



# Norma de Gestão de Incidentes

## SUMÁRIO

1. OBJETIVO .....	3
2. CAMPO DE APLICAÇÃO .....	3
3. DEFINIÇÕES .....	3
4. PAPÉIS E RESPONSABILIDADES .....	4
4.1. Usuários de TI.....	4
4.2. Equipe de Infraestrutura de TI .....	4
4.3. Encarregado de Segurança da Informação (ESI) .....	4
4.4. Ponto Focal.....	5
4.5. Encarregado de Proteção de Dados (DPO).....	5
4.6. Comitê de Segurança da Informação (CSI) .....	5
5. DESCRIÇÃO .....	5
5.1. Registro de Incidentes de TI .....	5
5.2. Incidentes Comuns .....	6
5.2.1. Identificação e Registro .....	6
5.2.2. Análise e Tratativa .....	6
5.2.3. Procedimento de Escalada .....	6
5.3. Incidentes de Segurança da Informação .....	7
5.3.1. Identificação e Registro .....	7
5.3.2. Análise e Tratativa .....	7
5.4. Incidentes de Segurança da Informação Envolvendo Dados Pessoais .....	8
5.5. Avaliação Pós Solução .....	9
6. EVIDÊNCIAS GERADAS.....	9
7. DOCUMENTOS DE REFERÊNCIA .....	9
8. REGISTRO DE ALTERAÇÕES .....	10
9. FORMALIZAÇÃO.....	10

## 1. OBJETIVO

Esta Norma define as regras e os procedimentos para gestão de incidentes atendidos pela Equipe de Infraestrutura de TI, com ênfase especial aos incidentes de segurança da informação.

## 2. CAMPO DE APLICAÇÃO

Aplicável a todos os colaboradores, próprios ou terceiros, que utilizam recursos de TI fornecidos pelo **Grupo Benner\*** para o exercício de suas atividades.

\* Denominação utilizada para designar as empresas: Benner Sistemas S.A., Benner Tecnologia e Sistemas em Saúde Ltda., Benner Tecnologia e Serviços em Saúde Ltda. e Infomed Benner Tecnologia e Serviços S.A.

## 3. DEFINIÇÕES

**CSI – Comitê de Segurança da Informação:** Equipe multidisciplinar, constituída por representantes de áreas-chave para o desenvolvimento e manutenção da cultura de segurança da informação na Empresa.

**DPO - *Data Protection Owner* (Encarregado de Proteção de Dados):** Profissional designado na Empresa para zelar pela proteção de dados pessoais, no âmbito da Lei Geral de Proteção de Dados (LGPD).

**ESI - Encarregado de Segurança da Informação:** Profissional designado pela Empresa para definir e manter políticas, procedimentos, registros e controles relacionados à segurança da informação.

**Incidente de Segurança da Informação:** Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação ou rede de computadores, que acarretam a perda de um ou mais princípios básicos de Segurança da Informação: Autenticidade, Confidencialidade, Disponibilidade, Integridade ou Irrefutabilidade.

**Incidente de Segurança com Dados Pessoais:** Refere-se a um incidente de segurança da informação com indícios de violação na segurança de dados pessoais, tais como: acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados considerada inadequada ou ilícita.

**NGI RISI - Relatório de Incidente de Segurança da Informação:** Documento a ser preenchido pelo Ponto Focal designado para tratativa de um incidente de segurança da informação.

**Ponto Focal:** Profissional designado pelo ESI para coordenar as ações e decisões relacionadas à tratativa de um incidente de segurança da informação.

**Siscon:** Sistema utilizado para registro e atendimento de chamados relativos à infraestrutura de TI do Grupo Benner. Acessível por meio do endereço: <https://siscon.benner.com.br/>.

Outros termos e definições utilizados no contexto da Segurança da Informação podem ser consultados no MSI - Manual de Segurança da Informação.

