Processo: Coleta de Evidências de Incidentes de Segurança Cibernética

Finalidade: O processo define quem e como se dará o acionamento da Equipe de Prevenção, Resposta e Tratamento de Incidentes Cibernéticos (ETIR) para a coleta de evidências de incidentes de segurança cibernética.

Aplicabilidade: Aplica-se a demandas de Segurança Cibernéticas, originadas a partir de uma provocação administrativa ou judicial com a finalidade de instrução processual.

Responsável: PROAGI/CTIC/SGTI

Número: INDEFINIDO

Versão: INDEFINIDO

Aprovação: INDEFINIDO

Elaborado por: Wilson Varaschin e Carlos Alberto Meier Basso

Termos e Definições

COLETA DE EVIDÊNCIAS DE SEGURANÇA EM REDES COMPUTACIONAIS: processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e de ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou a coleção de dados que contenham evidências do incidente;

SEGURANÇA CIBERNÉTICA: ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Atores e responsabilidades

Gestor de Segurança da Informação: Responsável pela comunicação entre a UNILA e o requisitante, também é o responsável pela abertura e encerramento do processo, quando da possibilidade do atendimento da demanda.

Agente Responsável: Ponto focal da ETIR e responsável por avaliar a possibilidade técnica de atendimento.

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR): equipe responsável pela coleta de evidências de incidentes de segurança em redes computacionais e elaboração do relatório final de atendimento.

Etapas

1. Analisar a demanda

Descrição: Verifica se a demanda pode ser atendida e: *i)* se for uma demanda de incidente cibernético, encaminha para o Agente Responsável pela ETIR; *ii)* se não for incidente cibernético, encaminha para o setor responsável; *iii)* caso não seja possível ser atendida, encerra o processo avisando o demandante.

Papéis: Gestor de Segurança da Informação

Entradas:

- Ofício de solicitação de coleta de evidências.

Saídas:

- Encaminhamento do processo ao agente responsável quando for demanda de segurança cibernética - *etapa 2*
- Encaminhamento ao setor responsável quando não for demanda de segurança cibernética;
- Resposta ao ofício sobre o atendimento a não possibilidade de atendimento - *etapa 3*

Atividades:

- Analisar a demanda e decidir sobre o encaminhamento.

Ferramentas:

- Processador de textos, e-mail e SIPAC.

Referências:

- Normativa de GSI - Art. 16 inciso XII

---

2. Verificar a possibilidade técnica de atendimento

Descrição: O agente responsável irá verificar se os dados da solicitação são suficientes para o prosseguimento do atendimento, a existência dos registros solicitados e impedimentos legais.

Papéis: Agente Responsável

Entradas:

- Processo do SIPAC aberto pelo Gestor de Segurança da Informação com as informações solicitadas - *etapa 1*
- Adendo à solicitação - *etapa 4*

Saídas:

- Resposta da não possibilidade de atendimento com as razões do não atendimento - *etapa 3;*
- Solicitação de mais dados ao Gestor de Segurança da Informação - *etapa 4;*
- Submissão dos dados a serem coletados - *etapa 5.*

Atividades:

- Verificação dos dados e escopo da solicitação.

Ferramentas:

- <Listar atividades>.

Referências:

- LGPD;
- LAI;
- MARCO CIVIL DA INTERNET;
- NORMATIVAS INTERNAS.

---

3. Submeter para arquivamento

Descrição: O processo será submetido para o arquivamento

Papéis: Gestor de Segurança da Informação

Entradas:

- Notificação que a demanda não pode ser atendida - *etapa 1 ou etapa 2*
- Relatório técnico com o resultado da coleta - *etapa 6*

Saídas:

- Finalização do processo

Atividades:

- Oficiar o requisitante.

Ferramentas:

- SIPAC
- Processador de texto

Referências:

- <Listar referências>.

---

4. Solicitar novas informações

Descrição: Oficiar o requisitante a apresentar mais informações para o atendimento da demanda.

Papéis: Gestor de Segurança da Informação.

Entradas:

- Solicitação de dados - *etapa 2*

Saídas:

- Ofício ao requisitante

Atividades:

- Oficiar o requisitante.

Ferramentas:

- SIPAC
- Processador de textos

Referências:

- <Listar referências>.

---

5. Coletar evidências

Descrição: A ETIR irá realizar a coleta das informações pertinentes à solicitação apresentada.

Papéis: ETIR

Entradas:

- Solicitação de dados a serem coletados - *etapa 2*

Saídas:

- Informações encontradas - *etapa 6*

Atividades:

- Coletar evidências nos registros dos sistemas ou ativos;

Ferramentas:

- Não se aplica.

Referências:

- <Listar referências>.

---

6. Elaborar o relatório

Descrição: A ETIR elaborará o relatório com as informações levantadas e encaminhará ao Gestor de Segurança da Informação.

Papéis: ETIR

Entradas:

- Evidências encontradas nos registros de sistemas ou ativos - *etapa 5*;

Saídas:

- Encaminhamento do relatório ao Gestor de Segurança da Informação - *etapa 2;*

Atividades:

- Redação do relatório técnico

Ferramentas:

- Processador de texto
- SIPAC

Referências:

- <Listar referências>.
