PO-08 POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

Revisão 03

Rua Irmã Gabriela, 51 – Salas: 201 e 202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
dexter@dexterengenharia.com.br
(11) 5543-3011

Sumário

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

1. CONTROLE DE REVISÕES

Revisão	Data	Alterações	Elaborado por:	Aprovado por:
00	03/02/20	Emissão inicial	Priscila Popovici	Ricardo Molari
01	05/05/21	Revisão e alteração endereço	Magda Montanari	Ricardo Molari
02	08/02/24	Inclusão do item: 7. Classificação da Informação	Magda Montanari e Priscila Popovici	Ricardo Molari
02	18/07/24	Inclusão dos itens: 2.1. Nossos valores em relação à segurança da informação 3.1. Procedimento para comunicar mudanças 5.1. Usuários da informação 7.3.7. Descarte segurança de informações 8.1. Plano de comunicação interna 8.2. Compromisso com a melhoria contínua 10.1. Sanções por violações 10.2. Procedimento de aplicação de sanções 10.3. Sanções para terceiros contratados ou prestadores de serviço 10.4. Atividades ilegais e danos à empresa 10.5. Procedimento de apelação 11.1. Procedimento de avaliação contínua	Magda Montanari e Priscila Popovici	Ricardo Molari

2. INTRODUÇÃO

Na DEXTER ENGENHARIA, nossa missão é oferecer serviços de engenharia consultiva e apresentar soluções e informações confiáveis para apoiar na tomada de decisão junto aos clientes.

Entendemos que a informação corporativa é essencial para nossas atividades e para garantir a qualidade e segurança dos produtos que oferecemos aos nossos clientes.

Compreendemos que a manipulação de nossas informações ocorre através de diferentes meios de suporte, armazenamento e comunicação, que são vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

DocuSigned by:
Adriana Bobrow
CF925E19491F478...
DocuSigned by:
CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

Dessa forma, estabelecemos nossa Política Geral de Segurança da Informação (PGSI), como parte integrante do nosso sistema de gestão corporativa, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção às informações da organização ou sob nossa responsabilidade.

2.1. NOSSOS VALORES EM RELAÇÃO À SEGURANÇA DA INFORMAÇÃO

Na DEXTER ENGENHARIA LTDA, somos guiados por um conjunto de valores fundamentais que orientam nossa abordagem à segurança da informação:

2.1.1. Compromisso com a Ética: Adotamos práticas de segurança da informação que refletem nosso compromisso com a ética e a integridade. A transparência e a honestidade são pilares fundamentais em nossas operações e na maneira como lidamos com a informação.

2.1.2. Conformidade com Regulamentações: Estamos comprometidos em cumprir todas as leis, regulamentos e normas aplicáveis à segurança da informação. Monitoramos continuamente o ambiente regulatório para garantir que nossas práticas estejam sempre em conformidade.

2.1.3. Proteção de Dados dos Clientes: A proteção dos dados de nossos clientes é nossa prioridade máxima. Implementamos medidas rigorosas para garantir a confidencialidade, integridade e disponibilidade das informações que nos são confiadas.

2.1.4. Inovação e Melhoria Contínua: Valorizamos a inovação contínua em nossas práticas de segurança da informação. Buscamos constantemente novas tecnologias e métodos para aprimorar a proteção de nossos ativos de informação.

2.1.5. Responsabilidade e Conscientização: Promovemos uma cultura de responsabilidade e conscientização entre todos os nossos colaboradores. Acreditamos que cada membro da equipe tem um papel crucial na proteção das informações da empresa.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...

Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

2.1.6. Continuidade de Negócios: Enfatizamos a importância da continuidade de negócios. Desenvolvemos e mantemos planos de continuidade e recuperação para garantir que possamos responder eficazmente a incidentes de segurança.

3. REVOGAÇÃO

Esta política revoga qualquer outro documento referente ao assunto. A empresa tem o direito de modificar, alterar, incluir ou excluir qualquer regra deste procedimento sempre que julgar conveniente, desde que previamente informada através de uma nova revisão deste documento.

3.1. PROCEDIMENTO PARA COMUNICAR MUDANÇAS

Para garantir que todos os colaboradores estejam cientes das alterações na Política Geral de Segurança da Informação (PGSI), adotaremos o seguinte procedimento:

3.1.1. Notificação Prévia: Qualquer modificação, alteração, inclusão ou exclusão de regras na PGSI será comunicada aos colaboradores com, pelo menos, 30 dias de antecedência à sua implementação.

