

Ficha técnica deste documento

Documento	P00-PGI
Versão	1.0
Data da Versão	11/10/2021
Criado Por:	Márcio Bordignon (Multip)
Revisado Por:	Marília Ramos Costa e Silva (IEPTB-GO)
Aprovado Por:	Frederico Junqueira (IEPTB-GO)
Vigência:	A partir de 02/09/2022
Nível de Confidencialidade	Público, uso interno
Número de Páginas	Este documento contém 3 páginas

Histórico de Alterações e Aprovações

Data	Versão	Editado por	Descrição da Alteração / Aprovação
11/10/21	Draft 1.0	Márcio Bordignon	Esboço do documento
06/04/2022	Draft 1.0	Marília Ramos Costa e Silva	Preenchimento de dados conforme procedimentos internos IEPTB GO.
01/09/22	Draft 1.0	Marília Ramos Costa e Silva	Revisão.
02/09/22	Draft 1.0	Frederico Junqueira	Aprovação

Controle de impressão

A versão digital deste documento é a versão mais recente. É responsabilidade de cada indivíduo garantir que qualquer versão impressa seja a versão mais recente. A versão impressa deste documento não é controlada e não pode ser invocada, exceto quando formalmente emitido e assinado pelo Controlador de Documentos e fornecido com indicação de controle de cópia, conforme indicado nos campos abaixo:

Versão:	1.0
Data da Emissão:	11/10/2021
Cópia Controlada	

1 Escopo, Responsabilidades e Referências

Este documento estabelece as disposições do IEPTB-GO para o gerenciamento de incidentes de segurança da informação, incluindo a comunicação sobre eventos de segurança

A Gerência Administrativa é responsável por todos os aspectos da implementação e gestão dessas disposições, salvo indicação em contrário.

Os gerentes e supervisores são responsáveis pela implementação dessas disposições dentro do escopo de suas responsabilidades e devem garantir que todos os funcionários sob seu controle compreendam e assumam suas responsabilidades de acordo.

Para glossário de termos e demais referências, consultar a PSI (Política de Segurança da Informação) do IEPTB-GO.

2 Gestão de Incidentes

O IEPTB-GO estabeleceu abordagem descrita a seguir para o gerenciamento ordenado de incidentes de segurança da informação, incluindo a comunicação sobre eventos

2.1 Comunicar, avaliar, decidir e responder a eventos de segurança da informação

Todos os colaboradores e fornecedores são obrigados a relatar prontamente e verbalmente quaisquer eventos de segurança da informação ao seu gerente e à Gerência de TI.

Exemplos de eventos de segurança da informação incluem:

- Perda/roubo/furto de serviço, equipamento ou instalações
- sobrecargas
- erros humanos
- não conformidade com políticas ou diretrizes
- violações das disposições de segurança física e/ou lógica
- eventos anômalos do sistema
- violações de acesso

Quando um evento de segurança da informação é relatado, a Gerência Administrativa avalia o evento para determinar se deve ser classificado como um incidente e, quando necessário, tomar as medidas corretivas imediatas para mitigar a ameaça.

A Gerência Administrativa trabalha para planejar e tomar as ações corretivas necessárias para evitar a recorrência das mesmas e ameaças semelhantes.

Ações para recuperação de violações de segurança e falhas de sistema são cuidadosa e formalmente controladas da seguinte forma:

- apenas colaboradores claramente identificados e autorizados têm permissão para acessar sistemas e dados ativos
- todas as ações de emergência tomadas são documentadas em detalhes
- ação de emergência é relatada à gerência e revisada de maneira ordenada
- a integridade dos sistemas e controles de negócios é confirmada com o mínimo de atraso

2.2. Reportando ocorrências de segurança da informação

Todos os colaboradores que usam os sistemas e serviços de informação do IEPTB-GO devem relatar ao seu gerente e à Gerência Administrativa qualquer suspeita na segurança da informação ou qualquer potencial para melhoria da segurança da informação.

Todo o pessoal foi instruído a não tentar solucionar problemas de segurança.

Quando uma suspeita ou sugestão de melhoria é relatada, a Gerência Administrativa toma as ações corretivas e/ou preventivas necessárias.

A Gerência Administrativa monitora e analisa os tipos, volumes e custos de incidentes de segurança da informação para ajudar a reduzir a probabilidade ou impacto de incidentes futuros.

A Gerência Administrativa comunica à Diretoria as ocorrências de incidentes de segurança da informação, para deliberação conjunta de providências.

2.3. Coleta de Evidências e providências de contenção e/ou remediação

O IEPTB-GO possui contrato com empresa especializada, para auxiliar na identificação, coleta, aquisição e preservação de informações, que podem servir de prova.

Quando um incidente que pode exigir a preservação de evidências é relatado à Gerência Administrativa, esta assume o controle como o primeiro a responder e:

- descreve resumidamente o incidente aos nossos consultores especializados
- solicita aos consultores especializados conselho inicial
- solicita aos consultores especializados apoio imediato para mitigação do problema de segurança sendo ou a ser tratado
- aplica os seguintes princípios de boas práticas para ajudar a garantir que provas hábeis sejam protegidas de modo a permanecerem admissíveis no tribunal:
 - não altere nenhum dado
 - não acesse os dados originais
 - manter uma trilha de auditoria detalhada do que foi feito