1. INTRODUÇÃO

A ARaymond, uma empresa familiar com 150 anos de experiência, desenvolve, fabrica e comercializa soluções de fixação e montagem. Em nossa longa história, sempre focamos na inovação e na industrialização. Os nossos valores fundamentais - cooperação, inovação, pensamento empreendedor e ação e criação de valor - definem quem somos e como trabalhamos, “ são o coração da nossa empresa

A tecnologia da informação é uma parte importante de todos os processos da empresa e, como tal, a ARaymond As empresas da rede devem garantir que um elevado grau de segurança, cuidado e qualidade seja aplicado nos principais áreas.

Devido ao elevado grau de confidencialidade da informação tratada, bem como dos processos e serviços envolvidos, a sua proteção e segurança são de considerável importância para nós.

Objetivos de Segurança da Informação e Proteção de Dados

Os objetivos de segurança da informação da Rede ARaymond são agir de acordo com a lei, ser econômico e responsável, evitar quaisquer riscos desconhecidos e evitar danos à própria Rede ARaymond, funcionários, clientes e parceiros de negócios.

A segurança da informação no sentido de confidencialidade, integridade e disponibilidade da informação trocada é de importância central para nós.

Nosso objetivo é a proteção de todas as informações recebidas, geradas, processadas, divulgadas, armazenadas e destruídas pelas atividades da empresa, bem como o atendimento adequado aos requisitos das regulamentações legais, padrões relevantes, especificações específicas do cliente, bem como obrigações contratuais.

Gestão de Segurança da Informação

Desenvolvemos um sistema de gestão de segurança da informação (SGSI) baseado na norma internacional ISO/IEC 27001 como um dos processos de gestão, que é operado globalmente pela ARaymond Information Technology (Raynet). Desta forma, garantimos que a organização está claramente definida no que diz respeito à segurança da informação, que está integrada em todos os processos de negócio relevantes, que as responsabilidades são reguladas e é garantida a implementação fiável de processos e procedimentos.

Manter a segurança da informação e melhorar continuamente a sua eficácia é uma obrigação para qualquer pessoa que trabalhe para ou em nome da Rede ARaymond.

Segurança da Informação e Proteção de Dados faz parte das tarefas da Gestão

A Administração apoia as estruturas e processos necessários. Para isso, nomearam pessoas responsáveis pela criação de diretrizes para segurança da informação e proteção de dados. Eles são publicados em diretrizes, documentação e instruções de trabalho. As partes responsáveis supervisionam o cumprimento destes regulamentos e procedimentos em todas as áreas. Isto é apoiado por informação e formação para as pessoas relevantes, para garantir que os requisitos são conhecidos e é promovida a sensibilização para a importância da segurança da informação e da protecção de dados.

2. FINALIDADE E APLICABILIDADE

O objetivo desta política é a confirmação do compromisso da ARaymond Brasil quanto à segurança da informação e proteção de dados para todas as partes interessadas externas (clientes, fornecedores, proceiros de negócios, órgão reguladores Brasil entre outros) da ARaymond Network, através da implementação do Sistema de Gestão da Segurança da Informação.

Políticas internas foram estabelecidas para garantir as diretrizes e orientações necessárias para assegurar que as informações recebam um nível adequado de proteção, descrevendo as responsabilidades de cada colaborador e prestador de serviços, quando aplicável, para a correta classificação, manuseio, reprodução, armazenamento, divulgação, eliminação e disposição de informações de propriedade da ARaymond Brasil de acordo com seu grau de sigilo, contemplando o ciclo da informação, desde a sua criação, manuseio, transmissão, transporte e descarte.

3. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Diante da implementação desta Política, a Alta Direção da ARaymond Brasil se compromete em assegurar que os processos e recursos necessários para a manufatura de seus produtos, assegurando a coleta, armazenamento e processamento das informações, sejam implementados, mantidos e monitorados, nomeando o LISO - Local Information Security Office como responsável pelo SGSI.

A ARaymond Brasil disponibiliza internamente sua Política de Segurança da Informação na íntegra a todos usuários internos, e quando necessário ou solicitado para suas partes interessadas externas.

4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta Política de Segurança do Sistema de Informação (ISSP) fornece o principal objetivo estratégico e os requisitos básicos de segurança cibernética a serem seguidos na rede ARaymond.