3.1.2. Métodos de Comunicação:

- **E-mail Corporativo:** Um e-mail detalhado será enviado a todos os colaboradores informando sobre as alterações na política. Este e-mail incluirá uma descrição das mudanças, a razão por trás delas e a data efetiva da implementação.
- **Intranet da Empresa:** As alterações serão publicadas na intranet da empresa, em uma seção dedicada à segurança da informação. Os colaboradores serão incentivados a revisar esta seção regularmente.
- **Reuniões e Treinamentos:** Serão realizadas reuniões e treinamentos específicos para explicar as alterações e responder a quaisquer dúvidas dos colaboradores. Sessões de perguntas e respostas serão incluídas para garantir a compreensão completa das mudanças.

3.1.3. Confirmação de Leitura e Entendimento:

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...

Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

- **Assinatura Digital:** Os colaboradores serão solicitados a confirmar a leitura e o entendimento das alterações na PGSI através de uma assinatura digital. Esta confirmação será registrada e mantida para auditorias futuras.

3.1.4. Documentação e Arquivamento:

- **Registro de Revisões:** Todas as revisões da PGSI serão documentadas, incluindo a data de revisão, as alterações feitas e os responsáveis pela revisão.
- **Arquivo Histórico:** Manteremos um arquivo histórico das versões anteriores da PGSI para referência e conformidade.

3.1.5. Feedback e Revisão Contínua:

- **Coleta de Feedback:** Após a implementação das mudanças, será solicitado feedback dos colaboradores sobre o processo de comunicação e a clareza das alterações. Este feedback será utilizado para melhorar futuros processos de comunicação.
- **Revisão Contínua:** O procedimento de comunicação de mudanças será revisado anualmente para garantir sua eficácia e adequação às necessidades da empresa.

4. OBJETIVO

Esta política visa estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores adotarem padrões de comportamento seguro, adequados às metas e necessidades da DEXTER, tais como:

- Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;
- Resguardar as informações da DEXTER, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;
- Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros;
- Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da DEXTER como resultado de falhas de segurança.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

- Promover a inovação contínua em práticas de segurança da informação, assegurando que a empresa se mantenha atualizada com as novas tecnologias e métodos para proteger ativos da informação.

5. APLICAÇÃO

Esta política se aplica a todos os usuários da informação, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a DEXTER, tais como: empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações da empresa e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura DEXTER.

5.1. USUÁRIOS DA INFORMAÇÃO

Para evitar ambiguidades e garantir clareza sobre quem são os usuários da informação, fornecemos as seguintes definições:

- **Empregados Atuais:** Inclui todos os funcionários em tempo integral, meio período, temporários e estagiários que trabalham na DEXTER ‘e têm acesso a informações da empresa.
- **Ex-Empregados:** Funcionários que trabalharam anteriormente na DEXTER e que podem ainda possuir conhecimento ou acesso a informações sensíveis da empresa.
- **Prestadores de Serviço Atuais:** Empresas e indivíduos contratados para fornecer serviços à DEXTER, como consultores, fornecedores de TI, empresas de manutenção e outros prestadores de serviços que têm acesso às informações da empresa como parte de suas responsabilidades.
- **Ex-Prestadores de Serviço:** Empresas e indivíduos que anteriormente prestaram serviços à DEXTER e que podem ter tido acesso a informações sensíveis durante o período de contrato.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

- **Colaboradores:** Inclui todos os membros da equipe que colaboram em projetos, sejam eles internos ou externos, e que têm acesso às informações da DEXTER como parte de suas responsabilidades.
- **Ex-Colaboradores:** Membros da equipe que colaboraram anteriormente em projetos com a DEXTER e que podem ter tido acesso a informações sensíveis da empresa.
- **Consultores:** Profissionais contratados para fornecer aconselhamento especializado ou conduzir projetos específicos que requerem acesso a informações da DEXTER.
- **Parceiros de Negócios:** Organizações com as quais a DEXTER mantém relações comerciais e que podem precisar acessar informações específicas para colaborar eficazmente.
- **Estagiários e Trainees:** Indivíduos em programas de estágio ou trainee que têm acesso a informações da empresa como parte de sua formação e atividades.
- **Subcontratados:** Empresas ou indivíduos contratados por prestadores de serviço principais para realizar partes específicas do trabalho e que têm acesso às informações da DEXTER.