## **4. PAPÉIS E RESPONSABILIDADES**

### **4.1. Usuários de TI**

Providenciar a abertura de um chamado no sistema Siscon, caso identifique qualquer anormalidade no uso dos recursos de TI que lhe forem disponibilizados ou que estejam em desacordo com a Política de Segurança da Informação e a Política de Privacidade da Empresa.

### **4.2. Equipe de Infraestrutura de TI**

Analisar os chamados abertos pelos Usuários de TI; classificar e atender os incidentes relacionados à sua área de atuação; notificar o ESI nos casos de incidentes de segurança da informação; manter os usuários informados a respeito do andamento das solicitações; manter os registros e os controles de TI atualizados.

### **4.3. Encarregado de Segurança da Informação (ESI)**

Avaliar os incidentes de segurança da informação e nomear um Ponto Focal responsável por sua tratativa; suportar junto ao Ponto Focal as decisões a serem tomadas para resolução do incidente; notificar o DPO nos casos de incidentes de segurança da informação que envolvam dados pessoais; manter o CSI, o DPO e demais partes interessadas cientes a respeito das informações e decisões envolvendo incidentes de segurança da informação; identificar e obter autorizações e aprovações, quando necessárias para tratativa de incidentes de segurança da informação.

#### 4.4. Ponto Focal

Registrar e acompanhar as ações necessárias para tratativa do incidente de segurança da informação; elaborar o NGI RISI – Relatório de Incidente de Segurança da Informação e manter o ESI informado a respeito das tratativas e das decisões a serem tomadas para resolução do incidente.

#### 4.5. Encarregado de Proteção de Dados (DPO)

Avaliar os incidentes de segurança da informação que envolvam dados pessoais; suportar junto às Equipes envolvidas as decisões a serem tomadas para resolução do incidente; manter o CSI, o ESI e demais partes interessadas (internas e/ou externas) cientes a respeito das informações e decisões para a tratativa de incidentes de segurança da informação com potencial violação de dados pessoais.

#### 4.6. Comitê de Segurança da Informação (CSI)

Avaliar o impacto (real ou potencial) dos incidentes de segurança da informação reportados; suportar as decisões e aprovações necessárias junto ao ESI e/ou DPO; deliberar a respeito de sanções administrativas e disciplinares, quando aplicáveis.

Outras definições de papéis, atividades e responsabilidades no contexto de segurança da informação estão detalhadas na Seção 6 da PSI - Política de Segurança da Informação.

### 5. DESCRIÇÃO

#### 5.1. Registro de Incidentes de TI

Os incidentes referem-se a eventos adversos que causam indisponibilidade, instabilidade ou falha no funcionamento dos recursos de TI. Conforme mencionado no MSI – Manual da Segurança da Informação, item 5.11. Registro e Tratamento de Eventos de Tecnologia da Informação: *“Qualquer incidente identificado pelo usuário deverá ser imediatamente registrado no Siscon para encaminhamento à Área de TI.*

Os chamados classificados como Incidentes não necessitam de aprovação gerencial e, por apresentar uma exceção no funcionamento normal dos recursos de TI, possuem prioridade no atendimento.

Durante a análise do chamado, a Equipe de Infraestrutura de TI avalia a abrangência e magnitude do incidente. Dependendo da quantidade de usuários, sistemas e processos de negócio que podem ser impactados, o chamado pode ser classificado como um

incidente comum ou um incidente de segurança da informação. A seguir, são definidos os critérios e as tratativas para cada tipo de incidente.

## **5.2. Incidentes Comuns**

### **5.2.1. Identificação e Registro**

Os incidentes nos sistemas de informação utilizados pelos clientes da Benner possuem tratativa específica, definidas pela Unidade de Negócio responsável pelo sistema. Desta forma, não são contemplados no escopo desta Norma.

Já os incidentes relativos à infraestrutura de TI da Benner podem ser identificados e registrados por qualquer Usuário de TI, por meio da abertura de um chamado no sistema Siscon. Uma vez registrados, os chamados são encaminhados para a Equipe de Infraestrutura de TI.

