Política de Segurança da Informação

Histórico de Alterações

Número da Versão	Data da Alteração	Resumo das Alterações	Autor
1.0	07/12/2017	Documento original	Vortex Security

Sumário

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

1. INTRODUÇÃO

A informação é um ativo que possui grande valor para a Elitravel, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas, normas e procedimentos que visem garantir a segurança da informação deve ser prioridade constante da empresa, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da organização.

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo, etc.

A Política de Segurança da Informação da Elitravel é uma declaração formal da organização acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores e prestadores de serviços.

Este documento de política engloba todos os aspectos da segurança em torno da informação confidencial da organização e deve ser distribuído a todos os colaboradores (funcionários, estagiários e prestadores de serviços), que devem ler este documento na íntegra e assinar o formulário confirmando que leram e entendem esta política completamente. Este documento será revisado e atualizado anualmente pela Alta Direção ou quando relevante para incluir padrões de segurança desenvolvidos recentemente na política ou se ocorrerem mudanças significativas no ambiente.

2. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Estabelecer diretrizes que permitam aos colaboradores da Elitravel seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da organização e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da Elitravel quanto à:

- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

3. USO ACEITÁVEL DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

As intenções da Elitravel de definir um uso aceitável da Política de Segurança da Informação não são para impor restrições que sejam contrárias à sua cultura de estabelecimento de relações de confiança, mas sim para proteger todos os colaboradores de ações ilegais ou prejudiciais aos negócios da organização. Dessa maneira, entende-se que:

- Os colaboradores são responsáveis por exercer um bom julgamento quanto à razoabilidade do uso pessoal;
- Os colaboradores devem garantir que tenham credenciais apropriadas e sejam autenticados para o uso de tecnologias;
- Os colaboradores devem tomar todas as medidas necessárias para impedir o acesso não autorizado a dados confidenciais que incluem dados do titular do cartão;
- Os colaboradores devem garantir que as tecnologias sejam usadas e configuradas em locais de rede aceitáveis e apropriados;
- Os colaboradores são responsáveis pela segurança de suas senhas e contas;
- Todas os servidores, PCs, notebooks e estações de trabalho devem ser protegidos com bloqueio de tela automático protegido por login e senha;
- Todos os dispositivos de entrada de POS e PIN devem ser adequadamente protegidos para que não possam ser adulterados;
- As postagens de colaboradores de um endereço de e-mail da organização para grupos de notícias devem conter uma declaração de responsabilidade que indique que as opiniões expressas são próprias e não necessariamente da Elitravel, a menos que a publicação esteja no decorrer de tarefas da organização;
- Os colaboradores devem ter extremo cuidado ao abrir anexos de e-mail recebidos de remetentes desconhecidos, que podem conter vírus, malwares, campanhas de phishing, etc.

4. ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO

4.1 DEFINIÇÃO

A estrutura normativa da Segurança da Informação da Elitravel é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

- Política de Segurança da Informação (Política): constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- Normas de Segurança da Informação (Normas): estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
- Procedimentos de Segurança da Informação (Procedimentos): instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da Elitravel.

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

4.2 DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política e as Normas de Segurança da Informação devem ser divulgadas a todos os colaboradores da Elitravel e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Os Procedimentos de Segurança da Informação devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

4.3 APROVAÇÃO E REVISÃO

Os documentos integrantes da estrutura normativa da Segurança da Informação da Elitravel deverão ser aprovados e revisados conforme os seguintes critérios:

(i) **Política:**
- Nível de Aprovação: Alta Direção.
- Periodicidade de Revisão: anual.

(ii) **Normas:**
- Nível de Aprovação: Alta Direção.
- Periodicidade de Revisão: anual.

(iii) **Procedimentos:**
- Nível de Aprovação: Gestor responsável pela área envolvida.
- Periodicidade de Revisão: anual.

5. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Cabe a todos os colaboradores e prestadores de serviços da Elitravel:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da Elitravel;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela Elitravel;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Elitravel;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente à Alta Direção qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

Adicionalmente, são definidas as seguintes responsabilidades e atribuições específicas relacionadas à segurança da informação:

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

5.1 ALTA DIREÇÃO

Em relação à segurança da informação, cabe à Alta Direção:

- Aprovar a Política de Segurança da Informação e suas revisões;
- Apoiar formalmente a importância e o cumprimento da Política e das normas e procedimentos relacionados;
- Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas de Segurança da Informação;
- Propor ajustes, aprimoramentos e modificações desta Política;
- Propor melhorias e aprovar as Normas de Segurança da Informação;
- Definir a classificação das informações pertencentes ou sob a guarda da Elitravel, com base no inventário de informações e nos critérios de classificação constantes de Norma específica;
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação;
- Propor projetos e iniciativas relacionados à melhoria da segurança da informação da Elitravel;
- Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
- Determinar a elaboração de relatórios, levantamentos e análises que dêem suporte à gestão de segurança da informação e à tomada de decisão;
- Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação; e
- Propor a relação de “proprietários” das informações da Elitravel.

5.2 PROPRIETÁRIO DA INFORMAÇÃO

O proprietário da informação é um diretor ou um gerente da Elitravel, formalmente indicado pela Alta Direção, responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes à organização ou sob a sua guarda.

Cabe ao proprietário da informação:

- Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções da Elitravel às autorizações de acesso concedidas;
- Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz de cargos e funções, a Política e as Normas de Segurança da Informação da Elitravel;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;
- Analisar os relatórios de controle de acesso fornecidos pela Alta Direção, com o objetivo de identificar desvios em relação à Política e às Normas de Segurança da Informação, tomando as ações corretivas necessárias;
- Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões da Alta Direção, prestando os esclarecimentos solicitados sobre as informações sobre sua responsabilidade.

6. DIRETRIZES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da Elitravel poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador manter-se atualizado em relação a esta Política de Segurança da Informação e aos procedimentos e normas relacionadas, buscando orientação do seu gestor imediato sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

6.1 REQUISITOS GERAIS

- Para a uniformidade da informação, a Política de Segurança da Informação deverá ser comunicada a todos os colaboradores da Elitravel a fim de que seja cumprida dentro e fora da empresa;
- Tanto a Política de Segurança da Informação quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da Alta Direção;
- Deverá constar em todos os contratos da Elitravel o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição;
- A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores;
- Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade;
- Todo incidente que afete a segurança da informação deverá ser comunicado à Alta Direção para análise;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação;
- Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução;
- Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a organização julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela Elitravel ou por terceiros;
- Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação;
- A Elitravel exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis;
- Esta Política de Segurança da Informação será implementada na Elitravel por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

6.2 ADOÇÃO DE COMPORTAMENTO SEGURO

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os colaboradores. Portanto, é fundamental para a proteção e salvaguarda das informações que os colaboradores adotem comportamento seguro e consistente com o objetivo de proteção das informações da organização, com destaque para os seguintes itens:

- Colaboradores devem assumir atitude pró-ativa e engajada no que diz respeito à proteção das informações da Elitravel;
- Os colaboradores da Elitravel devem compreender as ameaças externas que podem afetar a segurança das informações da organização, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação;
- Todo tipo de acesso à informação da Elitravel que não for explicitamente autorizado é proibido;
- Informações confidenciais da Elitravel não podem ser transportadas em qualquer meio (CD, DVD, pen-drive, papel etc.) sem as devidas autorizações e proteções;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.);
- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a colaboradores da própria organização), anotadas em papel ou em sistema visível ou de acesso não-protegido;
- Somente softwares homologados pela Elitravel podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de serviços de informática da organização;
- A política para uso de internet e correio eletrônico deve ser rigorosamente seguida. Arquivos de origem desconhecida nunca devem ser abertos e/ou executados;
- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos;
- Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com a Alta Direção.