6. DEFINIÇÕES

Item	Descrição
Ameaça	Causa potencial de um incidente que pode vir a prejudicar a DEXTER.
Ativo	Tudo aquilo que possui valor para a DEXTER.
Ativo de Informação	Patrimônio intangível da DEXTER, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a DEXTER por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da DEXTER ou por

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

	infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.
Comitê de Segurança da Informação (CSI)	Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da DEXTER, que tem por finalidade tratar questões ligadas à Segurança da Informação.
Confidencialidade	Propriedade dos ativos da informação da DEXTER, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.
Controle	Medida de segurança adotada pela DEXTER para o tratamento de um risco específico.
Disponibilidade	Propriedade dos ativos da informação da DEXTER, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.
Gestor da Informação	Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.
Incidente de Segurança da Informação	Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da DEXTER.
Integridade	Propriedade dos ativos da informação da DEXTER, de serem exatos e completos.
Risco de Segurança da Informação	Efeito da incerteza sobre os objetivos de segurança da informação da DEXTER.
Segurança da Informação	A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da DEXTER.
Usuário da Informação	Colaboradores com quaisquer modalidades de contrato ou terceiros alocados na prestação de serviços, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação da DEXTER.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

Vulnerabilidade	Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da DEXTER.
Autenticação Multifatorial (MFA)	Método de controle de acesso que requer a apresentação de duas ou mais formas de autenticação de diferentes categorias de credenciais; por exemplo, uma combinação de algo que o usuário sabe (senha), algo que o usuário possui (cartão de acesso) e algo que o usuário é (impressão digital).
Criptografia	Técnica utilizada para proteger a confidencialidade e a integridade das informações, convertendo dados legíveis (texto claro) em um formato codificado (texto cifrado) que só pode ser decifrado por aqueles que possuem a chave de decriptação apropriada.
Auditoria	Processo sistemático e independente de examinar evidências para determinar se as atividades e os resultados relacionados aos sistemas de informação atendem às políticas, processos e requisitos estabelecidos, além de identificar áreas de melhoria.
Monitoramento	Atividade contínua de observar e analisar as operações e atividades de sistemas de informação para detectar eventos de segurança e garantir que os sistemas funcionem conforme esperado. Isso inclui a análise de logs, a detecção de anomalias e a resposta a eventos suspeitos.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

7.1. INVENTÁRIO DE ATIVOS

A Dexter mantém um controle detalhado de seus ativos por meio do Inventário de Ativos, que é regularmente atualizado para refletir com precisão o status e a localização de todos os ativos da empresa. Qualquer alteração relevante nos ativos é registrada imediatamente para garantir a precisão e integridade dos dados do inventário.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

7.1.1. Periodicidade da Atualização: O Inventário de Ativos deve ser atualizado semestralmente, com revisões adicionais realizadas sempre que houver mudanças significativas nos ativos.

7.1.2. Revisão e Auditoria do Inventário:

- **Revisão Anual**: Uma revisão completa do Inventário de Ativos deve ser realizada anualmente para garantir a integridade e precisão dos dados.
- **Auditorias Periódicas**: Auditorias internas devem ser realizadas semestralmente para verificar a conformidade do inventário com as políticas da empresa. Os resultados das auditorias devem ser documentados e reportados ao Comitê de Segurança da Informação (CSI).

7.1.3. Controle de Inventário de Ativos:

O controle de ativos deverá manter as seguintes informações atualizadas:

Item	**Descrição**
Informações Gerais	Data de registro, responsável pelo registro, departamento/área, localização.
Detalhes do Ativo	Tipo do ativo (hardware/software), nome do ativo, fabricante, modelo, número de série, número do inventário, data de aquisição, custo de aquisição, data da instalação, fornecedor, garantia e data de expiração da garantia.
Observações adicionais	Qualquer informação adicional relevante sobre ativo.
Responsável pelo Ativo	Nome do responsável, cargo e contato.
Status do Ativo	Estado do ativo e motivo.

7.2. CLASSIFICAÇÃO E ROTULAGEM DA INFORMAÇÃO

Os documentos devem conter a rotulagem da informação na capa e no rodapé para garantir a clareza e a identificação da sensibilidade da informação contida neles. Desta forma, garantindo que os documentos sejam manuseados e compartilhados conforme sua classificação:

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...

Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

Classificação	Descrição
Confidencial	As informações e/ou documentos classificados com este nível de confidencialidade exigem o mais alto grau de proteção e devem ser manuseados exclusivamente pelos envolvidos diretos no processo. O compartilhamento dessas informações e/ou documentos requer autorização expressa da diretoria da empresa.
Interno	O mais baixo nível de confidencialidade indica que as informações e/ou documentos são de uso interno da Dexter e podem ser compartilhados com os envolvidos internos da empresa.
Público	As informações e/ou documentos são de acesso público e podem ser compartilhados tanto com os envolvidos internos quanto externos da Dexter.

