P020- Política de Segurança da Informação e Segurança Cibernética

Sumário

1 Objetivo 2
2 Abrangência 2
3 Definições 2
4 Diretrizes 2
5 Responsabilidades 3
5.7 Todos os Colaboradores e Terceirizados 3
6 Gestão da Segurança da Informação 3
7 Propriedades básicas da Segurança da Informação 4
8 Mecanismos de Segurança da Informação 4
9 Segurança Cibernética 5
9.1 Definição 5
9.2 Elementos da Segurança Cibernética: 5
9.3 Procedimentos e Controles: 5
9.4 Plano de Respostas a Incidentes: 5
10 LGPD – Lei Geral de Proteção de Dados Pessoais 5
11 Processamento e Armazenamento de Dados 6
12 Testes Periódicos de Segurança 6
13 Requisitos 6
14 Exceções 6
15 Glossário 6

1 Objetivo

Esta Política tem por objetivo estabelecer diretrizes e responsabilidades para o gerenciamento da segurança da informação, de acordo com a sensibilidade dos dados e das informações sob responsabilidade do Banco PACCAR. Esta Política possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida (integridade) e permitir que a informação esteja disponível quando for necessário (disponibilidade).

2 Abrangência

Destinam-se a todas as áreas internas do Banco PACCAR e respectivos colaboradores, bem como às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

3 Definições

O Banco PACCAR deve divulgar ao público resumo contendo as linhas gerais da Política de Segurança da Informação.

A Segurança da Informação não está restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspectos de proteção relacionada à tecnologia, procedimentos e pessoas.

4 Diretrizes

As diretrizes desta Política foram estabelecidas pela Diretoria e compreendem as seguintes definições:

- O comprometimento com a melhoria contínua dos procedimentos relacionados com a Segurança da Informação;
- As informações do Banco PACCAR, seus colaboradores, seus clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;
- Toda informação deve ser classificada conforme o nível de risco que ela representa, bem como, o nível de confidencialidade que ela requer;
- O acesso às informações e recursos só deve ser feito, se devidamente autorizado;
- A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;
- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;
- Os riscos às informações do Banco PACCAR devem ser reportados à área de Compliance; e

- As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes.

5 Responsabilidades

A governança da Segurança da Informação é exercida pela Diretoria do Banco PACCAR, com a supervisão do Comitê de Governança, Riscos e Compliance, observando-se as responsabilidades e atribuições apresentadas abaixo:

5.7 Todos os Colaboradores e Terceirizados

- Cumprir fielmente a Política, as normas e os procedimentos de Segurança da Informação do Banco PACCAR;
- Realizar os treinamentos obrigatórios;
- Proteger as informações contra acessos, modificações, destruição ou divulgação não autorizada pelo Banco PACCAR;
- Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Banco PACCAR;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais, etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais; e
- Comunicar imediatamente à área de Compliance sobre qualquer descumprimento ou violação desta Política e/ou normas ou procedimentos, bem como reportar quaisquer incidentes relacionados à Segurança da Informação.

6 Gestão da Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, o Banco PACCAR adota os seguintes procedimentos:

- Gestão de Ativos da Informação: os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, e ter documentação e planos de manutenção atualizados;
- Classificação da Informação: as informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações;
- Gestão de Acessos: as concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos do Banco PACCAR. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, para que seja responsabilizado por suas ações;
- Gestão de Riscos: os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação do Banco PACCAR, para que sejam recomendadas as

proteções adequadas. Os cenários de riscos de Segurança da Informação são escalonados nos fóruns apropriados, para decisão;

- Tratamento de Incidentes de Segurança da Informação: os incidentes de Segurança da Informação do Banco PACCAR devem ser reportados à área de Compliance;
- Conscientização em Segurança da Informação: o Banco PACCAR promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação;
- A disciplina do uso da Internet de acordo com os princípios estabelecidos pela regulamentação em vigor;
- O acesso à Internet, assegurando aos seus usuários/clientes direitos e garantias estabelecidas de acordo com a regulamentação em vigor; e
- As iniciativas para compartilhamento imediato de informações, sobre qualquer tentativa de ataque, problema ou risco detectado, desde que relevante, com as demais instituições financeiras.

7 Propriedades básicas da Segurança da Informação

As seguintes propriedades devem ser observadas na gestão da Segurança da Informação:

- Confidencialidade - propriedade que limita o acesso à informação tão somente aos usuários considerados legítimos, ou seja, àqueles autorizados pelo proprietário da informação;
- Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida;
- Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
- Autenticidade - propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;
- Irretratabilidade ou não repúdio - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita; e
- Conformidade - propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

8 Mecanismos de Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, o Banco PACCAR adota os seguintes mecanismos:

- Controles físicos - são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta. Exemplos de mecanismos de segurança que apoiam os controles físicos: portas, trancas, paredes, blindagem, guardas entre outros; e
- Controles lógicos - são barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada. Exemplos de mecanismos de

segurança que apoiam os controles lógicos: autenticação, a criptografia, a prevenção e a detecção de intrusão, entre outros.