### **5.2.2. Análise e Tratativa**

A Equipe de Infraestrutura de TI recebe os chamados registrados no sistema Siscon e verifica se é necessário fazer algum ajuste com relação ao tipo de chamado aberto e ao prazo estimado para resolução.

Todas as comunicações realizadas para a tratativa do incidente devem ser registradas no sistema Siscon, incluindo os contatos para realização de testes e/ou validações após a atuação do Analista responsável pelo atendimento. Quando novas informações são inseridas no sistema, notificações são enviadas automaticamente por e-mail aos envolvidos.

Após o registro da resolução e caso não haja manifestação contrária do usuário, o chamado é encerrado.

**Observação:** Em caso de incidentes envolvendo computadores cuja restauração não seja possível, a Equipe de Infraestrutura de TI deve providenciar a completa eliminação de todas as informações, utilizando ferramentas e procedimentos de deleção permanente dos dados, e atualizar as bases de dados correspondentes, de acordo com a Norma de Gestão de Ativos.

### **5.2.3. Procedimento de Escalada**

Durante o atendimento, o Analista responsável poderá acionar o suporte de provedores externos, de acordo com os níveis de serviços acordados nos contratos vigentes.

Caso seja constatado que se trata de um incidente com potencial de impacto a vários usuários, ou que possam afetar diversos sistemas e processos de negócio, o Encarregado de Segurança da Informação deve ser acionado para avaliar se o chamado deve ser classificado como um incidente de segurança da informação.

### **5.3. Incidentes de Segurança da Informação**

#### **5.3.1. Identificação e Registro**

Os incidentes de segurança da informação podem ser identificados a partir da análise de um chamado aberto por um Usuário de TI. Também podem ser registrados pela própria Equipe de Infraestrutura de TI, durante as atividades de administração e monitoramento do ambiente de TI, ou por meio da análise de notificações enviadas pelos Provedores Externos de Serviços.

Uma vez constatado que se trata de um incidente de segurança da informação, o chamado deve ser devidamente classificado como tal, e uma notificação deve ser enviada para o Encarregado de Segurança da Informação (ESI).

A partir da confirmação pelo Encarregado de Segurança da Informação (ESI), o chamado deve ser reclassificado como um incidente de segurança da informação no sistema Sicon, para que seja prontamente identificado, priorizado e receba as tratativas adequadas.

#### **5.3.2. Análise e Tratativa**

Ao confirmar que se trata de um incidente de segurança da informação, a primeira ação do ESI é a designação do Ponto Focal responsável pela tratativa o incidente. Tendo em vista as necessidades de comunicação e as decisões requeridas, é importante que o Ponto Focal seja um especialista ou tenha comprovada experiência na administração dos ativos de TI envolvidos no incidente.

Assim que for nomeado, o Ponto Focal deve iniciar o preenchimento do formulário NGI RISI - Relatório do Incidente de Segurança da Informação. Para melhor identificação e análise dos impactos (potenciais ou confirmados) do incidente, as seções de [Identificação do Incidente], [Avaliação de Impacto] e [Proteção de Dados Pessoais]

devem ser preenchidas, com informações suficientes para que o ESI possa avaliar os próximos passos para a tratativa do incidente.

De posse das informações iniciais preenchidas no NGI RISI, cabe ao ESI avaliar e definir outras entidades e pessoas que devem estar cientes e envolvidas no acompanhamento e na resolução do incidente de segurança da informação, assegurando que recebam as informações necessárias e de maneira tempestiva.

**Atenção!** Caso haja a possibilidade de violação de segurança em dados pessoais, o DPO deve ser imediatamente notificado, para que possa realizar os procedimentos específicos, conforme descrito no item 5.4 deste documento.

O ESI deve providenciar as aprovações e/ou autorizações necessárias para a tratativa do incidente, inclusive acionando o Comitê de Segurança da Informação (CSI) para validação das decisões tomadas, sempre que julgar necessário.

