DENOMINAÇÃO DO DOCUMENTO:			
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO			
ABRANGÊNCIA DE USO:	ÚLTIMA REVISÃO:	PRÓXIMA REVISÃO:	DATA INÍCIO VIGÊNCIA:
CORPORATIVO	ABRIL 2023	ABRIL 2024	SETEMBRO DE 2019
ÁREA RESPONSÁVEL:		CLASSIFICAÇÃO:	
TECNOLOGIA DA INFORMAÇÃO		INTERNO	
ELABORADO POR:	REVISADO POR:	APROVADO POR:	
PODIUM TECNOLOGIA	Dierikssen Caldeira e Samara Pelegrino	DIRETORIA	

Sumário

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.

A presente Política de Segurança tem por finalidade mitigar eventuais riscos e danos relacionados a ameaças externas ou internas, deliberadas ou acidentais, que possam impactar na confidencialidade, integridade e disponibilidade das informações de qualquer natureza, objetivando garantir sua preservação.

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 AD'ORO.

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

1 INTRODUÇÃO

A AD'ORO entende que a informação é um dos seus principais ativos e protegê-la é fundamental para garantir a Gestão de Riscos Corporativos. Atenta à criticidade do negócio, a empresa busca continuamente aderência às boas práticas de Segurança da Informação.

Esta Política de Segurança da Informação exige o cumprimento do Regulamento Interno da Ad'oro e de todas as leis e regulamentações aplicáveis em vigor relacionadas a proteção de dado incluindo, sem limitação, a Lei Geral de Proteção de Dados Pessoas (LGPD).

Assim, a AD'ORO estabelece a presente Política de Segurança da Informação a fim de garantir a confidencialidade, integridade e disponibilidade das informações.

2 OBJETIVO

Estabelecer diretrizes, responsabilidades e regras de Segurança da Informação para garantir a proteção adequada das informações, bem como, conscientizar sobre comportamentos a serem observados por todos colaboradores e terceiros em relação ao uso seguro da informação.

3 ABRANGÊNCIA

A Política de Segurança da Informação abrange todo ambiente da AD'ORO. Aplica-se a todos os colaboradores, estagiários, aprendizes e prestadores de serviços que, de forma direta ou indireta, tenham acesso, por meio digital ou não, às informações e dependências da AD'ORO.

4 LOCAL E DISPONIBILIDADE DESTA POLÍTICA

Este documento está disponível a todos os colaboradores, estagiários, aprendizes e prestadores de serviços nos formatos impresso e/ou digital.

- Impresso: departamento de Recursos Humanos e Jurídico.
- Digital: Intranet.

5 DIRETRIZES

5.1 ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

5.1.1 COMITÊ DE SEGURANÇA DA INFORMAÇÃO

O Comitê de Segurança da Informação (CSI) é um órgão tático-estratégico, responsável por promover a Segurança da Informação, apoiando a alta administração como órgão representante das áreas de negócio e atuando como interface tática com os Processos de Segurança da Informação (SI).

5.1.2 PAPÉIS E RESPONSABILIDADES

A Política de Segurança aplica-se a todos os colaboradores, parceiros e a qualquer pessoa custodiante de informações da Ad'oro ou de seus clientes. Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade industrial (Lei nº 9.279/96) e de direitos autorais (Lei nº 9610/98). A Ad'oro entende que o sistema de segurança da informação somente será eficaz com o comprometimento de TODOS.

A Política de Segurança da Informação (PSI) será aprovada, mantida, administrada e monitorada pelas áreas ou funções abaixo por meio das seguintes atribuições:

- **Colaboradores**, **estagiários, aprendizes e prestadores de serviços**
  - Cumprir as orientações dispostas na PSI;
  - Participar ativamente dos programas de conscientização e treinamentos, associados à PSI;
  - Buscar orientação junto ao gestor imediato em caso de dúvidas associadas à PSI e comunicar os responsáveis pela Segurança da Informação sempre que ocorrer possíveis violações dos controles estabelecidos.
  - Utilizar de forma ética, legal e responsável os recursos computacionais e as informações da AD'ORO; e
  - Assinar o Termo de Confidencialidade.