7.3. MANUSEIO DE ATIVOS

O manuseio das informações e/ou documentos deve seguir as seguintes diretrizes:

7.3.1. Documentos Eletrônicos: O acesso a documentos eletrônicos é restrito a colaboradores autorizados, utilizando senhas e criptografia para proteger o acesso aos documentos.

7.3.2. Sistemas de Informações:

- **Controle de Acesso:** O acesso é controlado por meio de autenticação multifatorial (MFA) para garantir a identidade do usuário, reduzindo o risco de acessos não autorizados.
- **Atualização de Segurança:** *Patches* e atualizações de segurança são aplicadas regularmente para proteger contra vulnerabilidades conhecidas. As atualizações são realizadas de acordo com uma programação estabelecida e monitoradas para garantir a conformidade.
- **Auditoria e Monitoramento:** A atividade dos usuários é auditada e monitorada continuamente para detectar e prevenir atividades suspeitas. Os relatórios de auditoria são revisados periodicamente pelo CSI.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

- **Registro de Log**: Logs detalhados de acesso e atividades dos usuários são mantidos e armazenados de forma segura por um período conforme a política de retenção de dados da DEXTER.
- **Gestão de Incidentes:** Um sistema de alerta e resposta a incidentes de segurança da informação é implementado, permitindo a identificação rápida e a tomada de medidas corretivas imediatas.
- **Treinamento Contínuo:** Treinamentos periódicos são realizados para os usuários sobre a importância da segurança dos sistemas de informação e como identificar e responder a potenciais ameaças. Os treinamentos ocorrem semestralmente.

7.3.3. Documentos em Papel: Documentos em papel são armazenados em áreas designadas com controle de acesso físico; armários trancados e etiquetas de classificação de sensibilidade são usados para identificar o nível de confidencialidade dos documentos.

7.3.4. Mídias de Armazenamento: Mídias removíveis são bloqueadas para proteger o acesso não autorizado em caso de perda ou roubo; o armazenamento é feito em áreas designadas com controle de acesso físico.

7.3.5. Informações Transmitidas Verbalmente: A discussão de informações sensíveis é restrita a ambientes seguros e privados; códigos ou siglas são utilizados para referenciar informações sensíveis em comunicações verbais em ambientes públicos; colaboradores são treinados sobre a importância de não discutir informações confidenciais em locais públicos ou não seguros.

7.3.6. E-mail: Criptografia é utilizada para proteger o conteúdo de e-mails contendo informações sensíveis; políticas de uso aceitável de e-mails orientam os colaboradores sobre o manuseio adequado de informações confidenciais; colaboradores são sensibilizados e treinados para reconhecer e-mails de *phishing* e outras ameaças de segurança.

7.3.7. Descarte Seguro de Informações:

- **Documentos Eletrônicos:** Softwares de destruição de dados são utilizados para garantir que as informações sejam irrecuperáveis.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

- **Documentos em Papel:** A destruição física, como fragmentação, é realizada para garantir que as informações não possam ser reconstruídas.
- **Mídias de Armazenamento:** Procedimentos específicos de destruição são aplicados para discos rígidos, CDs, DVDs e outros dispositivos de armazenamento, como a desmagnetização ou a fragmentação física.

8. DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO

A Política Geral de Segurança da Informação (PGSI) da DEXTER visa garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos na instituição.

A Diretoria e o Comitê de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação na DEXTER. Dessa forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da DEXTER.

8.1. PLANO DE COMUNICAÇÃO INTERNA

Para assegurar que a política e suas atualizações sejam amplamente comunicadas internamente, implementaremos o seguinte plano de comunicação:

8.1.1. Notificação por E-mail: Enviaremos um e-mail detalhado a todos os colaboradores informando sobre qualquer atualização ou alteração na PGSI. O e-mail incluirá uma descrição das mudanças, a razão por trás delas e a data efetiva da implementação.

8.1.2. Publicação na Intranet: Publicaremos todas as atualizações na intranet da empresa, em uma seção dedicada à segurança da informação. Os colaboradores serão incentivados a revisar esta seção regularmente.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

8.1.3. Reuniões e Treinamentos: Organizaremos reuniões e treinamentos específicos para explicar as alterações e responder a quaisquer dúvidas dos colaboradores. Sessões de perguntas e respostas serão incluídas para garantir a compreensão completa das mudanças.