6.3 PROTEÇÃO DE DADOS SENSÍVEIS

- Todos os dados sensíveis do titular do cartão armazenados e manuseados pela Elitravel e seus colaboradores devem estar protegidos de forma segura contra uso não autorizado em todos os momentos;
- Todos os dados sensíveis de cartões de crédito, que a Elitravel não exige para fins comerciais, devem ser descartados de forma segura e irrecuperável;
- Se não houver necessidade específica de visualização do PAN completo (número de conta permanente), ele deve ser mascarado quando exibido;
- Os PAN'S que não estão protegidos, conforme indicado acima, não devem ser enviados para a rede externa através de tecnologias de mensagens de usuários finais, como chats, instant messenger, etc.

É estritamente proibido armazenar:

- O conteúdo da faixa magnética do cartão de pagamento (dados da trilha) em qualquer mídia;
- O CVV / CVC (o número de 3 ou 4 dígitos no painel de assinatura no reverso do cartão de pagamento) em qualquer mídia;
- O PIN ou o bloco de PIN criptografado sob qualquer circunstância.

6.4 CLASSIFICAÇÃO DA INFORMAÇÃO

Os dados e mídias contendo informações devem sempre ser rotulados para indicar o nível de sensibilidade, conforme segue:

- **Confidenciais**: dados que podem incluir ativos de informações para os quais existem requisitos legais para prevenir a divulgação ou penalidades financeiras por divulgação,

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

ou dados que causariam danos graves à Elitravel se divulgados ou modificados. Os dados confidenciais incluem os dados do titular do cartão.

- **Internos**: dados que podem incluir informações que o proprietário dos dados entende que devem ser protegidas para impedir a divulgação não autorizada;
- **Públicos**: são informações que podem ser disseminadas livremente.

6.5 ACESSO AOS DADOS SENSÍVEIS DO TITULAR DO CARTÃO

Todo o acesso aos dados sensíveis do titular do cartão deve ser controlado e autorizado. Todas as funções de trabalho que exigem acesso aos dados do titular do cartão devem estar claramente definidas.

- Qualquer exibição do suporte do cartão deve ser restrita no mínimo dos primeiros 6 e os últimos 4 dígitos dos dados do titular do cartão;
- Os direitos de acesso a IDs de usuários privilegiados devem ser restritos a menos privilégios necessários para desempenhar responsabilidades de trabalho;
- Os privilégios devem ser atribuídos a indivíduos com base na classificação e função do trabalho (controle de acesso baseado em função);
- O acesso a informações sensíveis do titular do cartão, como PAN, informações pessoais e dados comerciais, é restrito a colaboradores que tenham uma necessidade legítima de visualizar essas informações;
- Nenhum outro colaborador deve ter acesso a esses dados confidenciais, a menos que eles tenham uma necessidade comercial genuína;
- Se os dados do titular do cartão forem compartilhados com um provedor de serviços (terceiro), uma lista desses fornecedores de serviços deverá ser mantida;
- A Elitravel assegurará um acordo por escrito que inclua um reconhecimento de que o provedor de serviços será responsável pelos dados do titular do cartão a que tiver acesso;
- A Elitravel assegurará que haja um processo estabelecido, incluindo a devida diligência adequada, antes de se envolver com um provedor de serviços;
- A Elitravel terá um processo no local para monitorar o status de conformidade PCI DSS do provedor de serviços.

6.6 SEGURANÇA FÍSICA

O acesso a informações confidenciais deve ser fisicamente restringido para impedir que pessoas não autorizadas obtenham esse dados.