- **Gestores**
  - Apoiar a conscientização da importância da Segurança da Informação e da PSI;
  - Garantir a efetiva participação dos colaboradores, estagiários, aprendizes e prestadores de serviços nas ações de Segurança da Informação e apoiar, quando necessário, no tratamento de incidentes de SI relacionados à sua área/departamento;
  - Fiscalizar e certificar que todos os colaboradores sob sua gestão estejam em conformidade com a PSI;
  - Aplicar sanções administrativas, orientadas pelo departamento de Recursos Humanos, no caso de descumprimento dos controles estabelecidos na PSI; e
  - 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 e garantir a efetiva participação dos gestores nas ações de Segurança da Informação;
  - Avaliar e validar o orçamento para as ações de Segurança da Informação;
  - Definir em conjunto com o departamento de Recursos Humanos e/ou Gestores, quando necessário, sanções em caso de violação da PSI; e
  - Autorizar o acesso ou compartilhamento das informações sob sua exclusiva responsabilidade.

- **Comitê de Segurança da Informação**
  - Analisar, avaliar e propor ações que mitiguem os riscos de segurança da informação na organização, facilitando o processo de aprovação das medidas pela Diretoria;
  - Desenvolver, manter e aprimorar a Política de Segurança da Informação;

- Propor a adoção de 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;
- Atuar como interface com as áreas de negócio no mapeamento de demandas relacionadas à PSI; e
- Solicitar apuração de possível violação da PSI.

- **Departamento de Recursos Humanos**
  - Coletar a assinatura dos colaboradores, estagiários, aprendizes e prestadores de serviços formalizando o aceite do Termo de Confidencialidade e manter em arquivo, em conformidade com a Lei 13.709/2018- Lei Geral de Proteção de Dados Pessoais; e
  - Orientar os gestores ao aplicar sanções administrativas em seus colaboradores, no caso de descumprimento dos controles estabelecidos na PSI;

- **Departamento Jurídico**
  - Analisar e avaliar juridicamente a PSI e suas revisões;
  - Elaborar e validar o Termo de Confidencialidade; e
  - 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 dos controles definidos em políticas, normas e processos associados à Segurança da Informação; e

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

5.2 SEGURANÇA EM RECURSOS HUMANOS

5.2.1 ANTES DA CONTRATAÇÃO

- Deve ser estabelecido um processo que assegure veracidade das informações fornecidas pelo profissional em processo de contratação.

5.2.2 NA CONTRATAÇÃO

- Deve ser assegurado que o profissional contratado tenha ciência da Política de Segurança da Informação antes de obter acesso às informações e sistemas da organização.
- Todos os colaboradores, estagiários, aprendizes e prestadores de serviços devem receber treinamento de conscientização de Segurança da Informação no momento de sua contratação.

5.2.3 DURANTE E APÓS A DEMISSÃO

- Deve ser estabelecido um processo que assegure a adequada proteção das informações da empresa durante e após a rescisão de contrato de colaboradores, estagiários, aprendizes e prestadores de serviços, garantindo que sejam devolvidos todos os ativos que estavam em sua posse (equipamentos, mídias, documentos, cartões de acesso e outros), remoção dos acessos, alteração das senhas e avaliação das pessoas que devem ser comunicadas sobre o desligamento.

5.3 GESTÃO DE ATIVOS

5.3.1 INVENTÁRIO

Todos os ativos da empresa devem ser inventariados. Os principais ativos de informação (sistemas, diretórios de rede, entre outros) devem ter o seu responsável definido. Os critérios de

classificação devem observar os níveis definidos no item 5.3.3 com objetivo de garantir a adequada proteção do ativo.

5.3.2 RECURSOS CORPORATIVOS

Todos os recursos computacionais corporativos (desktops, notebooks, celulares, softwares, servidores, impressoras e outros) devem ser utilizados somente para fins profissionais alinhados aos interesses da AD'ORO.

5.3.3 USO E CLASSIFICAÇÃO DA INFORMAÇÃO

As informações geradas, manipuladas e armazenadas na organização são de propriedade da AD'ORO e devem ser protegidas em todo o seu ciclo de vida. Com a classificação, assegura-se que a Informação receba um nível adequado de proteção de acordo com a sua importância para a organização.

