ANEXO ÚNICO
(PORTARIA GP nº063/2019)

Norma de tratamento de incidentes de segurança da informação de TIC1

1 Objetivo

Estabelecer diretrizes e procedimentos para o tratamento de incidentes de segurança da informação de TIC no Tribunal Regional do Trabalho da 15ª Região (TRT), com o intuito de restaurar a operação normal dos serviços o mais rápido possível, minimizando os prejuízos à operação do negócio do TRT e atendendo os níveis de serviço acordados.

2 Abrangência

O tratamento de incidentes de segurança da informação de TIC, definido nesta norma, tem seu escopo limitado às situações relacionadas ao ambiente, ativos de informação, projetos e processos de TIC.

3 Referências legais e normativas

ISO ABNT, 2013, NBR ISO 27001: Sistemas de gestão de segurança da informação, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

ISO ABNT, 2013, NBR ISO 27002: Código de prática para gestão de segurança da informação, que fornece diretrizes para práticas de gestão de segurança da informação.

Norma Complementar 01/IN01/DSIC/GSIPR, de 15 de outubro de 2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre a Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14.08.2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Resolução Nº 211 de 15/12/2015 do Conselho Nacional de Justiça (CNJ), que Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

TRT15 - Ato GP Nº 15/2007, de 27 de novembro de 2007. Institui a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 15ª Região.

4 Diretrizes

4.1 Diretrizes gerais

4.1.1 O tratamento de incidentes de segurança da informação de TIC tem em sua gestão como principal objetivo assegurar que incidentes de segurança da informação de TIC sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas.

4.1.2 Os incidentes de segurança da informação de TIC abrangidos por esta norma são os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam os ativos de informação, dados e processos de trabalho relacionados ao ambiente tecnológico do TRT.

4.1.3 Poderão ser analisados os incidentes de segurança da informação dos quais decorram degradação, interrupção ou indisponibilidade de serviço essencial, vulnerabilidades, divulgação, alteração ou destruição de informações, bem como a prática de ato definido como crime ou infração administrativa.

4.1.4 O TRT providenciará dispositivos de monitoramento e ferramentas de segurança, a fim de subsidiar o tratamento de incidentes de segurança da informação de TIC.

4.1.5 O tratamento de incidentes será gerido pela unidade de segurança da informação da SETIC.

4.2 Tratamento de incidentes de segurança da informação de TIC

4.2.1 O tratamento de incidentes de segurança da informação de TIC é contínuo.

4.2.2 A gestão de tratamento de incidentes de segurança da informação de TIC deve observar as seguintes etapas:

Detecção e registro: compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação.

Investigação e contenção: compreende a investigação e o tratamento do incidente, coleta de dados, comunicação às áreas afetadas, proposição e aplicação de ações de contenção, quando necessárias.

Encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente.

Avaliação: compreende a avaliação do histórico de incidentes, por intermédio da consolidação das informações e indicadores, bem como a verificação das oportunidades de melhoria e lições aprendidas.

4.3 Detecção e registro de incidentes de segurança da informação de TIC

4.3.1 Os incidentes, notificados ou detectados, devem ser registrados, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

4.3.2 A notificação de incidente, interna ou externa, deverá ser registrada por qualquer usuário, o mais breve possível, por intermédio da Central de Serviços de TIC.

4.3.3 Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos usuários, sob o risco de violar as normas e regulamentações de segurança da informação que regem a Instituição ou provocar danos aos recursos de TIC.

4.4 Investigação e contenção de incidentes de segurança da informação de TIC

4.4.1 A investigação e o tratamento de incidentes devem ser realizados de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, buscando o retorno das operações à normalidade no menor prazo possível, bem como minimizar futuras ocorrências, por intermédio da proposição de medidas de solução, quando existentes.

4.4.2 A SETIC deverá constituir uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRI), composta por servidores de sua lotação.

4.4.3 A ETRI deve investigar os incidentes e artefatos maliciosos, além de propor e implementar as ações de contenção.

4.4.4 A coleta de evidências dos incidentes de segurança da informação deve ser realizada por pessoal designado pela ETRI ou por ela própria.

4.4.5 Quando o incidente de segurança da informação decorrer de suspeita de descumprimento das normas e regulamentações de segurança da informação, será observado o sigilo durante todo o processo de investigação, ficando as evidências, informações e demais registros restritos aos envolvidos.

4.4.6 Esta investigação deverá ser formalmente autorizada pelo Secretário de TIC ou submetida, quando necessário, ao Comitê de Segurança da Informação.

4.4.7 Quando houver indícios de ilícitos durante o gerenciamento dos incidentes de segurança de TIC, a Administração do TRT e o Comitê de Segurança da Informação deverão ser comunicados, para avaliação das providências cabíveis.

4.5 Encerramento de incidentes de segurança da informação de TIC

O encerramento de um incidente de segurança da informação será realizado pela unidade de segurança da informação da SETIC, que deverá comunicar às demais partes interessadas.

4.6 Avaliação de incidentes de segurança da informação de TIC

4.6.1 O tratamento de incidentes de segurança da informação de TIC será avaliado por intermédio do seu respectivo histórico, buscando identificar as possíveis oportunidades de melhoria.

4.6.2 A avaliação do histórico do tratamento de incidentes será feita pela unidade de segurança da informação da SETIC, com apoio da ETRI.

5 Anexos

É parte integrante desta norma o seguinte anexo: “Tipos de incidentes de segurança da informação de TIC”

Anexo - Tipos de incidentes de segurança da informação de TIC

1 Objetivo

Relacionar os tipos de incidentes de segurança da informação de TIC.

2 Tipos de incidentes de segurança da informação de TIC

Classe do Incidente	Tipo do Incidente	Descrição / Exemplos
Conteúdo Abusivo	Spam	Mensagens de e-mail em massa, não solicitadas pelo destinatário, enviadas em grande quantidade.
	Assédio	Desacreditar ou discriminar alguém, perseguição virtual.
	Pornografia, pornografia infantil, violência	Conteúdo sexual, apologia à violência.
	Hoax	Mensagem eletrônica encaminhada a muitos destinatários e de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas.
Código Malicioso (malware)	Vírus	Software incluído ou inserido intencionalmente em um sistema com finalidade prejudicial. Normalmente é necessária a interação do usuário para ativar o código.
	Worm	
	Trojan	
	Spyware	
	Dialler	
Intrusão	Conta privilegiada comprometida	Comprometimento de um sistema, serviço ou aplicação que pode ter acontecido remotamente ou localmente por meio de acesso não
	Conta não privilegiada comprometida	

	Aplicação comprometida	autorizado
Segurança da Informação	Acesso não autorizado à informação	A segurança da informação pode ser ameaçada por uma conta de usuário válida ou aplicação comprometida que permitam acesso não autorizado à informação. Há, ainda, ataques que interceptam e acessam informações durante a transmissão dos dados pela rede.
	Modificação não autorizada à informação	
Fraude	Direitos autorais	Venda ou instalação de software comercial não licenciado ou material protegido por direitos autorais
	Mascarado	Tipo de ataque no qual uma entidade assume ilegalmente a identidade de outra para tirar benefícios.
	Phishing	Fraude eletrônica, caracterizada pela tentativa de obtenção de dados e informações pessoais com o uso de meios técnicos e de engenharia social.
Outros	Todos os incidentes não categorizados em um dos tipos anteriores devem ser classificados nesta classe.	Quando o número de incidentes nesta categoria aumentar, será o momento de rever esta tabela de classificações.