PSI

Política da Segurança da Informação

Ad'oro

CARTA DO DIRETOR

Prezado Colaborador,

Em função da natureza e da criticidade do nosso negócio, do crescente uso de ferramentas de tecnologia e com a facilidade com a qual as informações se difundem, o gerenciamento de riscos corporativos relacionados à Segurança da Informação torna-se cada vez mais importante.

Toda operação da empresa é realizada com base em informações, na maioria das vezes, críticas e sigilosas para o negócio, tais como materiais do processo produtivo, layout industrial, dados financeiros, balanços, contratos, folha de pagamento, planejamento estratégico, entre outras.

Proteger adequadamente as informações é fundamental para nosso negócio e fortalece a base da nossa Governança Corporativa.

Diante desse cenário, a Política de Segurança da Informação deve ser um instrumento forte, com papéis e responsabilidades bem definidos, conhecida e praticada por todos, tornando-se parte da cultura e da gestão da ADORO.

É vital que todos os colaboradores e parceiros compreendam a importância da Segurança da Informação para nosso negócio.

Todos os esforços devem ser mobilizados para que a Política de Segurança da Informação seja cumprida, mantida e melhorada continuamente, de forma responsável e sustentada no contexto do nosso negócio.

A Segurança das Informação é responsabilidade de todos!

Caio Lutfalla
Diretor Administrativo e Financeiro

SUMÁRIO

1. O que é segurança da informação?

Hoje em dia a informação é o bem mais valioso de uma empresa ou cliente, e o objetivo da Segurança da Informação é proteger esses dados adotando medidas preventivas e utilizando ferramentas para fazer com que os dados trafeguem e sejam armazenados de forma segura, além da conscientização dos colaboradores e terceiros sobre uso seguro da informação.

2. Por que alguém desejaria invadir seu computador

- Utilizar seu computador em alguma atividade ilícita, para esconder sua real identidade e localização;
- Para lançar ataques contra outros computadores ou propagar vírus;
- Utilizar seu disco rígido como repositório de dados;
- Meramente destruir informações (vandalismo);
- Disseminar mensagens alarmantes e falsas;
- Ler e enviar e-mails em seu nome;
- Furtar números de cartões, senhas bancárias, demais senhas e dados sigilosos.

3. O que é um incidente de segurança da informação

É qualquer evento adverso, confirmado ou sob suspeita relacionado a segurança dos sistemas de computação ou a rede de computadores.

4. Papéis e responsabilidades

Colaboradores, estagiários, aprendizes e prestadores de serviços

- Cumprir as orientações dispostas na PSI (Politica de Segurança da Informação);
- Participar do programas de conscientização e treinamentos;
- Buscar orientação junto ao gestor em caso de dúvidas associadas à PSI;
- Comunicar os responsáveis pela Segurança da Informação sempre que ocorrer possíveis violações.
- Utilizar de forma ética, legal e responsável os recursos computacionais e as informações da ADORO;
- Assinar o Termo de Confidencialidade.

Gestores

- Apoiar a conscientização da importância da Segurança da Informação e da PSI;
- Fiscalizar que seus colaboradores estejam em conformidade com a PSI;
- Aplicar sanções administrativas, no caso descumprimento da PSI;
- Autorizar o acesso ou compartilhamento das informações sob sua responsabilidade.

Diretoria

• Aprovar a Política de Segurança da Informação;

• Aprovar a constituição e composição do Comitê de Segurança da Informação;

• Apoiar na divulgação da PSI;

• Definir em conjunto com o departamento de RH e/ou Gestores, quando necessário, sanções em caso de violação da PSI;

• Autorizar o acesso ou compartilhamento das informações

Comitê de Segurança da Informação

• Analisar, avaliar e propor ações que mitiguem os riscos de segurança da informação na organização;

• Propor ações de conscientização e capacitação de pessoal, visando difundir os conhecimentos e dar efetividade à PSI;

• Monitorar a eficácia das ações de Segurança da Informação no âmbito Corporativo;

• Solicitar apuração de possível violação da PSI.

