6/2021 do Conselho Nacional de Justiça – CNJ – Aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

- Decreto nº 3.505, de 13 de junho de 2000 – 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.

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

SEÇÃO IV – Desenvolvimento de sistemas

1. Principais conceitos

- **Recursos privilegiados em um sistema**
  - Gerenciar outros usuários, perfis ou grupos;
  - Gerenciar funcionalidades disponíveis;
  - Gerenciar permissões;
  - Manipular dados ou arquivos de configuração;
  - Escalar privilégios, ou seja, simular acesso ou personificar outros usuários.
- **Dados privilegiados em um sistema**
  - Dados pessoais de terceiros exceto nome, matrícula e cargo;
  - Dados de processo administrativo ou judicial com restrição de acesso e/ou sigilo;
  - Registros de auditoria.

2. Diretrizes gerais para o ciclo de desenvolvimento de sistemas

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

- Qualquer atividade de desenvolvimento de *software* ou sistemas no âmbito dos TRTs deverá ocorrer com a participação da unidade responsável pela Tecnologia da Informação.

- O público-alvo de cada sistema deverá ser avaliado para a decisão de publicá-lo na Internet ou manter o acesso restrito às redes internas de cada Tribunal Regional.

- É recomendado integrar conceitos e controles de segurança da informação no ciclo de desenvolvimento de sistemas, desde a concepção de um novo sistema até sua liberação, visando aumentar a proteção contra, no mínimo, as ameaças relacionadas no guia OWASP Top Ten.

- A aplicação de testes manuais ou automáticos de segurança antes da liberação de novas versões dos sistemas abrangendo, no mínimo, os sistemas mantidos pelo próprio Tribunal Regional.

- É recomendado que o ambiente de desenvolvimento seja separado de outros ambientes, como homologação e produção.

- Caso seja necessária a réplica de dados de produção em ambiente de desenvolvimento, devem-se aplicar mecanismos de ofuscação de

dados pessoais ou privilegiados no momento da replicação, sempre que viável.

- Deve-se utilizar protocolo seguro de comunicação (como HTTPS ou SFTP), sempre com TLS na versão 1.2 ou superior, em todos os sistemas disponibilizados. Essa configuração também deve considerar a comunicação na infraestrutura computacional, como integração entre sistemas, bancos de dados e serviços de diretório.

- O ambiente computacional, os sistemas e seus componentes, incluindo as dependências e bibliotecas de código, devem ser mantidos atualizados, considerando sempre os repositórios oficiais de cada projeto ou sistema.

- Disponibilizar ambiente de desenvolvimento adequado e padronizado para utilização de todos os desenvolvedores.

- Os sistemas devem tratar (coletar, processar, armazenar ou transferir) dados pessoais somente quando imprescindíveis para seus objetivos e funcionalidades do sistema.

- Deve ser evitado o tráfego de dados sensíveis na URL da requisição.

- Toda verificação de segurança, como controles de autenticação e autorização, sanitização das informações de entrada dos usuários, regra de negócio sensível, entre outras, deverá ser realizada no *backend* da aplicação, sem prejuízo de qualquer controle aplicado no *frontend*.

- Garantir que todos os responsáveis pelo desenvolvimento de *software* recebam treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas.

3. Autenticação

- O acesso ao banco de dados deve ser realizado por meio de contas individualizadas por sistema, ou seja, cada sistema deve possuir suas próprias credenciais de acesso.

- O usuário das aplicações não deve ter permissões administrativas amplas, como “root”, “SA”, entre outras.

- Utilizar uma implementação centralizada para realizar os procedimentos de autenticação, disponibilizando bibliotecas que invoquem os serviços externos de autenticação.

- As senhas dos usuários de aplicação devem respeitar, no mínimo, o disposto na Seção 1 - Identidade e Acesso.

- Sempre que viável, o sistema deve implementar autenticação integrada ao serviço de diretórios de usuários utilizado no Tribunal Regional.

- É recomendado que os sistemas implementem autenticação de múltiplos fatores, quando viável.

- Se optar por usar redefinição de senha baseada em e-mail, deve ser enviado e-mail somente para o endereço pré-definido contendo *link* ou senha de acesso temporário que permita ao usuário redefinir a senha.

- Implementar controles contra-ataques de força bruta, considerando o disposto na Seção 1 - Identidade e Acesso.

4. Diretrizes para a geração de registros de auditoria (logs) nos sistemas da JT

- Devem ser registradas as tentativas de autenticação, bem sucedidas ou não, aos sistemas.

- Deve ser registrado o processo de *logout*/saída dos sistemas.

- Devem ser registrados o acesso, a manipulação ou a utilização de dados e recursos privilegiados.

- Os sistemas não devem oferecer funcionalidades que permitam a alteração de registros de auditoria. Quando necessário, devem ser providas funcionalidades apenas de visualização dessas informações. Essas visualizações também devem ser registradas.

- Cada registro, sempre que viável, deverá conter as seguintes informações:

  - Identificação inequívoca do usuário, como por exemplo o usuário utilizado para *login*, CPF, OAB, entre outros;
  - Descrição do evento e do resultado do evento;
  - Em caso de operação de escrita, os valores anteriores e novos;
  - Data, hora e fuso horário de cada evento, observando-se a Hora Legal Brasileira;
  - Endereço IP de origem;
  - Porta de origem da conexão;
  - Identificador do ativo ou instância relacionados;
  - Coordenadas geográficas, se disponíveis.

- Não armazenar informações sensíveis nos registros de *logs*, como detalhes desnecessários do sistema, identificadores de sessão e senhas.

5. Referências

- Melhores Práticas de Codificação Segura OWASP – Guia de Referência Rápida
  https://owasp.org/www-pdf-archive/OWASP_SCP_v1.3_pt-BR.pdf