Todos na organização devem conhecer e aplicar a Classificação da Informação, evitando desta forma, o tratamento indevido das informações.

- Confidenciais: são informações que necessitam de sigilo absoluto, devem ser protegidas e estarem disponíveis apenas para pessoas autorizadas. A divulgação indevida deste tipo de informação, pode ocasionar um sério impacto na continuidade dos negócios da empresa;
- Restritas: são informações referentes a um determinado assunto ou área da organização. A divulgação indevida deste tipo de informação poderá afetar os processos de negócio da empresa;
- Internas: são informações geradas, acessadas, manipuladas e armazenadas internamente na organização. A divulgação indevida este tipo de informação poderá afetar a imagem da empresa; e
- Públicas: são informações de conhecimento público e que não possuem restrições de acesso.

5.4 SEGURANÇA FÍSICA E DE AMBIENTE

Mecanismos de controles de acessos devem ser implementados nas entradas dos ambientes que possuam informações sensíveis da empresa, especialmente nos ambientes de *datacenters*, garantindo o controle e a rastreabilidade.

Todos os visitantes, terceiros e fornecedores somente podem ter acesso as instalações físicas da empresa quando devidamente autorizados, identificados e seus dados registrados.

Devem ser usados crachás distintos, com objetivo de permitir facilmente a identificação da pessoa, como sendo colaboradores, prestadores de serviços, visitantes e outros.

5.5 SEGURANÇA NAS OPERAÇÕES

5.5.1 GERENCIAMENTO DE SERVIÇOS DE TERCEIROS

- Os terceiros devem ter o mínimo acesso às informações e recursos da ADORO, que somente permita a adequada execução de suas atribuições.
- Convém que seja estabelecida uma norma clara com os requisitos de Segurança da Informação para terceiros, incluindo definições de requisitos, responsabilidade de reporte de incidentes, monitoramento e auditorias.

5.5.2 GESTÃO DE MUDANÇAS

- Deve ser estabelecido um processo para Gestão de Mudanças nos sistemas e na infraestrutura de TI, garantindo o efetivo planejamento e avaliação do impacto na Segurança da Informação.
- Este processo deve garantir a efetiva análise das mudanças, classificação de riscos, níveis de aprovação, fluxo de desenvolvimento, teste e produção.
- Convém que o processo de Gestão de Mudanças seja estendido, com os mesmos critérios, para todas as áreas de negócio.

5.5.3 BACKUP (CÓPIA DE SEGURANÇA)

- Um processo de cópia de segurança deve ser estabelecido e formalizado, com o objetivo de garantir a recuperação das informações sempre que necessário.

- Testes periódicos de recuperação de informações do backup devem ser realizados com o objetivo de garantir a integridade do processo.
- O tempo de retenção deve observar as necessidades do negócio e a legislação pertinente.
- Convém que pelo menos uma cópia de segurança seja mantida em um segundo ambiente físico.
- O controle de acesso ao backup deve ser rigoroso.

5.5.4 USO E INSTALAÇÃO DE SOFTWARE

O departamento de Tecnologia da Informação é responsável por homologar, controlar e manter os softwares utilizados na empresa, respeitando os direitos de propriedade intelectual.

Apenas softwares homologados e autorizados pelo departamento de Tecnologia da Informação podem ser instalados nos equipamentos da empresa.

5.5.5 TROCA DE INFORMAÇÕES

Toda troca de informação com clientes, parceiros e terceiros deve ser realizada por meios homologados e autorizados pelo departamento de Tecnologia da Informação, usando, sempre que possível, mecanismo de criptografia.

5.5.6 MONITORAMENTO

A AD'ORO resguarda-se o direito de monitorar, registrar e auditar, sem aviso prévio, os recursos existentes: estações de trabalho, servidores, correio eletrônico, conexões com a internet, sistemas e informações acessadas ou manipuladas no ambiente.

5.6 CONTROLE DE ACESSO LÓGICO

Um processo de Gestão de Acesso deve ser estabelecido e formalizado, garantindo responsabilidades claras e um fluxo para a definição, solicitação, autorização, liberação, remoção e mudanças nos acessos e nos perfis.

