# PORTARIA TRT 18ª SGP/CSIN Nº 3358/2022 *

**PODER JUDICIÁRIO DA UNIÃO**
**TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO**
**SECRETARIA-GERAL DA PRESIDÊNCIA**
**COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO**

** Texto atualizado até as alterações promovidas pela Portaria TRT18 n° 720/2024*

Disciplina a adoção dos manuais de referência da Estratégia Nacional de Segurança Cibernética no âmbito do Tribunal Regional do Trabalho da 18ª Região.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais, tendo em vista o que consta dos Processos Administrativos nº 15452/2020 e nº 14484/2014;

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria CNJ nº 162/2021, em especial os Manuais de Referência descritos em seus anexos IV, V, VI e VII;

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 145/2019, que Institui a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região, assim como o conteúdo das normas de segurança da informação instituídas pelo Tribunal e a ela alinhadas,

RESOLVE:

## CAPÍTULO I
## DAS DISPOSIÇÕES GERAIS

Art. 1º Fica estabelecida, na forma disciplinada por esta portaria, a adoção dos manuais de referência da ENSEC-PJ no âmbito do Tribunal Regional do

Biblioteca Digital

Trabalho da 18ª Região.

Parágrafo único. São quatro os manuais de referência adotados, cujas descrições constam nos anexos de IV a VII da Portaria CNJ nº 162/2021:

I – Proteção de Infraestruturas Críticas de TIC, anexo IV;

II – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, anexo V;

III – Gestão de Identidade e Controle de Acessos, anexo VI; e

IV – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário, anexo VII.

Art. 2º Para os fins desta Portaria, consideram-se as definições constantes do anexo VIII (Glossário) da Portaria CNJ nº 162/2021.

## CAPÍTULO II
## DO MANUAL "PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC"

Art. 3º Para a proteção de infraestruturas críticas de TIC, consideram-se minimamente aplicáveis neste Regional os controles e respectivas medidas de segurança contidas na publicação da versão 8 do *CIS Critical Security Controls* (*CIS - Center for Internet Security - cisecurity.org*) e que estejam nela classificados como *IG2* (grupo de implementação 2).

§ 1º O anexo I desta portaria contém uma lista simplificada dos controles e medidas de segurança do *CIS Critical Security Controls v8*.

§ 2º O colegiado temático de segurança da informação poderá deliberar sobre proposta de adoção de versão mais recente do *CIS Critical Controls*, conforme facultado no item 5.4 do anexo IV da Portaria CNJ Nº 162/2021.

§ 3º A priorização para implementação das medidas de segurança a que se refere o *caput* segue preferencialmente as recomendações da publicação contida no *CIS Critical Controls, onde sugere-se*:

I - implementar primeiro as medidas de segurança classificadas como *IG1*, em seguida as classificadas como *IG2* e finalmente as classificadas como *IG3*; e

Biblioteca Digital

II - dentro de cada grupo de implementação, implementar as medidas de segurança de menor numeração para as de maior numeração.

## CAPÍTULO III
## DO MANUAL “PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL”

Art. 4º A unidade de gestão de segurança da informação deste Regional deve propor nova regulamentação e processo de gestão de riscos de segurança da informação em conformidade com as recomendações contidas nos itens de 11 a 21 do anexo V da Portaria CNJ nº 162/2021, no que couber, tendo em vista as diretrizes já estabelecidas na Política de Gestão de Riscos e no Plano de Gestão de Riscos corporativos deste Regional.

Art. 5º A unidade de auditoria interna deste Regional deve considerar as orientações constantes nos itens de 22 a 25 do anexo V da Portaria CNJ nº 162/2021 com a finalidade de garantir qualidade das auditorias de segurança da informação.

Art. 6º A unidade de gestão de segurança da informação, com apoio das demais unidades administrativas do órgão, em especial a unidade de tecnologia da informação, deve planejar e coordenar a implementação das práticas constantes nos itens de 26 a 37 do anexo V da Portaria CNJ nº 162/2021 com a finalidade de aprimorar continuamente a resiliência cibernética do TRT18.

## CAPÍTULO IV
## DO MANUAL “GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS”

Art. 7º Compete à unidade de gestão de segurança da informação deste Regional propor nova regulamentação e processo de gestão de identidade e controle de acessos em conformidade com as recomendações contidas nos itens de 4 a 7 do anexo VI da Portaria CNJ nº 162/2021, atualizando ou substituindo o atual conjunto de diretrizes sobre o tema normatizado na “Política de Controle de Acessos - PO02” deste Regional.

## CAPÍTULO V
## DO MANUAL “POLÍTICA DE EDUCAÇÃO E CULTURA EM SEGURANÇA

Biblioteca Digital

CIBERNÉTICA DO PODER JUDICIÁRIO”

Art. 8º Compete à unidade de gestão de segurança da informação:

I – propor à escola de formação do TRT18 os temas prioritários a serem considerados em ações de formação, capacitação, reciclagem, fomento e conscientização em segurança cibernética;

II - propor à unidade de gestão de pessoas um conjunto de competências mínimas necessárias para compor a matriz de competências do TRT18 relacionadas à segurança cibernética;

III – propor à unidade de comunicação social os temas prioritários de segurança cibernética para inclusão no planejamento anual da unidade.

## CAPÍTULO VI
## DA EVOLUÇÃO DA MATURIDADE NA ADOÇÃO DOS MANUAIS

Art. 9º Os anexos de I a IV desta Portaria devem ser usados como listas para verificação do nível de maturidade na adoção (grau de implementação) dos manuais de referência da ENSEC-PJ.