Diretrizes Gerais Brasil

Esta política, baseada na política global desegurança da informação, demonstra nossa capacidade e integridade em lidar com todas as partes interessadas. Portanto, essa política assegura que:

• As informações estão protegidas contra acesso não autorizado;
• A confidencialidade da informação é mantida;
• As informações não são divulgadas às entidades não autorizadas por meio de ações deliberadas ou descuidadas;
• A integridade das informações é mantida para impedir modificações não autorizadas;
• As informações estão disponíveis para usuários autorizados, quando necessário;
• Sempre que ocorrer alterações legais, regulamentares, normativas ou contratuais que impactem o negócio da ARaymond Brasil, uma análise crítica é realizada a fim de que as adequações, se necessário, sejam realizadas;
• Cada indivíduo tenha conhecimento adequado dos controles de gestão, dos controles operacionais e técnicos que ajudam a proteger os recursos e bens tecnológicos de informação da ARaymond Brasil;
• As políticas, procedimentos e práticas são comunicados às partes envolvidas ARaymond Brasil.

Papéis e Responsabilidades

O Gerente Global de Segurança da Informação é o Principal Responsável pela Segurança da Informação na Rede ARaymond. Ele garante que as políticas de segurança da informação e os objetivos de segurança da informação sejam estabelecidos e sejam compatíveis com a direção estratégica da organização. Ele apoia e garante a integração dos requisitos dos sistemas de gestão de segurança da informação nos processos da Organização.
Ele é responsável por garantir que os recursos necessários para o sistema de gestão de segurança da informação estejam disponíveis. Ele orienta e apoia pessoas para que contribuam para a eficácia dos sistemas de gestão de segurança da informação e promove a melhoria contínua.

A coordenação e a melhoria contínua do "Quadro Global de Segurança da Informação" da Rede ARaymond são delegadas à Equipe Global de Gestão de Segurança da Informação (ISMT).

A Equipe Global de Gestão de Segurança da Informação fornece diretrizes e processos de base harmonizados globais dentro da "Estrutura Global de Segurança da Informação" da Rede ARaymond que devem ser respeitados nas implementações locais do SGSI para garantir que todos os países/entidades que usam a Rede ARaymond tenham o mesmo nível de informações sobre segurança.

Ele fornece metas globais de segurança da informação anualmente

Ele consolida e coleta riscos locais para fornecer uma visão global clara e centralizada aos tomadores de decisão e realizar uma revisão anual de documentos do SGSI global.

Ele garante a consistência das implementações do SGSI e monitora a conformidade com as normas relevantes e a estrutura do SGSI em um nível completo da rede ARaymond com auditorias internas. Cada membro da equipe precisa de uma Certificação Pessoal na ISO27001 de uma Empresa Certificadora para garantir o nível certo de conhecimento.

O Correspondente Global de Privacidade de Dados interage com o Gerente Global de Segurança da Informação e a Equipe Global de Gestão de Segurança da Informação para garantir que a "Estrutura Global de Segurança da Informação" implementada e as medidas relacionadas cobrirão os requisitos de Proteção da Privacidade de Dados.

Regulamentação

A ARaymond Brasil e as partes interessadas envolvidas se comprometem a atender integralmente aos requisitos de segurança da informação e privacidade aplicáveis ou exigidos por regulamentações, estatutos, leis e/ou cláusulas contratuais.

Riscos e Ameaças

Todos os ativos de informação e associados devem ser periodicamente avaliados e os respectivos riscos ao negócio ARaymond Brasil devem ser mapeados conforme metodologia global.

Os riscos e ameaças inerentes à segurança da informação devem ser tratados através da implementação de controles específicos e devem ser periodicamente reavaliados.

Fornecedores

A ARaymond Brasil dispõe de processo de avaliação de riscos dos fornecedores críticos.

Essa metodologia visa detectar, avaliar e gerenciar riscos nos serviços ou produtos prestados por fornecedores e que possam impactar diretamente no negócio da ARaymond Brasil.

Todos os terceiros devem se comprometer a agir de acordo com a Política de Segurança da Informação, sendo imprescindível que o contrato firmado entre as empresas possua cláusula que assegure a confidencialidade das informações e a adesão à Política de Segurança da Informação.

Continuidade de Negócios

A Tecnologia da Informação e Comunicação (TIC) da Araymond Brasil está pronta e preparada para garantir a continuidade dos negócios da organização e garantir que ela atinja seus objetivos.

A atividade de Continuidade de Negócios é assegurada por uma equipe dedicada.

