NORMA COMPLEMENTAR 04, DE 30 DE MARÇO DE 2022

Dispõe sobre o processo de Gestão de Incidentes de Segurança em Redes computacionais no âmbito do IFSertãoPE.

DISPOSIÇÕES PRELIMINARES

Art. 1º A gestão de incidentes de Segurança em Redes Computacionais proporcionará a identificação, o registro e a avaliação de incidentes de Segurança nas Redes de computadores das Unidades organizacionais do IFSertãoPE em tempo hábil, acompanhada por decisões de contenção e/ou solução adequadas.

Art. 2º Estão abrangidos por esta norma os eventos, confirmados ou sob suspeita, relacionados à segurança de sistemas ou redes computacionais, vulnerabilidades de segurança, divulgação, alteração ou destruição de dados, que comprometam o ambiente tecnológico do IFSertãoPE, seus ativos, informações e processos de negócio, além daqueles que contrariem a Política de Segurança da Informação da Instituição, dos quais decorram interrupção, parcial ou total, de serviço essencial ao desempenho das atividades.

CONCEITOS

Art. 3º Para os fins desta Normativa Complementar específica devem ser adotadas as seguintes definições:

I. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II. Informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

III. Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

IV. Unidade organizacional: Repartição, refere-se à Reitoria e a cada campus do IFSertãoPE;

V. Usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, aluno e pessoa da sociedade civil habilitada pela administração para acessar os ativos de informação do IFSertãoPE;

VI. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

DISPOSIÇÕES GERAIS

Art. 4º O processo de Gestão de Incidentes de Segurança em Redes Computacionais deverá ser contínuo e composto pelas seguintes etapas:

I – Detecção e registro: compreende a identificação de incidente ou recebimento de notificação deste, seu registro e obtenção das autorizações necessárias para o encaminhamento de investigação;

II – Investigação e contenção: compreende a investigação e tratamento do incidente, coleta e preservação de evidências, comunicação às áreas afetadas, proposição e aplicação de ações de contenção, quando necessárias.

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

IV – Avaliação: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas.

Art. 5º A notificação de incidente de segurança sob suspeita ou confirmação poderá ser feita por qualquer usuário pelo correio eletrônico para o endereço **etir@ifsertao-pe.edu.br**.

Parágrafo único. A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR do IFSertãoPE poderá receber notificações externas sobre incidentes de segurança apenas por correio eletrônico para o endereço **etir@ifsertao-pe.edu.br**.

Art. 6º É recomendado aos usuários notificar, com brevidade, os incidentes de Segurança da Informação e vulnerabilidades de que tenham conhecimento ou suspeita.

Art. 7º Os incidentes de Segurança da Informação em Redes de Computadores do IFSertãoPE, notificados ou detectados, deverão ser registrados, de forma específica em relatório (Anexo I).

Art. 8º A coleta de evidência destes incidentes deverá ser realizada pela ETIR ou por pessoal competente e por ela autorizado.

Art. 9º Quando o incidente for originário de suspeita de descumprimento da Política de Segurança da Informação ou de suas normas complementares, será observado o sigilo durante todo o processo de investigação, ficando as evidências, informações e demais registros restritos aos envolvidos.

Art. 10º. Quando houver indícios de ilícitos durante o gerenciamento destes incidentes, o Comitê Gestor de Segurança da Informação deverá ser comunicado, para avaliação das providências cabíveis.

Art. 11º. O encerramento do incidente de segurança em redes computacionais será realizado pela ETIR, com comunicação a todas as áreas interessadas.

DISPOSIÇÕES FINAIS

Art. 12º. Esta norma poderá ser revisada a qualquer tempo, quando identificada a necessidade de alteração, não excedendo o período máximo de 04 (quatro) anos.

Art. 13º. Caberá à ETIR esclarecer os casos omissos a esta Norma.

Art. 14º. Está normativa entra em vigor a partir da data de sua publicação.

Anexo I

RISI - RELATÓRIO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO
DOCUMENTO DE ACESSO RESTRITO

RISI n. XX/20XX

Descrição	*Identificar resumidamente o que ocorreu - p.ex. ataques DDoS*
Período em que ocorreu o incidente	**Data/hora início:**
	Data/hora fim:
Severidade do incidente	**( ) Alta ( ) Média ( ) Baixa**
Tipo de Impacto	**( ) Confidencialidade ( ) Integridade ( ) Disponibilidade**
Origem do alerta	*Informar quem ou qual sistema alertou sobre o incidente*
Comunicação do incidente	*Informar a quem ou as quais setores o incidente foi informado*

Detalhamento do Incidente

<informar a categoria do incidente. Ex.: Alteração não planejada, Ataque DDoS, Não Conformidade com a PSI, etc>
<descrever o que ocorreu, extensão e impactos do incidente, bem como detalhar as causas do incidente, áreas envolvidas na investigação do incidente, etc>

Tratamento do Incidente

<descrever ações executadas para contenção e/ou contorno do problema/incidente, equipes/pessoas envolvidas. Atentar ao fato de que determinadas ações de contenção/contorno podem demandar sua prévia comunicação e/ou autorização de instâncias superiores>

Análise e Encerramento do Incidente

<descrever se necessárias outras ações e recursos necessários para finalizar o tratamento do incidente e/ou para evitar que o incidente volte a ocorrer, informando, se possível, prazos e responsáveis para execução.>
<lições aprendidas>
<informar identificador do chamado/problema vinculado ao incidente, se houver>
Considerar também a necessidade de:
- reversão da solução de controle/contorno
- implementação de uma correção para a causa-raiz do problema;
- implantação de um novo serviço/sistema;
- substituição do ativo/sistema afetado;
- revisão de procedimentos/processos.

ASSINATURAS

Andson da Silva Rodrigues:07396115426

Assinado de forma digital por Andson da Silva Rodrigues:07396115426
Dados: 2022.04.14 09:41:14 -03'00'

APROVAÇÃO
Presidente do Comitê Gestor de Segurança da Informação