Art. 10. A escala para apoiar a medida do grau de implementação é formada pelos seguintes níveis:

I – “não implementado” (requisito atendido ou medida de segurança implementada de 0% a 24,9% das situações, ex.: em ativos tecnológicos, em dados tratados, em processos de trabalho, em pessoas envolvidas etc.), valendo 0,00 ponto;

II – “implementado em menor parte” (a implementação abrange de 25% a 49,9% das situações aplicáveis), valendo 0,25 ponto;

III – “implementado parcialmente” (de 50% a 74,9%), valendo 0,50 ponto;

IV – “implementado em maior parte” (de 75% a 99,9%), valendo 0,75 ponto; e

V – “implementado totalmente” (100%), valendo 1,00 ponto.

Biblioteca Digital

Parágrafo único. Especificamente para o manual “Proteção de Infraestruturas Críticas de TIC”, deve-se utilizar os seguintes níveis de maturidade, que também servirão de insumo para o processo gestão de riscos de segurança da informação: *(parágrafo incluído pela Portaria TRT18 n° 720/2024)*

I – “1” (a medida de segurança não é implementada ou é implementada de forma inconsistente), valendo 0,00 ponto; *(alínea incluída pela Portaria TRT18 n° 720/2024)*

II – “2” (a medida de segurança é implementada integralmente em alguns ativos ou parcialmente em todos os ativos), valendo 0,25 ponto; *(alínea incluída pela Portaria TRT18 n° 720/2024)*

III – “3” (a medida de segurança é implementada em todos os ativos), valendo 0,50 ponto; *(alínea incluída pela Portaria TRT18 n° 720/2024)*

IV – “4” (a medida de segurança é testada e as inconsistências são corrigidas), valendo 0,75 ponto; e *(alínea incluída pela Portaria TRT18 n° 720/2024)*

V – “5” (a medida de segurança possui mecanismos que garantem uma implementação consistente ao longo do tempo), valendo 1,00 ponto. *(alínea incluída pela Portaria TRT18 n° 720/2024)*

Art. 11. O grau de implementação de um manual é calculado em função da soma da pontuação de cada item da lista, dividida pelo total de itens e multiplicada por 100.

Art. 12. Compete à unidade de gestão de segurança da informação:

I – identificar e cientificar, junto às unidades administrativas do TRT18, os responsáveis pela implementação de medidas de segurança ou pelo atendimento de requisitos elencados na lista para verificação de cada manual;

II – esclarecer aos envolvidos qual o escopo aplicável de cada medida de segurança ou requisito a ser atendido, quando necessário;

III – obter uma linha de base para planejamento estratégico, ou seja, levantar com os responsáveis o grau de implementação (em percentual) de cada manual de referência;

IV – propor à Alta Administração, por meio do colegiado temático de segurança da informação e em conjunto com as unidades administrativas do TRT18 envolvidas, plano de metas anuais até 2026 para a evolução da maturidade na adoção de cada manual de referência a partir da linha de base levantada;

V - relatar anualmente ao colegiado temático de segurança da informação o andamento do planejamento e da execução das ações para a evolução da maturidade na adoção de cada manual, assim como o respectivo nível de maturidade alcançado;

VI - assegurar o alinhamento do planejamento e das ações de

Biblioteca Digital

implementação dos manuais ao planejamento estratégico e de gestão do TRT18.

Parágrafo único. Em substituição à obtenção de linha de base e proposição de plano de metas, referidos nos incisos III e IV, a evolução da maturidade na adoção do manual “Proteção de Infraestrtururas Críticas de TIC” deverá ser realizada por meio de ciclos de gestão de riscos, tão logo seja implementado um processo de gestão de riscos de segurança da informação que utilize metodologia compatível com o CIS v8. *(parágrafo incluído pela Portaria TRT18 n° 720/2024)*

Art. 13. Compete às unidades administrativas envolvidas na implementação dos manuais de referência fazer constar em seus documentos oficiais de planejamento as ações necessárias à evolução do nível de maturidade na adoção dos manuais conforme plano de metas aprovado pela Alta Administração, cuidando de tomar as providências necessárias à efetiva execução das mesmas.

## CAPÍTULO VII
## DAS DISPOSIÇÕES FINAIS

Art. 14. Esta Portaria entra em vigor na data de sua publicação.

Publique-se no Diário Eletrônico da Justiça do Trabalho.

***(assinado eletronicamente)***
**DANIEL VIANA JÚNIOR**
Desembargador-Presidente
TRT da 18ª Região

Biblioteca Digital

**ANEXO I**

Lista para verificação do grau de implementação do manual
"PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC"