8.1.4. Confirmação de Leitura e Entendimento: Solicitaremos que os colaboradores confirmem a leitura e o entendimento das alterações na PGSI através de uma assinatura digital. Esta confirmação será registrada e mantida para auditorias futuras.

8.2. COMPROMISSO COM A MELHORIA CONTÍNUA

Reconhecemos que a segurança da informação é um campo em constante evolução e, portanto, estamos comprometidos com a melhoria contínua de nossas práticas de segurança da informação. Este compromisso inclui:

8.2.1. Avaliação Regular: Realizaremos avaliações regulares das nossas políticas, procedimentos e controles de segurança para identificar áreas de melhoria. Essas avaliações incluirão auditorias internas e externas, bem como feedback de colaboradores e outras partes interessadas.

8.2.2. Adaptação a Novas Tecnologias e Ameaças: Permaneceremos atualizados sobre as novas tecnologias e tendências em segurança da informação. Adotaremos inovações tecnológicas e melhores práticas para fortalecer nossa postura de segurança contra ameaças emergentes.

8.2.3. Capacitação Contínua: Investiremos continuamente na capacitação de nossos colaboradores através de treinamentos regulares e programas de conscientização sobre segurança da informação. Acreditamos que uma equipe bem-informada é fundamental para a proteção eficaz das informações da empresa.

8.2.4. Melhoria de Processos: Implementaremos processos de melhoria contínua, utilizando métricas e indicadores de desempenho para monitorar a eficácia das nossas medidas de

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

segurança. As lições aprendidas de incidentes de segurança e auditorias serão usadas para aprimorar nossas práticas.

8.2.5. Feedback e Participação Ativa: Encorajaremos todos os colaboradores a fornecer feedback sobre as políticas e procedimentos de segurança da informação. A participação ativa de todos é crucial para identificar e mitigar riscos de forma eficaz.

9. PAPÉIS E RESPONSABILIDADES

9.1. COMITÊ DE SEGURANÇA DA INFORMAÇÃO – CSI

O Comitê de Segurança da Informação (CSI) é composto por uma equipe multidisciplinar, incluindo pelo menos um representante da diretoria e membros seniores das áreas de Tecnologia da Informação, Segurança da Informação, Recursos Humanos e Jurídico.

9.1.1. Responsabilidades do CSI:

- Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação.
- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação.
- Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PGSI.
- Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da Dexter.

9.1.2. Qualificações Necessárias para os Membros do CSI:

- **Diretoria:** Experiência mínima de 5 anos em gestão estratégica e conhecimento profundo das operações da empresa.
- **Tecnologia da Informação:** Profissionais com formação superior em TI ou áreas correlatas, com certificações relevantes e pelo menos 5 anos de experiência em segurança da informação.
- **Recursos Humanos:** Profissionais com formação em Recursos Humanos ou áreas correlatas, com experiência em gestão de políticas e conformidade.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

- **Jurídico:** Advogados com experiência em direito digital e conformidade regulatória.

9.1.3. Frequência das Reuniões do CSI:

O CSI se reunirá trimestralmente para revisar e discutir questões de segurança, além de reuniões extraordinárias sempre que necessário para tratar de incidentes críticos ou mudanças significativas na política de segurança.

9.2. GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

9.2.1. Responsabilidades da Gerência de Segurança da Informação:

- Conduzir a gestão e operação da segurança da informação, tendo como base esta política e demais resoluções do CSI.
- Apoiar o CSI em suas deliberações.
- Elaborar e propor ao CSI as normas e procedimentos de segurança da informação necessários para fazer cumprir a PGSI.
- Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco.
- Tomar as ações cabíveis para fazer cumprir os termos desta política.
- Realizar a gestão dos incidentes de segurança da informação conforme a Política de Resposta a Incidentes de Segurança da Informação (PO-13-PRISI).
- Monitorar continuamente a eficácia das medidas de segurança implementadas, realizando auditorias internas periódicas e relatando os resultados ao CSI.
- Manter-se atualizado sobre as novas ameaças e tendências em segurança da informação, adotando tecnologias e práticas inovadoras para fortalecer a postura de segurança da organização.
- Desenvolver e manter planos de continuidade de negócios e recuperação de desastres, assegurando que estejam testados e atualizados conforme necessário.
- Garantir a conformidade com todas as leis, regulamentações e normas aplicáveis relacionadas à segurança da informação, reportando quaisquer não-conformidades ao CSI e às autoridades competentes, quando necessário.