Departamento de Recursos Humanos

• Coletar a assinatura dos colaboradores e prestadores de serviços formalizando o aceite do Termo de Confidencialidade;

• Orientar os gestores ao aplicar sanções administrativas no caso de violação da PSI;

Departamento Jurídico

• Analisar e avaliar juridicamente a PSI e suas revisões;

• Elaborar e validar o Termo de Confidencialidade;

• Orientar juridicamente, quando necessário, nas tratativas dos incidentes de Segurança da Informação.

Departamento de Tecnologia da Informação

• Apoiar e orientar a ADORO em relação à Segurança da Informação;

• Trabalhar na divulgação e conscientização da importância da PSI;

• Atuar na melhoria contínua da Segurança da Informação e da PSI;

• Monitorar e auditar os recursos tecnológicos nos aspectos de Segurança da Informação;

Assegurar a devida implementação da PSI;

Analisar e reportar os incidentes de Segurança da Informação para o Comitê de Segurança da Informação.

5. Gestão de ativos

• Todos os recursos corporativos (desktops, notebooks, celulares, impressoras, etc.) devem ser utilizados somente para fins profissionais;

• Apenas softwares homologados e autorizados pela T.I. podem ser instalados;

• A ADORO resguarda-se o direito de monitorar, registrar e auditar, sem aviso prévio, os recursos estações de trabalho, servidores, correio eletrônico, conexões com a internet, etc, e o não cumprimento das normas do PSI será uma violação às regras internas e sujeitará às medidas administrativas e legais cabíveis;

• Todos os visitantes, terceiros e fornecedores somente podem ter acesso as instalações da empresa quando devidamente autorizados, identificados;

• Devem ser usados crachás distintos, com objetivo de permitir facilmente a identificação da pessoa;

• Todos os incidentes ou fragilidades de Segurança da Informação devem ser reportados à equipe de Segurança da Informação, que deverá realizar o registro, análise e o tratamento.

• Todos os colaboradores, estagiários, aprendizes e prestadores de serviços devem estar cientes do cumprimento das regras dispostas na Política de Segurança da Informação.

6. Normas gerais

6.1. Uso do e-mail

Os colaboradores são responsáveis pelas informações enviadas de seus e -mails, portanto deve ser utilizado somente para fins profissionais.

Não é permitido:

• Encaminhar e/ou armazenar mensagens de conteúdo impróprio;

• Cadastrar o e-mail corporativo com propósitos não relacionados as atividades corporativas;

• Utilizar o e-mail particular (ex. gmail, yahoo, uol, etc.), exceto em casos formalmente autorizados;

• Abrir ou encaminhar mensagens consideradas suspeitas ou caracterizadas como corrente, SPAM e Phishing (técnica de fraude online).

É importante que se tenha atenção redobrada com links recebidos em mensagens não solicitadas ou de origem duvidosa. Em caso de dúvida, solicitar o apoio do departamento de tecnologia da informação .

6.2. Uso da internet

Todo o conteúdo de acesso a internet é monitorado;

Não é permitido:

• Sites de conteúdo ilícito;

• Fazer download de materiais indevidos (filmes, músicas, etc);

• Acessar sites e ferramentas cujo o objetivo seja burlar as regras de controle de acesso da empresa;

• Utilizar serviço de armazenamento na nuvem não homologado.

6.3. Redes Sociais

Não é autorizado publicar nas redes sociais fotos, vídeos e áudios com informações da empresa, exceto aqueles que são autorizados devido às suas atribuições corporativas ou em casos autorizados expressamente.

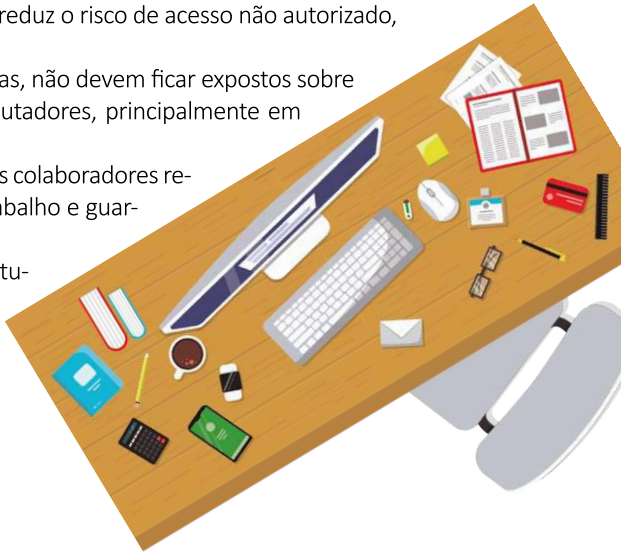
6.4. Política da mesa limpa

O uso da política de mesa e tela limpa, reduz o risco de acesso não autorizado, perda e dano da informação.