| Controle | Medida de Segurança | Título | IG1 | IG2 | IG3 | Nível/Grau de implementação |
|---|---|---|---|---|---|---|
| **1** | | **Inventário e controle de ativos corporativos** | * | * | * | |
| 1 | 1.1 | Estabelecer e manter um inventário detalhado de ativos corporativos | x | x | x | |
| 1 | 1.2 | Endereçar ativos não autorizados | x | x | x | |
| 1 | 1.3 | Usar uma ferramenta de descoberta ativa | | x | x | |
| 1 | 1.4 | Usar o Dynamic Host Configuration Protocol (DHCP) para atualizar o inventário de ativos corporativos | | x | x | |
| 1 | 1.5 | Usar uma ferramenta de descoberta passiva | | | x | |
| **2** | | **Inventário e controle de ativos de software** | * | * | * | |
| 2 | 2.1 | Estabelecer e manter um inventário de software | x | x | x | |
| 2 | 2.2 | Assegurar que o software autorizado seja atualmente suportado | x | x | x | |
| 2 | 2.3 | Endereçar o software não autorizado | x | x | x | |
| 2 | 2.4 | Utilizar ferramentas automatizadas de inventário de software | | x | x | |
| 2 | 2.5 | Lista de permissões de Software autorizado | | x | x | |
| 2 | 2.6 | Lista de permissões de bibliotecas autorizadas | | x | x | |
| 2 | 2.7 | Lista de permissões de Scripts autorizados | | | x | |
| **3** | | **Proteção de dados** | * | * | * | |
| 3 | 3.1 | Estabelecer e manter um processo de gestão de dados | x | x | x | |
| 3 | 3.2 | Estabelecer e manter um inventário de dados | x | x | x | |
| 3 | 3.3 | Configurar listas de controle de acesso a dados | x | x | x | |
| 3 | 3.4 | Aplicar retenção de dados | x | x | x | |
| 3 | 3.5 | Descartar dados com segurança | x | x | x | |
| 3 | 3.6 | Criptografar dados em dispositivos de usuário final. | x | x | x | |
| 3 | 3.7 | Estabelecer e manter um esquema de classificação de dados | | x | x | |
| 3 | 3.8 | Documentar Fluxos de Dados | | x | x | |
| 3 | 3.9 | Criptografar dados em mídia removível | | x | x | |
| 3 | 3.10 | Criptografar dados sensíveis em trânsito | | x | x | |
| 3 | 3.11 | Criptografar dados sensíveis em repouso | | x | x | |
| 3 | 3.12 | Segmentar o processamento e o armazenamento de dados com base na sensibilidade | | x | x | |
| 3 | 3.13 | Implantar uma solução de prevenção contra perda de dados | | | x | |
| 3 | 3.14 | Registrar o acesso a dados sensíveis | | | x | |
| **4** | | **Configuração segura de ativos corporativos e software** | * | * | * | |
| 4 | 4.1 | Estabelecer e manter um processo de configuração segura | x | x | x | |
| 4 | 4.2 | Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede | x | x | x | |

Biblioteca Digital

| Controle | Medida de Segurança | Título | IG1 | IG2 | IG3 | Nível/Grau de implementação |
|---|---|---|---|---|---|---|
| 4 | 4.3 | Configurar o bloqueio automático de sessão nos ativos corporativos | x | x | x | |
| 4 | 4.4 | Implementar e gerenciar um firewall nos servidores | x | x | x | |
| 4 | 4.5 | Implementar e gerenciar um firewall nos dispositivos de usuário final | x | x | x | |
| 4 | 5.6 | Gerenciar com segurança os ativos e software corporativos | x | x | x | |
| 4 | 4.7 | Gerenciar contas padrão nos ativos e software corporativos | x | x | x | |
| 4 | 4.8 | Desinstalar ou desativar serviços desnecessários nos ativos e software corporativos | | x | x | |
| 4 | 4.9 | Configurar servidores DNS confiáveis nos ativos corporativos | | x | x | |
| 4 | 4.10 | Impor o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final | | x | x | |
| 4 | 4.11 | Impor a capacidade de limpeza remota nos dispositivos portáteis do usuário final | | x | x | |
| 4 | 4.12 | Separar os Espaços de Trabalho Corporativos nos dispositivos móveis | | | x | |
| **5** | | **Gestão de contas** | * | * | * | |
| 5 | 5.1 | Estabelecer e manter um inventário de contas | x | x | x | |
| 5 | 5.2 | Usar senhas exclusivas | x | x | x | |
| 5 | 5.3 | Desabilitar contas inativas | x | x | x | |
| 5 | 5.4 | Restringir privilégios de administrador a contas de Administrador dedicadas | x | x | x | |
| 5 | 5.5 | Estabelecer e manter um inventário de contas de serviço | | x | x | |
| 5 | 5.6 | Centralizar a gestão de contas | | x | x | |
| **6** | | **Gestão do controle de acesso** | * | * | * | |
| 6 | 6.1 | Estabelecer um Processo de Concessão de Acesso | x | x | x | |
| 6 | 6.2 | Estabelecer um Processo de Revogação de Acesso | x | x | x | |
| 6 | 6.3 | Exigir MFA para aplicações expostas externamente | X | x | x | |
| 6 | 6.4 | Exigir MFA para acesso remoto à rede | x | x | x | |
| 6 | 6.5 | Exigir MFA para acesso administrativo | x | x | x | |
| 6 | 6.6 | Estabelecer e manter um inventário de sistemas de autenticação e autorização | | x | x | |
| 6 | 6.7 | Centralizar o controle de acesso | | x | x | |
| 6 | 6.8 | Definir e manter o controle de acesso baseado em funções | | | x | |
| **7** | | **Gestão contínua de vulnerabilidades** | * | * | * | |
| 7 | 7.1 | Estabelecer e manter um processo de gestão de vulnerabilidade | x | x | x | |
| 7 | 7.2 | Estabelecer e manter um processo de remediação | x | x | x | |
| 7 | 7.3 | Executar a gestão automatizada de patches do sistema operacional | x | x | x | |
| 7 | 7.4 | Executar a gestão automatizada de patches de aplicações | x | x | x | |
| 7 | 7.5 | Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos internos | | x | x | |

