CONTABILIS

POLITICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Cabo Frio
2024

1. Introdução

1.1. Objetivo

A Política de Segurança da Informação (PSI) da Contabilis tem como objetivo:

- Estabelecer as diretrizes e requisitos essenciais para garantir a proteção eficaz dos dados financeiros e fiscais de seus clientes;
- Assegura a conformidade com a LGPD no tratamento de informações pessoais e outras leis vigentes;
- Garantir a continuidade dos negócios através de planos de recuperação de desastres e mitigação de riscos envolvendo fornecedores e parceiros;
- Promover uma cultura de segurança entre os colaboradores, tornando-os mais preparados para agir com responsabilidade e segurança na sociedade digital; e
- Proteger os processos de BPO Financeiro, assegurando que todos os requisitos de segurança sejam atendidos, com auditorias e monitoramento contínuos para garantir a implementação eficaz das medidas estabelecidas.

1.2. Escopo

A Política de Segurança da Informação (PSI) da Contabilis é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os funcionários, contratados, fornecedores e parceiros que, direta ou indiretamente, lidam com as informações e ativos da organização. Isso inclui qualquer pessoa ou entidade que tenha acesso a dados sensíveis, sistemas, infraestrutura de TI, redes e serviços da Contabilis, seja no ambiente físico ou digital. A PSI abrange o uso, armazenamento, transmissão e descarte seguro de informações, estabelecendo requisitos para garantir a confidencialidade, integridade e disponibilidade dos dados.

2. Princípios de Segurança

2.1. Confidencialidade

A confidencialidade é um dos pilares da Política de Segurança da Informação (PSI) da Contabilis. Ela deve ser interpretada como à garantia de que as informações sensíveis e dados confidenciais da empresa e de seus clientes sejam acessados exclusivamente por pessoas autorizadas.

2.2. Integridade

A integridade é um dos pilares da Política de Segurança da Informação (PSI) da Contabilis. Ela deve ser interpretada como à garantia de que as informações e dados mantidos pela empresa sejam precisos, completos e não tenham sido alterados ou corrompidos de forma não autorizada, portanto ela deve assegurar que qualquer modificação nas informações, deve ser realizada de maneira controlada e registrada, assegurando que os dados reflitam a realidade e possam ser confiáveis para a tomada de decisões.

2.3. Disponibilidade

A disponibilidade é um dos pilares da Política de Segurança da Informação (PSI) da Contabilis. Ela deve ser interpretada como à garantia de que as informações e os sistemas estejam acessíveis e utilizáveis sempre que necessário, tanto para os colaboradores quanto para os clientes. Portanto ela deve assegurar, que as infraestruturas de TI, redes e dados; estejam operacionais e prontos para uso, minimizando interrupções, que possam afetar a continuidade dos serviços.

3. Gerenciamento de Acesso

3.1 Deverá ser criada identidade virtual para uso dos equipamentos internos, apenas para pessoas autorizadas.

3.2 Será usado apenas Whatsapp Empresarial para comunicação com clientes, mantendo conexão apenas nas estações de trabalho.

3.3 Para compartilhamento de documentos será usado apenas o drive oficial da empresa, mantendo conexão apenas com conta autorizada.

3.4 Para acesso ao drive oficial da empresa será permitido acesso apenas de contas com e-mail institucional da empresa.

4. Segurança Física e Ambiental

4.1. Controle de acesso físico

4.2.1 Deverá ser demarcada a área restrita a colaboradores.

4.2.2 Deverão ser demarcadas separadamente as áreas mais vulneráveis a vazamentos (sala da biblioteca e sala do servidor)

4.2.3 Acesso a área interna da empresa será permitido apenas para colaboradores autorizados

4.2.4 As áreas da sala da biblioteca e sala do servidor devem ter acesso controlado sempre por identificação biométrica ou facial.

4.2. Segurança ambiental

4.2.1 Aparelhos celulares ou fotográficos não serão permitidos na sala da biblioteca.

4.2.2 Deverá ser mantida em dia a inspeção de segurança do corpo de bombeiros.

4.2.3 Deve ser mantido o devido cuidado e manutenção com a rede elétrica do local

5. Segurança de Redes e Comunicações

5.1. Proteção de redes

5.1.1 A Contabilis implementa controles de segurança robustos para proteger suas redes contra ameaças internas e externas, garantindo a integridade, confidencialidade e disponibilidade dos sistemas e dados.

5.1.2 Os firewalls de rede estão configurados para inspecionar conexões com base em regras de segurança predefinidas, bloqueando tráfego suspeito ou não autorizado.

5.1.3 Os dados em trânsito são protegidos por protocolos de criptografia, como TLS/SSL, para evitar interceptações e garantir que apenas destinatários autorizados tenham acesso às informações.

5.1.4 As redes sem fio estão protegidas com padrões de segurança como WPA3, e utilizam mecanismos avançados de autenticação, incluindo certificados digitais e autenticação multifator (MFA), assegurando que somente dispositivos e usuários autorizados possam acessar as redes corporativas.

5.2. Monitoramento e detecção de intrusões

5.2.1 A Contabilis mantém sistemas de monitoramento e detecção de intrusões (IDS/IPS) para identificar, em tempo real, atividades suspeitas na rede. Esses sistemas detectam padrões de ataques conhecidos e comportamentos atípicos, gerando alertas automáticos para a equipe de segurança.

5.2.3 Ferramentas de análise contínua de tráfego de rede e registros de eventos (logs) estão implementadas, permitindo uma resposta rápida e eficaz a incidentes de segurança.