• Documentos com informações sigilosas, não devem ficar expostos sobre a mesa de trabalho ou nas telas de computadores, principalmente em locais de fácil acesso;

• No final de expediente, convém que os colaboradores recolham os documentos de sua mesa de trabalho e guarde-os em local seguro;

• Todos os colaboradores devem efetuar logoff ou bloquear a tela do Windows (atalho: Tecla Win + L) sempre que se ausentarem do seu local de trabalho.



6.5. Política de senha

As credenciais de acesso aos sistemas são de responsabilidade única e exclusiva dos usuários.

Para manter a segurança da senha, os cuidados abaixo devem ser observados:

• Nunca informar, compartilhar ou divulgar suas credenciais de acesso;

• Não utilizar senhas de fácil dedução;

• Não anotar a senha em nenhum local (físico ou digital);

• Trocar a senha periodicamente, inclusive as administrativas;

• Não armazenar nos navegadores (ex. Internet Explorer, Google Chrome, Firefox) as senhas de acesso a sites de internet;

• Não usar a mesma senha dos sistemas corporativos fora da empresa em questões particulares.

Não é permitido, independentemente do nível hierárquico ou área de negócio, solicitar aos usuários a credencial de acesso.

Caso algum usuário constate que outra pessoa está utilizando sua credencial de acesso ou de outrem, a equipe de Segurança da Informação deve ser comunicada e a senha alterada imediatamente.

Sanções serão aplicadas aos usuários que forem identificados pela TI, compartilhando ou utilizando a credencial de acesso de outra pessoa.

6.6. Impressoras

• O uso de impressoras deve estar relacionado somente aos interesses da empresa.
• Ao usar uma impressora, deve-se recolher, imediatamente, os documentos impressos;

6.7. Dispositivos móveis

Compreende-se como dispositivo móvel qualquer equipamento eletrônico com mobilidade, por exemplo, notebook, smartphone ou tablet.

Dispositivos Móveis Corporativos

• Deve ser usado apenas para fins corporativos;
• Os colaboradores são responsáveis pela guarda, proteção, bom uso do equipamento e das informações nele contidas;
• Convém implementar o uso de criptografia nos dispositivos móveis para realizar o armazenamento e o transporte de dados;

Uso de notebooks fora da empresa:

• Deslocamento de carro, priorize armazenar no porta malas;
• Em locais públicos mantenha próximo e sempre à vista;
• Em viagem, deve ser levado como bagagem de mão;
• Não deixar no carro quando não estiver no veículo.

Dispositivos Móveis Particulares

• Não é permitido, salvo exceções autorizadas:
• Gravar áudio, vídeo ou foto nas dependências da empresa;
• Armazenar informações corporativas;
• Enviar informações corporativas por meio de: WhatsApp, Telegram, SMS, entre outros;
• Acessar o e-mail corporativo através do equipamento pessoal.

6.8. Dispositivos removíveis

• Não é permitido o uso de pen drive, HD externo, cartão de memória independente ou do celular ou similares.
• Toda exceção, deve ser autorizada e homologada pelo departamento de T.I.

6.9 Backup (cópia de segurança)

• Os documentos devem ser salvos na rede, uma vez que não é possível fazer backup dos dados armazenados na máquina local;

• Os usuários não estão autorizados a utilizar recursos (pen drive, cloud etc.) para efetuar backup;

• O backup é uma atribuição exclusiva do departamento de T.I.

6.10 Descarte das informações

• As informações impressas e de conteúdo sensível, quando não mais necessárias, devem ser trituradas;

• O descarte de recursos tecnológicos (ex. mídias, equipamentos etc.) deve ser realizado pelo departamento de T.I.

7. Referências

• ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. 2ª ed. ABNT, 2013.

• ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – Técnicas de segurança – Sistema de gestão de segurança da informação. 2ª ed. ABNT, 2013.

www.adoro.com.br