Biblioteca Digital

| Controle | Medida de Segurança | Título | IG1 | IG2 | IG3 | Nível/Grau de implementação |
|---|---|---|---|---|---|---|
| 7 | 7.6 | Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos expostos externamente | | x | x | |
| 7 | 7.7 | Corrigir vulnerabilidades detectadas | | x | x | |
| **8** | | **Gestão de registros de auditoria** | * | * | * | |
| 8 | 8.1 | Estabelecer e manter um processo de gestão de log de auditoria | x | x | x | |
| 8 | 8.2 | Coletar logs de auditoria | x | x | x | |
| 8 | 8.3 | Garantir o armazenamento adequado do registro de auditoria | x | x | x | |
| 8 | 8.4 | Padronizar a sincronização de tempo | | x | x | |
| 8 | 8.5 | Coletar logs de auditoria detalhados | | x | x | |
| 8 | 8.6 | Coletar logs de auditoria de consulta dns | | x | x | |
| 8 | 8.7 | Coletar logs de auditoria de requisição de url | | x | x | |
| 8 | 8.8 | Coletar logs de auditoria de linha de comando | | x | x | |
| 8 | 8.9 | Centralize Audit Logs | | x | x | |
| 8 | 8.10 | Retain Audit Logs | | x | x | |
| 8 | 8.11 | Conduct Audit Log Reviews | | x | x | |
| 8 | 8.12 | Collect Service Provider Logs | | | x | |
| **9** | | **Proteções de e-mail e navegador Web** | * | * | * | |
| 9 | 9.1 | Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente | x | x | x | |
| 9 | 9.2 | Usar serviços de filtragem de DNS | x | x | x | |
| 9 | 9.3 | Manter e impor filtros de URL baseados em rede | | x | x | |
| 9 | 9.4 | Restringir extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas | | x | x | |
| 9 | 9.5 | Implementar o DMARC | | x | x | |
| 9 | 9.6 | Bloquear tipos de arquivo desnecessários | | x | x | |
| 9 | 9.7 | Implantar e manter proteções antimalware de servidor de e-mail | | | x | |
| **10** | | **Defesas contra malware** | * | * | * | |
| 10 | 10.1 | Instalar e manter um software anti-malware | x | x | x | |
| 10 | 10.2 | Configurar atualizações automáticas de assinatura anti-malware | x | x | x | |
| 10 | 10.3 | Desabilitar a execução e reprodução automática para mídias removíveis | x | x | x | |
| 10 | 10.4 | Configurar a varredura anti-malware automática de mídia removivel | | x | x | |
| 10 | 10.5 | Habilitar recursos anti-exploração | | x | x | |
| 10 | 10.6 | Gerenciar o software anti-malware de maneira centralizada | | x | x | |
| 10 | 10.7 | Usar software anti-malware baseado em comportamento | | x | x | |
| **11** | | **Recuperação de dados** | * | * | * | |
| 11 | 11.1 | Estabelecer e manter um processo de recuperação de dados | x | x | x | |

Biblioteca Digital

| Controle | Medida de Segurança | Título | IG1 | IG2 | IG3 | Nível/Grau de implementação |
|---|---|---|---|---|---|---|
| 11 | 11.2 | Executar backups automatizados | x | x | x | |
| 11 | 11.3 | Proteger os dados de recuperação | x | x | x | |
| 11 | 11.4 | Estabelecer e manter uma instância isolada de dados de recuperação | x | x | x | |
| 11 | 11.5 | Testar os dados de recuperação | | x | x | |
| **12** | | **Gestão da infraestrutura de rede** | * | * | * | |
| 12 | 12.1 | Assegurar que a infraestrutura de rede esteja atualizada | x | x | x | |
| 12 | 12.2 | Estabelecer e manter uma arquitetura de rede segura | | x | x | |
| 12 | 12.3 | Gerenciar infraestrutura de rede com segurança | | x | x | |
| 12 | 12.4 | Estabelecer e manter diagrama(s) de arquitetura | | x | x | |
| 12 | 12.5 | Centralizar a autenticação, autorização e auditoria (AAA) de rede | | x | x | |
| 12 | 12.6 | Usar protocolos de comunicação e gestão de rede seguros | | x | x | |
| 12 | 12.7 | Assegurar que os dispositivos remotos utilizem uma VPN e estejam se conectando a uma infraestrutura AAA da empresa | | x | x | |
| 12 | 12.8 | Estabelecer e manter recursos de computação dedicados para todo o trabalho administrativo | | | x | |
| **13** | | **Monitoramento e defesa da Rede** | * | * | * | |
| 13 | 13.1 | Centralizar o alerta de eventos de segurança | | x | x | |
| 13 | 13.2 | Implantar solução de detecção de intrusão baseada em host | | x | x | |
| 13 | 13.3 | Implantar uma solução de detecção de intrusão de rede | | x | x | |
| 13 | 13.4 | Realizar filtragem de tráfego entre segmentos de rede | | x | x | |
| 13 | 13.5 | Gerenciar controle de acesso para ativos remotos | | x | x | |
| 13 | 13.6 | Coletar logs de fluxo de tráfego da rede | | x | x | |
| 13 | 13.7 | Implantar solução de prevenção de intrusão baseada em host | | | x | |
| 13 | 13.8 | Implantar uma solução de prevenção de intrusão de rede | | | x | |
| 13 | 13.9 | Implantar controle de acesso no nível de porta | | | x | |
| 13 | 13.10 | Executar filtragem da camada de aplicação | | | x | |
| 13 | 13.11 | Ajustar Limites de Alerta de Eventos de Segurança | | | x | |
| **14** | | **Conscientização sobre segurança e treinamento de competências** | * | * | * | |
| 14 | 14.1 | Estabelecer e manter um programa de conscientização de segurança | x | x | x | |
| 14 | 14.2 | Treinar membros da força de trabalho para reconhecer ataques de engenharia social | x | x | x | |
| 14 | 14.3 | Treinar membros da força de trabalho nas melhores práticas de autenticação | x | x | x | |
| 14 | 14.4 | Treinar a força de trabalho nas Melhores Práticas de Tratamento de Dados | x | x | x | |
| 14 | 14.5 | Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados | x | x | x | |
| 14 | 14.6 | Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança | x | x | x | |