9.2.2. Qualificações Necessárias para a Gerência de Segurança da Informação:

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

- Formação superior em Tecnologia da Informação, Segurança da Informação ou áreas correlatas.
- Certificações relevantes.
- Experiência mínima de 5 anos em gestão de segurança da informação.
- Conhecimento atualizado sobre as melhores práticas, normas e regulamentações em segurança da informação.

9.3. GESTORES DA INFORMAÇÃO

9.3.1. Responsabilidades dos Gestores da Informação:

- Ler, compreender e cumprir integralmente os termos da PGSI, bem como as demais normas e procedimentos de segurança aplicáveis.
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a PGSI, suas normas e procedimentos à Gerência de Segurança da Informação ou, quando pertinente, ao CSI.
- Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da DEXTER.
- Assinar o Termo de Uso de Sistemas de Informação da DEXTER, formalizando a ciência e o aceite integral das disposições da PGSI, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento.
- Responder pela inobservância da PGSI, normas e procedimentos de segurança, conforme definido no item sanções e punições.

9.4. USUÁRIOS DA INFORMAÇÃO

9.4.1. Responsabilidades dos Usuários da Informação:

- Ler, compreender e cumprir integralmente os termos da PGSI, bem como as demais normas e procedimentos de segurança aplicáveis.
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a PGSI, suas normas e procedimentos à Gerência de Segurança da Informação ou, quando pertinente, ao CSI.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

- Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da DEXTER.
- Assinar o Termo de Uso de Sistemas de Informação da DEXTER, formalizando a ciência e o aceite integral das disposições da PGSI, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento.
- Responder pela inobservância da PGSI, normas e procedimentos de segurança, conforme definido no item sanções e punições.

10. SANÇÕES E PUNIÇÕES

10.1. SANÇÕES POR VIOLAÇÕES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como das demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e demissão por justa causa. A escolha da penalidade será baseada na gravidade da violação e nas circunstâncias de cada caso.

10.1.1. Exemplos de Violações e Respectivas Sanções:

Violação	Descrição	Sanção
Acesso Não Autorizado	Acessar informações confidenciais sem a devida autorização.	1. Advertência por escrito na primeira ocorrência; 2. Suspensão não remunerada em caso de reincidência.
Compartilhamento Indevido de Informações	Divulgar informações sensíveis a terceiros sem autorização.	1. Suspensão não remunerada na primeira ocorrência; 2. Demissão por justa causa em caso de reincidência.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

Uso Indevido de Recursos da Empresa	Utilizar sistemas e recursos da empresa para fins pessoais ou fora do escopo permitido.	1. Advertência verbal na primeira ocorrência; 2. Advertência por escrito em caso de reincidência.
Negligência na Proteção de Informações	Deixar documentos confidenciais desprotegidos ou não seguir procedimentos de segurança estabelecidos.	1. Advertência por escrito na primeira ocorrência; 2. Suspensão não remunerada em caso de reincidência.
Fraude ou Falsificação de Documentos	Criar ou alterar documentos de forma fraudulenta.	1. Demissão por justa causa.

10.2. PROCEDIMENTO DE APLICAÇÃO DE SANÇÕES

A aplicação de sanções e punições será realizada conforme a análise do Comitê de Segurança da Informação (CSI), devendo-se considerar:

- A gravidade da infração.
- O efeito alcançado pela violação.
- A recorrência da infração.
- As hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho (CLT).
- Outras circunstâncias atenuantes ou agravantes identificadas pelo CSI.

O CSI, no uso do poder disciplinar que lhe é atribuído, aplicará a pena que entender cabível quando tipificada a falta grave.

10.3. SANÇÕES PARA TERCEIROS CONTRATADOS OU PRESTADORES DE SERVIÇO

No caso de terceiros contratados ou prestadores de serviço, o CSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato. As penalidades podem incluir:

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

- Rescisão do contrato de prestação de serviços.
- Multas contratuais.
- Outras sanções previstas em contrato.

10.4. ATIVIDADES ILEGAIS E DANOS À EMPRESA

Para o caso de violações que impliquem em atividades ilegais ou que possam incorrer em dano à DEXTER, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 10.1, 10.2 e 10.3 desta política. Além disso, a DEXTER cooperará com as autoridades competentes para a investigação e eventual responsabilização criminal dos envolvidos.

10.5. PROCEDIMENTO DE APELAÇÃO

Qualquer colaborador que receba uma sanção tem o direito de apelar da decisão. O procedimento de apelação é:

10.5.1. Submissão de Apelação: O colaborador deve submeter uma apelação por escrito ao CSI dentro de 10 dias úteis após a notificação da sanção. A apelação deve incluir uma explicação detalhada dos motivos pelos quais o colaborador acredita que a sanção foi injusta ou incorreta.

