Sumário

1. Objetivo

Estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação, incluindo Segurança Cibernética, que possam impactar ativos/serviços de informação ou recursos computacionais da Itaesbra.

2. Sumário executivo

A Política de Gestão de Incidentes de Segurança da Informação, complementa a Política Geral de Segurança da Informação, definindo as diretrizes para responder a eventos ou incidentes de segurança que estejam impactando ou possam vir a impactar ativos/serviços de informação ou recursos computacionais da Itaesbra.

3. Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação e se aplica a todos os processos, tecnologias, funcionários e terceiros da Itaesbra.

4. Acrônimos

Termos	Definições
ANPD	Autoridade Nacional de Proteção de Dados Pessoais é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil.
Segurança Cibernética	O processo de proteção de informações, prevenindo, detectando e respondendo a ataques.
Incidente de Segurança	Qualquer evento adverso, confirmado, que gerou algum impacto e leve à perda de confidencialidade, integridade ou disponibilidade das informações.

5. Diretrizes Gerais

As diretrizes para o tratamento de incidentes de segurança da informação, incluindo os incidentes de segurança cibernética, são:

- As responsabilidades e os procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação. Devem ser estabelecidos procedimentos para preparação e planejamento da resposta a incidentes;
- Procedimentos para monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação devem ser implementados;
- Incidentes de segurança da informação devem ser notificados através dos canais disponíveis da empresa (SAVI, telefone, e Microsoft Teams) para que sejam rapidamente remediados;
- Quando necessário deverá ser feito um comunicado, via email, aprovado pela Diretoria, em caso de uma violação de dados, à autoridade competente e aos titulares dos dados;
- Todo evento suspeito deverá ser analisado rapidamente, a fim de validar a ocorrência de um incidente de segurança da informação;
- Em caso de detecção de incidentes que envolvam a marca da empresa ou apropriação de informações sensíveis ao negócio da Itaesbra, a alta direção deverá ser notificada imediatamente;
- Todo funcionário, estagiário, terceiro, fornecedor, parceiro ou cliente será responsável por relatar o mais rápido possível à área de TI qualquer tipo de evento e fragilidades que possam causar danos de segurança aos ativos da empresa. Quando a origem do relato for interna, poderá ser feito através de email ou da abertura de um chamado de suporte (SAVI), se a origem do relato for externa, deverá ser feito através de email para o endereço dpo@itaesbra.com.br, conforme descrito na Política de Privacidade.

- Somente pessoal treinado e autorizado poderá acionar medidas corretivas nos sistemas;
- Após as medidas corretivas serem aplicadas, será avaliado a ações que serão necessárias para informar as equipes envolvidas do ocorrido.

6. Papéis e Responsabilidades

Gerência de Tecnologia da Informação:

- Atuar como responsável por ocorrências e eventos de segurança e garantir a existência de recursos, identificar, escalar, mitigar, conter, e erradicar incidentes de segurança.
- Aconselhar a diretoria da Itaesbra sobre quais informações sobre eventos e incidentes de segurança da informação podem ser divulgadas para públicos internos e externos.

Time de Tecnologia da Informação:

- Apoiar as equipes no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento operacionais dentro da área de especialidade de cada um dos participantes do time de TI;
- Aplicar as ações técnicas efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente;

Diretoria:

- Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público.

7. Orientações

7.1. Incidentes de Segurança da Informação

- Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da Itaesbra serão caracterizadas como um incidente de segurança da informação;
- Incidentes de segurança devem ser priorizados com base na criticidade dos processos relacionados ao atendimento dos clientes da Itaesbra, por exemplo, processos como Faturamento/ Expedição, Produção;
- Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados a área de tecnologia da informação através de email ou Teams e abertura de um chamado de Suporte (SAVI);
- A área de tecnologia da informação deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas;
- Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser avaliados e se for o caso isolados do ambiente corporativo, como por exemplo, retirando o ativo da rede corporativa, de forma a garantir a contenção do incidente;
- A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e/ou mitigação do risco desse incidente;

- Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente. Os incidentes de segurança da informação devem ser avaliados para a verificação de necessidades de melhorias ou a adoção de controles adicionais para reduzir a frequência, dano e custo de ocorrências futuras. A necessidade de revisão da Política de Segurança da Informação também deve ser considerada.

7.2. Disseminação de informação sobre incidentes de segurança da informação

- Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas da Itaesbra sem aprovação expressa e formal da diretoria.
- O vazamento de **dados pessoais** deve ser comunicado à Autoridade Nacional de Proteção de Dados, nos termos dos seus regulamentos. O comunicado à ANPD será precedido de avaliação das áreas de negócio envolvidas, da equipe de TI, pelo DPO e aprovação/autorização da Diretoria.
- O vazamento de **dados pessoais sensíveis** devem ser comunicado à Autoridade Nacional de Proteção de Dados e também aos Titulares de Dados Pessoais vazados, nos termos dos seus regulamentos. O comunicado à ANPD será precedido de avaliação da equipe de TI, pelo DPO e aprovação/autorização da Diretoria.
- Na impossibilidade de comunicação individual ao Titular de Dados Pessoais, a Itaesbra providenciará publicação em mídias de massa, com o propósito de garantir minimamente condições de que os afetados sejam notificados do vazamento.

8. Referências de materiais utilizados

- Política de Segurança da Informação;

- ABNT NBR ISO/IEC 27001/27002
- Boas práticas do Mercado.

Esta norma deve ser revisada anualmente ou quando for necessária a alteração.

Controle de Revisão do Documento				
Nº	**Data**	**Elaborado por**	**Histórico da Revisão**	**Revisado por**
00	03/06/24	Julio Nicolosi	Publicação inicial	Eduardo Scaramucci