Biblioteca Digital

| Controle | Medida de Segurança | Título | IG1 | IG2 | IG3 | Nível/Grau de implementação |
|---|---|---|---|---|---|---|
| 14 | 14.7 | Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança | x | x | x | |
| 14 | 14.8 | Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras | x | x | x | |
| 14 | 14.9 | Conduzir treinamento de competências e conscientização de segurança para funções específicas | | x | x | |
| **15** | | **Gestão de provedor de serviços** | * | * | * | |
| 15 | 15.1 | Estabelecer e manter um inventário de provedores de serviços | x | x | x | |
| 15 | 15.2 | Estabelecer e manter uma política de gestão de provedores de serviços | | x | x | |
| 15 | 15.3 | Classificar provedores de serviços | | x | x | |
| 15 | 15.4 | Garantir que os contratos do provedor de serviços incluam requisitos de segurança | | x | x | |
| 15 | 14.5 | Avaliar provedores de serviços | | | x | |
| 15 | 15.6 | Monitorar provedores de serviços | | | x | |
| 15 | 15.7 | Descomissionar com segurança os provedores de serviços | | | x | |
| **16** | | **Segurança de aplicações** | * | * | * | |
| 16 | 16.1 | Estabelecer e manter um processo seguro de desenvolvimento de aplicações | | x | x | |
| 16 | 16.2 | Estabelecer e manter um processo para aceitar e endereçar vulnerabilidades de software | | x | x | |
| 16 | 16.3 | Executar análise de causa raiz em vulnerabilidades de segurança | | x | x | |
| 16 | 16.4 | Estabelecer e gerenciar um inventário de componentes de software de terceiros | | x | x | |
| 16 | 16.5 | Usar componentes de software de terceiros atualizados e confiáveis | | x | x | |
| 16 | 16.6 | Estabelecer e manter um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações | | x | x | |
| 16 | 16.7 | Usar modelos de configurações de segurança padrão para infraestrutura de aplicações | | x | x | |
| 16 | 16.8 | Separar sistemas de produção e não produção | | x | x | |
| 16 | 16.9 | Treinar desenvolvedores em conceitos de segurança de aplicações e codificação segura | | x | x | |
| 16 | 16.10 | Aplicar princípios de design seguro em arquiteturas de aplicações | | x | x | |
| 16 | 16.11 | Aproveitar os módulos ou serviços controlados para componentes de segurança de aplicações | | x | x | |
| 16 | 16.12 | Implementar verificações de segurança em nível de código | | | x | |
| 16 | 16.13 | Realizar teste de invasão de aplicação | | | x | |
| 16 | 16.14 | Conduzir aplicações de modelagem de ameaças | | | x | |
| **17** | | **Gestão de respostas a incidentes** | * | * | * | |
| 17 | 17.1 | Designar Pessoal para Gerenciar Tratamento de Incidentes | x | x | x | |
| 17 | 17.2 | Estabelecer e manter informações de contato para relatar incidentes de segurança | x | x | x | |

Biblioteca Digital

| Controle | Medida de Segurança | Título | IG1 | IG2 | IG3 | Nível/Grau de implementação |
|---|---|---|---|---|---|---|
| 17 | 17.3 | Estabelecer e manter um processo corporativo para relatar incidentes | x | x | x | |
| 17 | 17.4 | Estabelecer e manter um processo de resposta a incidentes | | x | x | |
| 17 | 17.5 | Atribuir funções e responsabilidades chave | | x | x | |
| 17 | 17.6 | Definir mecanismos de comunicação durante a resposta a incidente | | x | x | |
| 17 | 17.7 | Conduzir exercícios de resposta a incidentes rotineiros | | x | x | |
| 17 | 17.8 | Conduzir análises pós-incidente | | x | x | |
| 17 | 17.9 | Estabelecer e manter limites de incidentes de segurança | | | x | |
| **18** | | **Testes de invasão** | * | * | * | |
| 18 | 18.1 | Estabelecer e manter um programa de teste de invasão | | x | x | |
| 18 | 18.2 | Realizar testes de invasão externos periódicos | | x | x | |
| 18 | 18.3 | Corrigir as descobertas do teste de invasão | | x | x | |
| 18 | 18.4 | Validar as Medidas de Segurança | | | x | |
| 18 | 18.5 | Realizar testes de invasão internos periódicos | | | x | |

Biblioteca Digital

**ANEXO II**

Lista para verificação do grau de implementação do manual

"PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL"

| Seq. | Item | Referencial | Nível/Grau de Implementação |
|---|---|---|---|
| **1.** | **Padrões mínimos de Gestão de Riscos de Segurança da Informação** | | |
| 1.1. | Existe um Processo de Gestão de Riscos de Segurança Cibernética estabelecido. | NBR 27.005:2019 | |
| 1.2. | O Processo de Gestão de Riscos de Segurança Cibernética é chancelado pela administração superior. | NBR 27.005:2019 | |
| 1.3. | O Processo de Gestão de Riscos de Segurança Cibernética está associado ao Sistema de Gestão de Segurança da Informação. | NBR 27.005:2019 | |
| 1.4. | O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Estabelecimento de Contexto definida. | NBR 27.005:2019 | |
| 1.5. | O Processo de Gestão de Riscos de Segurança Cibernética possui um subprocesso de Avaliação de Riscos definido. | NBR 27.005:2019 | |
| 1.5.1. | O subprocesso de Avaliação de Riscos contempla atividade de Identificação de Riscos. | NBR 27.005:2019 | |
| 1.5.2. | O subprocesso de Avaliação de Riscos contempla atividade de Análise de Riscos. | NBR 27.005:2019 | |
| 1.5.3. | O subprocesso de Avaliação de Riscos contempla atividade de Avaliação de Riscos. | NBR 27.005:2019 | |
| 1.5.4. | Critérios para determinação do impacto/criticidade e probabilidade dos riscos de segurança cibernética estão definidos. | NBR 27.005:2019 | |
| 1.5.5. | Critérios para aceitação de riscos de segurança cibernética estão definidos. | NBR 27.005:2019 | |
| 1.6. | O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Tratamento de Riscos definida. | NBR 27.005:2019 | |
| 1.7. | O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Monitoramento e Análise Crítica definida. | NBR 27.005:2019 | |
| 1.8. | O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Comunicação e Consulta definida. | NBR 27.005:2019 | |
| 1.9. | O Processo de Gestão de Riscos de Segurança Cibernética é periodicamente revisado e atualizado. | NBR 27.005:2019 | |
| **2.** | **Previsões para a fiscalização da adequação dos requisitos de segurança inclusive sob contratação externa e/ou criação de rotina de auditorias cruzadas** | | |