5.2.4 O sistema de prevenção de intrusões está configurado para bloquear automaticamente tentativas de intrusão e isolar ameaças, minimizando o impacto na operação.

6. Gestão de Incidentes de Segurança

6.1. Resposta a incidentes

6.1.1 A Contabilis possui um plano formal de resposta a incidentes de segurança, com o objetivo de minimizar o impacto de qualquer violação ou ameaça detectada.

6.1.2 O plano inclui procedimentos claros para a identificação, contenção, erradicação e recuperação de incidentes, além de análises pós-incidente para identificar causas raiz e implementar ações corretivas.

6.1.3 O plano é revisado e atualizado periodicamente, garantindo sua conformidade com as necessidades da empresa.

6.1.4 Em casos de incidentes de segurança e eventos que comprometam a integridade física ou lógica das informações da empresa, a Contabilis tem o dever de fornecer informações aos órgãos competentes para apuração, e, quando necessário, disponibilizar provas que estiverem sob sua responsabilidade ou das quais tenha conhecimento.

6.1.5 Em casos de incidentes cuja causa tenha sido violação de alguma política se segurança, o responsável pela violação deverá ser responsabilizado de acordo com a gravidade da violação podendo incluir advertência, demissão ou responsabilização legal.

6.2. Relatórios de incidentes

6.2.1 Todos os colaboradores da Contabilis são treinados para identificar e relatar incidentes de segurança ou atividades suspeitas.

6.2.2 Canais de comunicação dedicados, como sistemas de relatórios de incidentes, estão disponíveis para garantir o contato imediato com a equipe de segurança da informação.

6.2.3 Os relatórios de incidentes são documentados detalhadamente, incluindo o contexto, áreas afetadas, causas e ações tomadas, permitindo respostas rápidas e efetivas.

6.2.4 Revisões periódicas desses processos asseguram a eficiência na gestão de incidentes e a mitigação de riscos.

7. Conscientização e Treinamento em Segurança

7.1. Programa de conscientização

7.1.1 O programa de conscientização em segurança da informação tem como objetivo aumentar a compreensão dos colaboradores sobre suas responsabilidades em relação à segurança da informação e a importância de proteger os dados sensíveis da empresa.

7.1.2 O conteúdo do programa abrange tópicos como identificação de ameaças (vazamentos de informação, ataques hackers), boas práticas de segurança (uso seguro de dispositivos pessoais, cuidados com senhas) e as políticas internas.

7.1.3 São utilizados formatos variados, como workshops, e-learning e materiais impressos, para atender a diferentes estilos de aprendizado.

7.1.4 Avaliações são realizadas por meio de testes e feedbacks, medindo a eficácia do programa e identificando áreas que necessitam de mais ênfase.

7.2. Treinamento em segurança

7.2.1 Treinamentos de segurança são realizados semestralmente, com atualizações sempre que houver mudanças nas políticas ou surgirem novas ameaças.

7.2.2 O conteúdo dos treinamentos inclui módulos sobre a proteção de dados, resposta a incidentes e a importância de reportar comportamentos suspeitos.

7.2.3 Certificados são emitidos para os colaboradores que completarem o treinamento, incentivando o engajamento.

8. Avaliação e Melhoria Contínua

8.1. Auditorias de segurança

8.1.1 Auditorias de segurança periódicas são realizadas para avaliar a adesão às políticas de segurança e a eficácia das práticas implementadas.

8.1.2 Vulnerabilidades são identificadas, com foco em encontrar brechas de segurança e áreas que necessitam de melhorias.

8.2. Revisão de políticas e procedimentos

8.2.1 Um cronograma de revisão regular é estabelecido para revisar e atualizar as políticas de segurança, refletindo mudanças tecnológicas, novas ameaças e lições aprendidas com incidentes anteriores.

8.2.2 As atualizações são comunicadas a todos os colaboradores, e o treinamento necessário é fornecido.

8.3. Análise de riscos

8.3.1 Riscos associados aos ativos da organização, como servidores e estações de trabalho, e o uso de dispositivos pessoais, são avaliados regularmente.

8.3.2 Medidas de mitigação são desenvolvidas e implementadas, como a instalação de firewalls e a restrição de acesso a informações sensíveis.

8.4. Medição de desempenho

8.4.1 Métricas e KPIs são estabelecidos para medir a eficácia dos programas de segurança.

8.4.2 A taxa de incidentes de segurança, a participação nos treinamentos e os resultados de auditorias são monitorados para avaliar a conformidade e a eficácia das políticas de segurança.

9. Conformidade Legal e Regulatória

9.1. Conformidade com leis e regulamentações

9.1.1 Garantir conformidade com LGPD e marco civil da internet, assim como atualizar políticas de segurança quando necessário devido a mudanças na legislação

9.2. Gerenciamento de vulnerabilidades e patches

9.2.1 O GTI deve estabelecer um processo contínuo para identificar, avaliar e corrigir vulnerabilidades de segurança em sistemas e aplicativos, garantindo a proteção contra ameaças cibernéticas.

9.2.2 O GTI deve garantir que todos os sistemas e aplicativos estejam atualizados com os patches de segurança mais recentes para mitigar riscos conhecidos.

10. Responsabilidades

10.1. Direção

10.1.1 A direção é responsável por responder por eventuais falhas da empresa

10.1.2 A direção é responsável por apontas nomear a equipe de segurança da informação e os funcionários

10.2. Equipe de segurança da informação

A equipe de segurança da informação é deverá garantir a correta aplicação e atualização das políticas de segurança

10.3. Funcionários

Os colaboradores devem respeitar as políticas de segurança estabelecidas pela equipe de segurança da informação.