10.5.2. Revisão da Apelação: O CSI revisará a apelação, considerando todas as evidências apresentadas pelo colaborador e quaisquer informações adicionais relevantes.

10.5.3. Audiência de Apelação: Se necessário, uma audiência será agendada para permitir que o colaborador apresente seu caso pessoalmente. O colaborador pode ser acompanhado por um representante de sua escolha.

10.5.4. Decisão Final: O CSI emitirá uma decisão final por escrito dentro de 15 dias úteis após a submissão da apelação ou da audiência, se realizada. A decisão será final e obrigatória.

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: R.B. CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

10.6. COMUNICAÇÃO DAS SANÇÕES

Todos os colaboradores, contratados e terceiros serão informados das sanções e punições possíveis e do processo de aplicação destas, como parte do treinamento inicial e contínuo sobre segurança da informação.

11. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê de Segurança da Informação (CSI) para posterior deliberação.

11.1. PROCEDIMENTO DE AVALIAÇÃO CONTÍNUA

Para garantir que os casos omissos sejam devidamente avaliados, documentados e utilizados para a melhoria contínua das políticas e procedimentos, implementaremos o seguinte procedimento:

11.1.1. Identificação de Casos Omissos: Todos os colaboradores têm a responsabilidade de relatar quaisquer situações ou incidentes que não estejam claramente cobertos pela Política Geral de Segurança da Informação (PGSI) ou pelos procedimentos existentes. Estes relatos devem ser feitos diretamente ao CSI por meio de um formulário específico disponível na intranet da empresa.

11.1.2. Avaliação Inicial: O CSI revisará todos os relatos de casos omissos na sua próxima reunião programada, ou em uma reunião extraordinária se o caso exigir atenção imediata. A avaliação incluirá a análise do incidente, seu impacto potencial e as circunstâncias envolvidas.

11.1.3. Documentação: Todos os casos omissos serão documentados detalhadamente, incluindo a descrição do incidente, a análise realizada pelo CSI, as decisões tomadas e quaisquer medidas corretivas ou preventivas implementadas. Esta documentação será mantida em um registro específico de casos omissos.

11.1.4. Atualização de Políticas e Procedimentos: Com base na avaliação dos casos omissos, o CSI fará recomendações para atualizar a PGSI e os procedimentos relacionados,

DocuSigned by: Adriana Bobrow CF925E19491F478...
DocuSigned by: CE312D8BE870458...
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

garantindo que situações semelhantes sejam adequadamente cobertas no futuro. As atualizações propostas serão submetidas à aprovação da Diretoria Executiva antes de serem implementadas.

11.1.5. Comunicação das Atualizações: Uma vez aprovadas, as atualizações serão comunicadas a todos os colaboradores conforme o Plano de Comunicação Interna descrito na seção 8.1. Isto incluirá notificações por e-mail, publicações na intranet, reuniões e treinamentos.

11.1.6. Revisão e Melhoria Contínua: O CSI realizará revisões periódicas das políticas e procedimentos para garantir que estejam atualizados e reflitam as lições aprendidas dos casos omissos. Estas revisões serão documentadas e incorporadas no processo de auditoria interna.

11.1.7. Feedback e Aprendizado: Os colaboradores serão incentivados a fornecer feedback sobre a eficácia das atualizações e a identificar quaisquer novas áreas de melhoria. O CSI considerará este feedback nas revisões contínuas das políticas e procedimentos.

As diretrizes estabelecidas nesta política, bem como nas demais normas e procedimentos de segurança, não são exaustivas devido à contínua evolução tecnológica e ao surgimento constante de novas ameaças. Portanto, é obrigação de cada usuário da informação da DEXTER adotar, sempre que possível, medidas de segurança adicionais além das aqui previstas, para garantir a proteção das informações da empresa.

Essa política entrará em vigor 30 dias após assinatura da Diretoria.

Aprovado em: São Paulo, 31 de julho de 2024.

DocuSigned by:
Adriana Bobrow
CF925E19491F478...
Adriana Bobrow
Diretora

DocuSigned by:
R.B.
CE312D8BE870458...
Ricardo Molari
Diretor

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

ACEITAÇÃO

Eu, _____, portador(a) do R.G. nº. _____ e do CPF _____, recebi uma cópia da Política de Segurança da Informação da DEXTER ENGENHARIA LTDA., declaro ter lido e estar de acordo com as normas e procedimentos aqui apresentados, firmando o compromisso de cumprir as diretrizes da Política Geral de Segurança da Informação – PGSI (PO-08).