Os acessos aos sistemas de informação, aplicativos, diretórios de rede, equipamentos de TI e demais recursos devem ser restritos às pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Deve-se aplicar a regra de mínimo acesso.

5.7 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Requisitos de Segurança da Informação devem ser estabelecidos pelo departamento de Tecnologia da Informação antes do início do processo de desenvolvimento, durante a implantação e na manutenção dos Sistemas.

O ambiente de desenvolvimento deve ser segregado do ambiente de produção.

5.8 GESTÃO DE INCIDENTES

Os incidentes de Segurança da Informação são eventos indesejados que podem comprometer a Segurança da Informação e ameaçar as operações do negócio.

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

Convém que seja estabelecido um processo formal para gestão de incidentes de Segurança da Informação, definindo responsabilidades, hierarquia no tratamento, diretrizes de resposta a incidente, entre outros pontos relevantes.

5.9 GESTÃO DE CONTINUIDADE DE NEGÓCIOS

Um processo de Gestão de Continuidade de Negócios (GCN) deve ser estabelecido, com o objetivo de identificar possíveis ameaças e impactos nas operações caso alguma ameaça se concretize, fortalecendo a resiliência organizacional, capaz de responder aos eventos de desastres, protegendo as partes interessadas, a reputação, a marca e a continuidade dos processos críticos.

5.10 CONFORMIDADE

A Política de Segurança da Informação está em conformidade com os requisitos do negócio, com as regulamentações pertinentes e com a legislação.

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

5.10.1 ADERÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O não cumprimento desta Política e das Normas de Segurança da Informação acarretará violação às regras internas da empresa e sujeitará os colaboradores, estagiários, aprendizes e

prestadores de serviços às medidas administrativas e legais cabíveis.

5.10.2 AUDITORIA

O processo de auditoria externa deve ser estabelecido, com o objetivo de garantir avaliações sistemáticas e ações de melhorias e mitigação de riscos de Segurança da Informação.

6 NORMAS GERAIS

6.1 USO DO E-MAIL

Os colaboradores são responsáveis pelas informações enviadas por seus e-mails.

O e-mail corporativo deve ser utilizado somente para fins profissionais alinhado aos interesses da AD'ORO.

Não é permitido:

- Encaminhar e/ou armazenar mensagens de conteúdo censurável ou impróprio (ex. conteúdo difamatório, discriminatório, preconceituoso, obsceno, pornográfico, ofensivo etc.), que possam violar direitos de terceiros e leis aplicáveis;
- Cadastrar o e-mail corporativo com propósitos não relacionados as atividades corporativas (ex. redes sociais, sites, fóruns, lista de discussão, entre outros);
- Utilizar o e-mail particular (ex. gmail, yahoo, uol etc.) quando conectado na rede da AD'ORO, exceto em casos formalmente autorizados;
- Abrir ou encaminhar mensagens consideradas suspeitas ou caracterizadas como corrente, *SPAM* e *Phishing (técnica de fraude online);*
- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas.

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

Os colaboradores, estagiários, aprendizes e prestadores de serviços devem acessar somente sites confiáveis, autorizados e com o conteúdo relacionado às atividades da AD'ORO.

Não é permitido:

- Acessar página com conteúdo ilícito;
- Fazer *download* de material indevido, entre eles, músicas, filmes, conteúdo com direito autoral não autorizado;
- Acessar sites e ferramentas cujo objetivo seja burlar as regras de controle de acesso da empresa;
- Utilizar serviços de armazenamento em nuvem, não homologados e autorizados pelo departamento de Tecnologia da Informação.
- A internet disponibilizada pela AD'ORO aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.
- É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

6.3 REDES SOCIAIS

Os colaboradores, estagiários, aprendizes e prestadores de serviços não estão autorizados a publicar fotos, vídeos, áudios ou informações, da empresa ou em nome da empresa, nas Redes Sociais,

exceto aqueles que são autorizados devido às suas atribuições corporativas ou em casos autorizados expressamente.

6.4 POLÍTICA DE MESA E TELA 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

O acesso aos recursos de informação do ambiente da AD'ORO é realizado por autenticação dos usuários por meio de senhas. 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;
- 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 USO E INSTALAÇÃO DE SOFTWARE

- Não é permitida a instalação de nenhum programa ou aplicativo sem a homologação e autorização do departamento de Tecnologia da Informação.
- É proibida a utilização de qualquer software *portable* (que não necessita instalação no equipamento) no ambiente.