Biblioteca Digital

| Seq. | Item | Referencial | Nível/Grau de Implementação |
|---|---|---|---|
| 2.1. | Considerar para, determinação de objetivos, no planejamento anual do programa interno de auditorias do órgão: requisitos de segurança da informação legais, normativos e contratuais, riscos de segurança da informação para as áreas auditadas e clientes da auditoria e, quando aplicável, riscos e oportunidades determinados na fase de planejamento do sistema de gestão de segurança da informação. | ISO 27007:2018 | |
| 2.2. | Para determinar a abrangência e as prioridades das auditorias sobre requisitos de segurança, considerar: complexidade dos sistemas a serem auditados, número de localidades similares, importância da preservação da confidencialidade, integridade e disponibilidade das informações e riscos para o negócio. Quando aplicável, considerar tamanho, complexidade e riscos para o sistema de gestão de segurança da informação. | ISO 27007:2018 | |
| 2.3. | Considerar na avaliação de riscos de execução das auditorias requisitos legais, normativos e contratuais de confidencialidade e outros tipos, se relevantes. | ISO 27007:2018 | |
| 2.4. | Utilizar termos de confidencialidade, técnicas de anonimização e cláusulas contratuais específicas quando requerido por auditados e outras partes pertinentes. | ISO 27007:2018 | |
| 2.5. | Estabelecer um cronograma de trabalho das auditorias que permitam uma análise crítica dos auditores sobre a eficácia das ações de abordagem de riscos de segurança da informação e, quando aplicável, ao sistema de gestão de segurança da informação. | ISO 27007:2018 | |
| 2.6. | Considerar como possíveis objetivos de uma auditoria individual, quando aplicável, considerando o escopo de um sistema de gestão de segurança da informação: avaliar se o órgão identifica e aborda os requisitos de segurança da informação, avaliar processos que suportam os requisitos de segurança da informação e determinar a abrangência da conformidade controles de segurança da informação com os requisitos e procedimentos determinados. | ISO 27007:2018 | |
| 2.7. | Considerar os riscos de segurança da informação na determinação do escopo de uma auditoria individual e, quando aplicável, os riscos para o sistema de gestão de segurança da informação. | ISO 27007:2018 | |
| 2.8. | Considerar como critérios de uma auditoria individual para determinar a conformidade com requisitos de segurança, quando aplicáveis: política de segurança da informação; objetivos da segurança da informação; políticas e procedimentos adotados pelo auditado; requisitos legais normativos, contratuais e outros relevantes para o auditado; critérios de riscos de segurança da informação do auditado e os processos de avaliação e tratamento de riscos; justificativas para inclusão e exclusão de controles para atendimentos de requisitos ou ao estabelecimento de um sistema de gestão de segurança da informação; definição de controles para tratamento apropriado de riscos de segurança da informação; método e critérios usados para monitoramento, medição, análise e avaliação de desempenho da gestão de segurança da informação ou do sistema de gestão de segurança da informação; requisitos de segurança da informação de clientes, fornecedores ou terceirizados. | ISO 27007:2018 | |