9 Segurança Cibernética

9.1 Definição

Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como Segurança de TI.

9.2 Elementos da Segurança Cibernética:

Elementos como segurança de aplicações e bancos de dados, gerenciamento de identidade, segurança para dispositivos móveis, times de exercícios de segurança, *Threat Hunting*, recuperação de desastres/planejamento de continuidade de negócios (relativos a TI), educação do usuário final, entre outros, são alguns exemplos aplicados em segurança cibernética.

9.3 Procedimentos e Controles:

Os procedimentos e os controles adotados para reduzir a vulnerabilidade do Banco PACCAR a incidentes e atender aos demais objetivos de segurança cibernética, encontram-se relacionados no item 13 Anexos, deste documento.

9.4 Plano de Respostas a Incidentes:

O Plano de Resposta a Incidentes considera o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do Banco PACCAR.

Este Plano abrange também os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais do Banco PACCAR.

Além disso, são elaborados cenários de incidentes considerados nos testes de continuidade de negócios. Além disso, será requerida a classificação dos dados e as informações quanto à relevância, conforme critérios estabelecidos no item 6 Gestão da Segurança da Informação desta Política. Adicionalmente, deverão ser definidos os parâmetros a serem utilizados na avaliação da relevância dos incidentes.

O Banco PACCAR deverá elaborar relatório anual sobre a implementação do Plano de Ação e de Resposta a Incidentes, com data base de 31 de dezembro.

10 LGPD – Lei Geral de Proteção de Dados Pessoais

O Banco PACCAR adota e segue as diretrizes e definições contidas no documento "Política de Segurança e Proteção de Dados Pessoais" elaborada para todas as empresas do Grupo PACCAR no Brasil.

Este documento é parte integrante desta política e deve ser lida em conjunto com ela.

11 Processamento e Armazenamento de Dados

O Banco PACCAR tem critérios definidos para contratação de serviços relevantes de processamento e armazenamento de dados, que estão descritos na seção dedicada ao Risco Operacional no Manual de Gestão Integrada de Riscos e incluem a identificação e segregação de dados dos clientes, além de garantia de confidencialidade, integridade, disponibilidade e recuperação de dados e informações processadas ou armazenadas.

A área compartilhada de TI da DAF é responsável pela prestação de serviços de processamento e armazenamento de dados e conta com um servidor próprio de propriedade do Banco PACCAR com redundância no servidor da DAF, cujo controle é feito através de mecanismos lógicos e físicos.

Sem prejuízo do dever de sigilo e livre concorrência, o Banco PACCAR mantém disponível e compartilha com o Banco Central os incidentes relevantes registrados e analisados incluindo aqueles ocorridos na estrutura terceirizada da DAF.

12 Testes Periódicos de Segurança

De acordo com a regulamentação vigente, o Banco PACCAR prevê a existência de testes periódicos de segurança para os sistemas de informações, sejam eles físicos, cujos testes estão previstos no Manual de Gestão de Documentos, ou especialmente para os mantidos em meio eletrônico, cujos testes estão previstos no Manual de Tecnologia da Informação.

Os testes estão descritos no Plano de Testes para Sistemas de Informação.

13 Requisitos

A Política de Segurança da Informação deve ser utilizada em conjunto com as diretrizes estabelecidas pelo Código de Conduta Ética do Banco PACCAR, além da Política de Gerenciamento de Riscos Operacionais, o Manual de Tecnologia da Informação, o Manual de Gestão Integrada de Riscos, o Manual de Gestão de Documentos, o Plano de Testes para Sistemas de Informação e o Plano de Resposta a Incidentes.

Esta Política segue, além das regulamentações vigentes, as regras de conduta e diretrizes globais do Grupo PACCAR.

14 Exceções

Assuntos contraditórios e/ou não contemplados nesta Política deverão ser endereçados, discutidos e aprovados pelo Diretor responsável e/ou Comitê de Governança, Riscos e Compliance, se necessário.

15 Glossário

- Criptografia: permite a transformação reversível da informação de forma a torná-la ininteligível a terceiros;
- *Threat Hunting:* é um processo de pesquisa proativa e frequente pelas redes para detectar e isolar ameaças avançadas que escapam às soluções de segurança existentes; e
- Propriedade intelectual: tecnologias, marcas, metodologias e quaisquer informações que pertençam à Instituição não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.