Os planos de continuidade de negócios são produzidos, mantidos e testados de acordo com as expectativas ARaymond Brasil

Classificação e Rotulagem da Informação

As informações devem ser classificadas de acordo com seu valor para uma organização (classificação). Para esta classificação, o valor da informação para a organização deve ser avaliado com base em fatores como confidencialidade, integridade e disponibilidade. O tratamento das informações de acordo com sua classificação será definido e implementado pelos Colaboradores.

O Gestor/Supervisor é responsável pela classificação das informações na sua área de responsabilidade.

Normalmente, ele faz parte do gerenciamento departamental ou de projetos ou tem responsabilidades abrangentes (por exemplo, segurança da informação, segurança ocupacional e proteção de dados). A classificação determina o grupo de usuários (pessoas internas e externas) por nome ou por funções, bem como suas autorizações. A responsabilidade pela classificação das informações também pode ser delegada a outros colaboradores.

Rotulagem implícita significa que um documento não precisa de rotulagem quando não sai da área central onde todos os usuários estão cientes da classificação. Rotulagem Explícita significa que a classificação deve ser adicionada ao documento em cada caso.

- Classificação "Público”
- Classificação “Interna”

- Classificação “Confidencial”
- Classificação “Estritamente Confidencial”

Treinamento e Conscientização

Araymond Brasil possui programa de comunicados e treinamentos para todos os colaboradores e partes interessadas apropriadas.

Incidentes de Segurança da Informação

A detecção e a defesa contra eventos de segurança exigem uma abordagem eficaz e consistente. Para este propósito, as responsabilidades e procedimentos para lidar com eventos de segurança da informação são especificados para garantir uma reação imediata a esses eventos. Canais de denúncia adequados e a sensibilização de todos os colaboradores são elementos essenciais destes procedimentos.

É criada uma política para relatar eventos ou vulnerabilidades de segurança da informação, incluindo pelo menos os seguintes requisitos:

- Reação a eventos de segurança da informação de acordo com níveis definidos de criticidade
- Formulário de denúncia, canal de denúncia, organização de processamento.
- Especificações para procedimento de feedback
- Indicação de medidas técnicas e organizacionais (como medidas disciplinares)
- Rastreamento e armazenamento de evidências

Desenvolvimento Seguro

O desenvolvimento seguro é um requisito para construir serviço, arquitetura, software e sistema seguros na ARaymond Brasil. Para isso, devem ser considerados minimamente aspectos:

- separação dos ambientes de desenvolvimento, teste e produção;
- segurança no ciclo de vida do desenvolvimento de software:
- requisitos de segurança na fase de especificação e design;
- pontos de verificação de segurança em projetos;
- repositórios seguros para código-fonte e configuração;
- segurança no controle de versão;
- conhecimento e treinamento necessários de segurança de aplicações;
- capacidade dos desenvolvedores para prevenir, encontrar e corrigir vulnerabilidade.

Para os testes de sistemas, selecionar, proteger e gerenciar as informações, considerando:

- não copiar informações sensíveis nos ambientes de desenvolvimento e teste do sistema, a menos que sejam fornecidos controles equivalentes para os sistemas de desenvolvimento e teste;
- proteger informações sensíveis por remoção ou mascaramento, se usadas para testes

Segurança nas comunicações

Todas as comunicações entre os ambientes tecnológicos ARaymond Brasil e as partes interessadas pertinentes devem utilizar canais de comunicações criptografados, utilizando cifras e algoritmos reconhecidamente seguros.

Cópias de Segurança

Cópias de informações, configuração de softwares e sistemas devem ser mantidas e testadas regularmente de acordo com as políticas específicas sobre backup, permitindo a recuperação de dados ou sistemas, se necessário. Para prevenir o vazamento de dados, devem ser usadas medidas como criptografia, controle de acesso e proteção física da mídia de armazenamento, quando aplicável.

Disposições Finais

Qualquer necessidade de ação em desacordo com as regras estabelecidas na Política de Segurança da Informação e suas políticas complementares devem ser direcionadas à Segurança da Informação Local Brasil para análise do risco, seu registro, e envio para a apreciação pela alçada competente.

O colaborador que fizer uso indevido ou não autorizado dos recursos das empresas, violar controle de segurança, ou de qualquer modo agir em desacordo com os termos dessa política, fica sujeito à aplicação de medidas disciplinares legalmente previstas, podendo haver responsabilização penal, civil e/ou administrativa, na forma da legislação em vigor.