Quando se tratar de incidentes com expressivo potencial de impactos operacionais e financeiros, ou que possam afetar negativamente a reputação da Empresa, cabe ao Comitê de Segurança da Informação avaliar a necessidade de decretar uma situação de crise. Tal situação pode ser requerida para melhor gerenciar as ações e as comunicações decorrentes de incidentes desta natureza.

**Importante:** Dependendo da natureza do incidente, o Ponto Focal e o ESI devem avaliar a necessidade de preservação das evidências, quando medidas legais ou disciplinares forem aplicáveis. Sendo assim, devem aplicar procedimentos específicos para garantir que a identificação, coleta, aquisição e manuseio das informações ocorreram de maneira apropriada.

Durante todo o processo de diagnóstico e resolução do incidente, as decisões tomadas e as ações executadas devem ser compartilhadas e alinhadas entre o Ponto Focal e o ESI. Cabe ao Ponto Focal inserir as informações referentes às seções de [Diagnóstico do Incidente] e [Resolução do Incidente], além de manter a seção [Registro de Eventos] sempre atualizada, com as principais atividades ocorridas desde a sua designação. Para isso, o Ponto Focal deve assegurar que as equipes envolvidas registrem todos os procedimentos realizados para tratativa do incidente de segurança da informação.

#### **5.4. Incidentes de Segurança da Informação Envolvendo Dados Pessoais**



Além das tratativas descritas no item 5.3, para os incidentes de segurança da informação que possam gerar violações na segurança de dados pessoais (confirmada ou potencialmente), o DPO deve ser imediatamente notificado pelo ESI.

Cabe ao DPO assegurar que todo incidente envolvendo dados pessoais seja devidamente avaliado e tratado em conformidade com a Lei Geral de Proteção de Dados (LGPD), de acordo com a Norma Gestao incidentes e vazamento de dados pessoais.

### **5.5. Avaliação Pós Solução**

Uma vez retomada a normalidade das operações, o Ponto Focal e o ESI devem complementar o preenchimento do NGI RISI, atualizando a seção [Lições Aprendidas] com informações a respeito das ações realizadas para mitigar os riscos e/ou prevenir a recorrência de incidentes similares.

Quando ficar constatado que o incidente de segurança da informação ocorreu em virtude da conduta inadequada de colaboradores, cabe ao Comitê de Segurança da Informação deliberar a respeito das medidas administrativas e/ou disciplinares a serem aplicadas.

Um sumário dos incidentes de segurança da informação e dos incidentes de violação de privacidade ocorridos no período deve ser apresentado nas reuniões periódicas do CSI.

## **6. EVIDÊNCIAS GERADAS**

Sistema Siscon: registro dos chamados abertos pelos Usuários de TI, posteriormente classificados como Incidentes.

NGI RISI – Relatório de Incidente de Segurança da Informação preenchido e anexado no sistema Siscon para todo chamado classificado como incidente de segurança da informação. Indicador: Incidentes de SI e de violação de privacidade no período mensal).

## **7. DOCUMENTOS DE REFERÊNCIA**

PSI - Política de Segurança da Informação

MSI - Manual de Segurança da Informação

NGA - Norma de Gestão de Ativos de TI


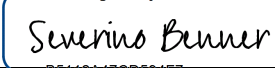
Plano de Resposta a Incidentes Envolvendo Dados Pessoais

Plano de Resposta a Incidentes Envolvendo Ransomware

## 8. REGISTRO DE ALTERAÇÕES

Versão	Data	Etapa	Responsável
00	11/07/2022	Emissão do documento	Infraestrutura de TI e CEO
01	15/10/2023	Revisão	Infraestrutura de TI

## 9. FORMALIZAÇÃO

Elaboração		Aprovação	
Jorge Espinhara – Governança de TI		Severino Benner - CEO	
16/10/2023	<small>DocuSigned by:</small>  <small>48FC1E7A18DC49D...</small>	16/10/2023	<small>DocuSigned by:</small>  <small>B5112A47CD594F7...</small>