Biblioteca Digital

| Seq. | Item | Referencial | Nível/Grau de Implementação |
|---|---|---|---|
| 2.9. | No caso de auditorias integradas/compartilhadas, conjuntas, contratadas ou cruzadas providenciar, necessariamente, contrato, termos de cooperação técnica, convênios ou instrumento que formalize a prestação da auditoria nos moldes especificados e, obrigatoriamente, acompanhados dos devidos acordos de confidencialidade assinados pelas partes envolvidas. | ISO 27007:2018 | |
| 2.10. | Incluir no conhecimento global da equipe de auditoria conhecimentos sobre gestão de riscos de segurança da informação, suficiente para avaliar métodos usados, e gestão de segurança da informação, suficiente para avaliar a implementação de requisitos de segurança da informação, ou, quando aplicável, o funcionamento de um sistema de gestão de segurança da informação. | ISO 27007:2018 | |
| 2.11. | No contato inicial com o auditado comprovar, por instrumento apropriado, que os auditores obtiveram autorização para acessos às informações necessárias para a auditoria. | ISO 27007:2018 | |
| 2.12. | Determinar e formalizar a inviabilidade ou comprometimento de algum aspecto da auditoria no caso de negação de acesso pelo auditado às evidências que contemplem informações sensíveis ou sigilosas. | ISO 27007:2018 | |
| 2.13. | Conscientizar a equipe de auditoria, especialmente o auditor líder, que a atividade de auditoria implica ampliação de riscos das informações do auditado (vazamento, exclusão acidental, alteração intencional, indisponibilidade de serviço etc.). | ISO 27007:2018 | |
| 2.14. | Acordar, com as áreas envolvidas e impactadas, por meio do auditor líder, melhor cronograma para interrupções e perda de desempenho de serviços, quando imprescindíveis para as atividades de auditoria. | ISO 27007:2018 | |
| 2.15. | Equipe de auditoria deve classificar e tratar documentos de trabalho de acordo com suas classificações originais quanto a sigilo ou à sensibilidade. | ISO 27007:2018 | |
| 2.16. | Equipe de auditoria deve validar a documentação de trabalho de acordo com escopo e critérios da auditoria, confirmando se os controles estão relacionados com os processos de análise e tratamento de riscos e se são rastreáveis em relação aos objetivos e política de segurança da informação. | ISO 27007:2018 | |
| 2.17. | Basear a coleta e validação de informações e técnicas de auditoria de TIC, que incluem: análise crítica de informação documentada (logs, trilhas, arquivos, massas de dados, configurações etc.), visitas às instalações de processamento de informações para inspeção visual, observação de processo e controles relacionados aos requisitos de segurança da informação e, quando aplicável, ao sistema de gestão de segurança da informação e uso de ferramentas automatizadas de auditoria. | ISO 27007:2018 | |
| 2.18. | Não comprometer a classificação ou sensibilidade de uma evidência em razão da indisponibilidade desta para avaliação da auditoria. O auditor líder deve tratar o assunto no relatório de auditoria, incluindo o impacto nos resultados causado pela ausência da evidência. | ISO 27007:2018 | |
| 2.19. | Adotar medidas para garantir a confidencialidade do relatório, incluindo a encriptação dele quando | ISO 27007:2018 | |

Biblioteca Digital

| Seq. | Item | Referencial | Nível/Grau de Implementação |
|---|---|---|---|
| | em meio eletrônico. | | |
| 2.20. | Selecionar auditores para auditorias tomando como base inclusive: quando aplicável, tipos de negócios suportados, complexidade, abrangência, diversidade tecnológica e avaliações anteriores do sistema de gestão de segurança da informação ou relacionados aos requisitos de segurança auditados; abrangência de acordos e contratos com terceiros relacionados aos requisitos de segurança ou, quando aplicável, ao escopo do sistema de gestão de segurança da informação; normas, requisitos legais e outros requisitos do programa de auditoria. | ISO 27007:2018 | |
| 2.21. | Incluir no plano de capacitação de auditores conhecimentos sobre tecnologia da informação, segurança da informação e conhecimentos inerentes aos requisitos de negócio da organização, inclusive legais, normativos e contratuais. | ISO 27007:2018 | |
| 2.22. | Avaliar a conformidade de *requisitos de segurança da informação* por meio de auditorias de forma contínua e planejada com o objetivo de apoiar o aperfeiçoamento da gestão de segurança da informação no órgão, garantir a *conformidade legal, normativa e contratual* sobre segurança da informação e com requisitos de referência sobre *boas práticas de segurança da informação e gestão de segurança da informação*. | NC 11 IN01/DSIC/GSIPR | |
| 2.23. | No que diz respeito às auditorias de segurança da informação, basear o planejamento do programa de auditorias na análise e avaliação de riscos. | NC 11 IN01/DSIC/GSIPR | |
| 2.24. | No que diz respeito ao planejamento da auditoria individual de segurança da informação, considerar a análise e avaliação de riscos na determinação de escopo e objetivos da auditoria. | NC 11 IN01/DSIC/GSIPR | |
| 2.25. | Entregar o relatório da auditoria individual para a alta administração do órgão e, quando existente, para o gestor de segurança da informação do órgão. | NC 11 IN01/DSIC/GSIPR | |
| 2.26. | Adequar, de forma geral ou específica para segurança da informação, normativos internos dos órgãos para admitir as formas de auditoria: terceirizada (executada por terceirizado contratado), integrada/compartilhada (área de auditoria de um órgão audita o outro órgão com a participação da área de auditoria do auditado) e, quando previsto em normativo próprio do Poder Judiciário, cruzada (área de auditoria de um órgão audita o outro órgão sem a participação da área de auditoria do auditado). | Res. 309 de 11/03/2020 do CNJ | |
| 2.27. | Em relação aos requisitos de segurança da informação, considerar nos planejamentos dos programas de auditoria e das auditorias individuais as auditorias nas formas: terceirizada (executada por terceirizado contratado), integrada/compartilhada (área de auditoria de um órgão audita o outro órgão com a participação da área de auditoria do auditado) ou, quando previsto em normativo próprio do Poder Judiciário, cruzada (área de auditoria de um órgão audita o outro órgão sem a participação da área de auditoria do auditado). | Res. 309 de 11/03/2020 do CNJ | |

Biblioteca Digital

| Seq. | Item | Referencial | Nível/Grau de Implementação |
|---|---|---|---|
| **3.** | **Confiança digital, prevenção e mitigação de ameaças cibernéticas** | | |
| 3.1. | A organização possui mecanismos de resiliência cibernética que implementam uma fase de **IDENTIFICAÇÃO** de ameaças. | *Framework* de resiliência cibernética. IDC, 2020. | |
| 3.2. | A organização possui mecanismos de resiliência cibernética que implementam uma fase de **PROTEÇÃO** de ativos. | *Framework* de resiliência cibernética. IDC, 2020. | |
| 3.3. | A organização possui mecanismos de resiliência cibernética que implementam uma fase de **DETECÇÃO** de ameaças. | *Framework* de resiliência cibernética. IDC, 2020. | |
| 3.4. | A organização possui mecanismos de resiliência cibernética que implementam uma fase de **RESPOSTAS** a ameaças. | *Framework* de resiliência cibernética. IDC, 2020. | |
| 3.5. | A organização possui mecanismos de resiliência cibernética que implementam uma fase de **RECUPERAÇÃO**. | *Framework* de resiliência cibernética. IDC, 2020. | |