_____, _____.

Nome Completo:	
RG:	
CPF:	

_____
Diretoria

Rua Irmã Gabriela, 51 – Salas: 201/202.
Cidade Monções – São Paulo – SP
04571-130

www.dexterengenharia.com.br
lgpd@dexterengenharia.com.br
(11) 5543-3011

DocuSign

Certificado de Conclusão

Identificação de envelope: DD63DDEA611943389B2D4A68A7D396AC
Status: Concluído
Assunto: PO-08-v03-PGSI-rev03.pdf
Envelope fonte:
Documentar páginas: 24
Assinaturas: 44
Remetente do envelope:
Certificar páginas: 5
Rubrica: 0
MAGDA RIBEIRO DA SILVA MONTANARI
Assinatura guiada: Ativado
Rua Irmã Gabriela, 51 - Salas 201 e 202.
Selo com EnvelopeId (ID do envelope): Ativado
SAO PAULO, SP 04571-130
Fuso horário: (UTC-03:00) Brasília
magda.montanari@dexterengenharia.com.br
Endereço IP: 177.198.73.254

Rastreamento de registros

Status: Original
29/07/2024 18:24:27
Portador: MAGDA RIBEIRO DA SILVA MONTANARI
magda.montanari@dexterengenharia.com.br
Local: DocuSign

Eventos do signatário	Assinatura	Registro de hora e data
Adriana Bobrow adriana.bobrow@dexterengenharia.com.br Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	DocuSigned by: Adriana Bobrow CF925E19491F478... Adoção de assinatura: Estilo pré-selecionado Usando endereço IP: 201.26.18.47	Enviado: 29/07/2024 18:31:37 Reenviado: 30/07/2024 09:38:09 Reenviado: 30/07/2024 09:39:05 Visualizado: 31/07/2024 13:48:44 Assinado: 31/07/2024 13:49:08
Termos de Assinatura e Registro Eletrônico: Aceito: 31/07/2024 13:48:44 ID: 696c6737-8c8e-4c7e-a5e2-e9e2f3b1ab18		
Ricardo Bruno Molari ricardo.molari@dexterengenharia.com.br Diretor Financeiro Dexter Engenharia Ltda Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	DocuSigned by: CE312D8BE870458... Adoção de assinatura: Desenhado no dispositivo Usando endereço IP: 177.139.34.175 Assinado com o uso do celular	Enviado: 29/07/2024 18:31:39 Reenviado: 30/07/2024 09:38:10 Reenviado: 30/07/2024 09:39:06 Visualizado: 30/07/2024 17:48:18 Assinado: 30/07/2024 17:49:07
Termos de Assinatura e Registro Eletrônico: Aceito: 30/07/2024 17:48:18 ID: 6c36f575-64c4-48ee-ae57-8fb13ec3a712		

Eventos do signatário presencial	Assinatura	Registro de hora e data
Eventos de entrega do editor	**Status**	**Registro de hora e data**
Evento de entrega do agente	**Status**	**Registro de hora e data**
Eventos de entrega intermediários	**Status**	**Registro de hora e data**
Eventos de entrega certificados	**Status**	**Registro de hora e data**
Eventos de cópia	**Status**	**Registro de hora e data**
Eventos com testemunhas	**Assinatura**	**Registro de hora e data**
Eventos do tabelião	**Assinatura**	**Registro de hora e data**
Eventos de resumo do envelope	**Status**	**Carimbo de data/hora**

Eventos de resumo do envelope	Status	Carimbo de data/hora
Envelope enviado	Com hash/criptografado	29/07/2024 18:31:39
Entrega certificada	Segurança verificada	30/07/2024 17:48:18
Assinatura concluída	Segurança verificada	30/07/2024 17:49:07
Concluído	Segurança verificada	31/07/2024 13:49:08

Eventos de pagamento	Status	Carimbo de data/hora

Termos de Assinatura e Registro Eletrônico

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Dexter Engenharia Ltda. (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Dexter Engenharia Ltda.:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: magda.montanari@dexterengenharia.com.br

To advise Dexter Engenharia Ltda. of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at magda.montanari@dexterengenharia.com.br and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Dexter Engenharia Ltda.

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to magda.montanari@dexterengenharia.com.br and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Dexter Engenharia Ltda.

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to magda.montanari@dexterengenharia.com.br and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Dexter Engenharia Ltda. as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Dexter Engenharia Ltda. during the course of your relationship with Dexter Engenharia Ltda..