6.7 IMPRESSORAS

O uso de impressoras deve estar relacionado somente aos interesses da empresa.

- Ao usar uma impressora, deve-se recolher, imediatamente, os documentos impressos;
- O uso de senhas para a impressão de documentos caso o equipamento forneça tal recurso, deve ser aplicado.

6.8 DISPOSITIVOS MÓVEIS

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

- **Dispositivos Móveis Corporativos:**
  - Devem ser usado apenas para fins corporativos, alinhados aos interesses da AD'ORO;
  - 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;

- O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela AD'ORO.
- As seguintes práticas para uso de notebooks fora da empresa devem ser seguidas:
  - Durante o deslocamento de carro, priorize armazenar o equipamento no porta-malas;
  - Em locais públicos (recepção de hotéis, feiras, eventos, restaurantes, dentre outros), mantenha o notebook próximo e sempre à vista;
  - Em aeroportos, evite colocar o equipamento no carrinho de malas;
  - Em viagem, o equipamento deve ser levado como bagagem de mão;
  - Não deixar o equipamento no carro quando não estiver no veículo.

Dispositivos Móveis Particulares - No ambiente da AD'ORO não é permitido utilizar o dispositivo móvel particular para as atividades abaixo listadas, salvo exceções, com permissão do departamento de Tecnologia da Informação:

- Gravar áudio, vídeo ou foto nas dependências da empresa;
- Armazenar informações corporativas;
- Utilizá-lo como modem;

6.9 EXCEÇÕES AO USO DO APLICATIVO DE COMUNICAÇÃO WHATSAPP SERÃO ADMITIDAS, MEDIANTE AUTORIZAÇÃO DO GESTOR DA ÁREA.

6.10 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 Tecnologia da Informação, em função das necessidades operacionais dos colaboradores, estagiários, aprendizes e prestadores de serviços.

6.11 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 Tecnologia da Informação.

6.12 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 Tecnologia da Informação.

6.13 DISPOSIÇÕES FINAIS

O comprometimento com a ética e a participação de todos os usuários da AD'ORO com a Política de Segurança da Informação se faz necessário para um maior controle e minimização dos riscos do negócio, primando pela excelência das atividades e melhorando a imagem da empresa junto à sociedade.

7 GLOSSÁRIO

- **Acesso Lógico**: acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação.
- **Credencial de Acesso**: usuário e senha fornecidos aos colaboradores para acessar os recursos computacionais da AD'ORO, tais como, logon de rede, logon de sistema.
- **Colaborador:** indivíduo que exerce uma atividade sob um contrato de trabalho com a empresa, em tempo parcial ou integral;
- **CSI**: Comitê de Segurança da Informação.

- **Incidentes de SI:** ação ou atitude dos colaboradores, estagiários, aprendizes e prestadores de serviços que não esteja aderente aos controles estabelecidos na PSI e normas internas.
- **PSI:** Política de Segurança da Informação.
- **Recursos Computacionais**: computadores, monitores, scanner, impressoras, notebooks, Datashow, celulares corporativos.
- **Servidores:** equipamento de TI que suporta os aplicativos, software, arquivos de rede e processa as informações.
- **SI:** Segurança da Informação.
- **TI:** Tecnologia da Informação
- **Usuários**: todos os colaboradores, estagiários, aprendizes e prestadores de serviços, fornecedores, clientes ou quaisquer outros que, porventura, venham a utilizar os recursos de Tecnologia da Informação.

8 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.

9 REVISÕES

Para um melhor nível de maturidade desta política, as revisões devem ser feitas anualmente ou sempre que houver alguma mudança significativa nos controles que a contemplam.

REVISÃO	DESCRIÇÃO	RESPONSÁVEL	DATA
1.0	VERSÃO INICIAL	DEPARTAMENTO DE TI	09/2019
2.0	Revisão em razão da entrada em vigor da LGPD	Comitê de Proteção de Dados e Privacidade	03/2022
3.0	Revisão anual obrigatória	TI e DPO	05/2023