Biblioteca Digital

**ANEXO III**

Lista para verificação do grau de implementação do manual
"GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS"

| Seq. | Item | Referencial | Nível/Grau de Implementação |
|---|---|---|---|
| 1 | Formalizar Política de Gestão de Identidade e Controle de Acesso em conformidade com as diretrizes previstas neste Manual e boas práticas de segurança. | *Anexo VI P.CNJ 162/2021* | |
| 2 | Aplicação dos critérios de padronização de nome de usuário e de conta de e-mail. | *Anexo VI P.CNJ 162/2021* | |
| 3 | Realizar processo de revisão para identificar privilégios excessivos de usuários, administradores de TI e de contas de serviço. | *Anexo VI P.CNJ 162/2021* | |
| 4 | Definir e utilizar um processo para a revogação de direitos de acesso, desabilitando imediatamente as contas no momento do término do vínculo ou da alteração das responsabilidades de um servidor ou prestador de serviços. | *Anexo VI P.CNJ 162/2021* | |
| 5 | Manter um inventário de cada um dos sistemas de autenticação da organização, incluindo aqueles internos ou em provedores de serviços remotos. | *Anexo VI P.CNJ 162/2021* | |
| 6 | Adotar modelo de controle de acesso baseado em funções (RBAC). | *Anexo VI P.CNJ 162/2021* | |
| 7 | Registrar em logs acessos, operações e período para fins de auditoria. | *Anexo VI P.CNJ 162/2021* | |
| 8 | Garantir que todas as contas tenham uma data de expiração de senha e que isso seja configurado e monitorado. | *Anexo VI P.CNJ 162/2021* | |
| 9 | Gerenciar acessos e ações executadas com credenciais privilegiadas, não utilizando credenciais genéricas e de uso compartilhado. | *Anexo VI P.CNJ 162/2021* | |
| 10 | Criptografar ou embaralhar (hash) com a utilização de salt as credenciais de autenticação armazenadas. | *Anexo VI P.CNJ 162/2021* | |
| 11 | Utilizar criptografia no canal de comunicação ao trafegar credenciais de acesso. | *Anexo VI P.CNJ 162/2021* | |
| 14 | Configurar o acesso a todas as contas por meio da menor quantidade de pontos de autenticação centralizados possível, incluindo sistemas de rede, segurança e sistemas em nuvem. | *Anexo VI P.CNJ 162/2021* | |
| 15 | Garantir que todas as contas (usernames) e senhas sejam transmitidas em rede utilizando canais criptografados. | *Anexo VI P.CNJ 162/2021* | |

Biblioteca Digital

| Seq. | Item | Referencial | Nível/Grau de Implementação |
|---|---|---|---|
| 16 | Manter um inventário de todas as contas organizadas por sistema de autenticação. | *Anexo VI P.CNJ 162/2021* | |
| 17 | Desabilitar contas, em vez de excluí-las, visando à preservação de trilhas de auditoria. | *Anexo VI P.CNJ 162/2021* | |
| 18 | Desabilitar qualquer conta que não possa ser associada a um processo de negócio ou a um usuário. | *Anexo VI P.CNJ 162/2021* | |
| 19 | Desabilitar automaticamente contas não utilizadas após um período de inatividade pré-definido. | *Anexo VI P.CNJ 162/2021* | |
| 20 | Bloquear automaticamente as estações de trabalho após um período de inatividade pré-definido. | *Anexo VI P.CNJ 162/2021* | |
| 21 | Monitorar tentativas de acesso a contas desativadas, por meio de logs de auditoria. | *Anexo VI P.CNJ 162/2021* | |
| 22 | Segregar as redes de comunicação a depender do grupo dos serviços, sistemas ou usuários. | *Anexo VI P.CNJ 162/2021* | |
| 23 | Implementar controles de acesso físico aos ativos de TIC. | *Anexo VI P.CNJ 162/2021* | |

Biblioteca Digital

**ANEXO IV**

Lista para verificação do grau de implementação do manual

"POLÍTICA DE EDUCAÇÃO E CULTURA EM SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO"

| Seq. | Item | Referencial | Nível/Grau de Implementação |
|---|---|---|---|
| 1 | A escola de formação do TRT da 18ª Região adota medidas para a concretização da Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário - PECSC-PJ contida no manual de referência do anexo VII. | *Portaria CNJ nº 162/2021, anexo VII, item 3.1.1* | |
| 2 | A unidade de gestão de pessoas adota, no que couber, as medidas viabilizadoras indicadas no manual de referência do anexo VII. | *Portaria CNJ nº 162/2021, anexo VII, item 3.2* | |
| 3 | A unidade de comunicação social adota as medidas de planejamento indicadas no manual de referência do anexo VII. | *Portaria CNJ nº 162/2021, anexo VII, item 3.3* | |
| 4 | O TRT da 18ª Região apresenta ao CNJ, no início de cada ano, o relatório que comprova a efetividade das ações realizadas no exercício anterior e o respectivo desempenho dos usuários e profissionais treinados e conscientizados em cibersegurança. | *Portaria CNJ nº 162/2021, anexo VII, item 4.2* | |

Goiânia, 18 de dezembro de 2022.
[assinado eletronicamente]

DANIEL VIANA JÚNIOR

DESEMB. PRES. DE TRIBUNAL

Biblioteca Digital