- Os colaboradores são responsáveis por exercer um bom julgamento quanto à razoabilidade do uso pessoal;
- Os colaboradores devem garantir que tenham credenciais apropriadas e sejam autenticados pelo uso de tecnologias;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Os colaboradores devem tomar todas as medidas necessárias para impedir o acesso não autorizado a dados confidenciais que incluem dados do titular do cartão;
- Os colaboradores devem garantir que as tecnologias sejam usadas e configuradas em locais de rede aceitáveis e apropriados;
- Uma lista de dispositivos que aceitam dados do cartão de pagamento deve ser mantida;
- A lista deve incluir marca, modelo e localização do dispositivo;
- A lista deve ter o número de série ou um identificador exclusivo do dispositivo;
- A lista deve ser atualizada quando os dispositivos são adicionados, removidos ou realocados;
- As superfícies dos dispositivos POS devem ser periodicamente inspecionadas para detectar adulteração ou substituição;
- O pessoal que usa os dispositivos deve ser treinado e conscientizado para lidar com os dispositivos POS;
- O pessoal que usa os dispositivos deve verificar a identidade de terceiros que reivindiquem reparar ou executar tarefas de manutenção nos dispositivos, instalar novos dispositivos ou substituir dispositivos;
- O pessoal que usa os dispositivos deve ser treinado para reportar comportamentos suspeitos e indícios de adulteração dos dispositivos à equipe responsável;
- Mantenha as senhas seguras e não compartilhe contas. Os usuários autorizados são responsáveis pela segurança de suas senhas e contas;
- A mídia é definida como qualquer papel impresso ou manuscrito, faxes recebidos, fitas de backup, disco rígido do computador, etc;
- Os meios que contêm informações sensíveis do titular do cartão devem ser tratados e distribuídos de forma segura por indivíduos confiáveis;
- Procedimentos devem estar em vigor para ajudar todo o pessoal a distinguir facilmente entre colaboradores e visitantes, especialmente em áreas onde os dados do titular do cartão estão acessíveis;
- "Colaborador" refere-se a colaboradores em tempo integral e a tempo parcial, colaboradores temporários, e consultores que são "alocados" nos sites da organização. Um "visitante" é definido como um vendedor, convidado de um colaborador, prestador de serviço ou qualquer pessoa que precise entrar nas instalações por uma curta duração, geralmente não mais de um dia;
- Os visitantes devem sempre ser acompanhados por um colaborador confiável quando em áreas que possuem informações sensíveis do titular do cartão;
- Os conectores de rede localizados em público e em áreas acessíveis aos visitantes devem ser desativados e habilitados quando o acesso à rede é explicitamente autorizado;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Todos os dispositivos de entrada de POS e PIN devem ser adequadamente protegidos e protegidos para que não possam ser adulterados ou alterados;
- Controle estrito deve mantido sobre a distribuição externa ou interna de qualquer mídia contendo dados do titular do cartão e deve ser aprovado pela Alta Direção.

6.7 PROTEÇÃO DE DADOS EM TRÂNSITO

Todos os dados sensíveis do titular do cartão devem ser protegidos de forma segura se ele deve ser transportado fisicamente ou eletronicamente.

- Os dados do titular do cartão nunca devem ser enviados pela internet por e-mail, bate-papo instantâneo ou qualquer outra tecnologia de usuário final;
- Se houver uma justificativa de negócios para enviar dados do titular do cartão via e-mail ou via internet ou qualquer outro modo, então deve ser feito após a autorização da Alta Direção e usando um mecanismo de criptografia forte (ou seja, criptografia AES, criptografia PGP, SSL, TLS, IPSEC, GSM, GPRS, tecnologias sem fio etc.);
- O transporte de mídia que contenha dados sensíveis do titular do cartão para outro local deve ser autorizado pela Alta Direção, logado e inventariado antes de sair das instalações. Apenas serviços de correio seguro podem ser usados para o transporte de tais mídias. O status da remessa deve ser monitorado até que seja entregue à sua nova localização.

6.8 DESCARTE DE DADOS ARMAZENADOS

- Todos os dados devem ser descartados de forma segura quando não for mais exigido pela Elitravel, independentemente da mídia ou do tipo de aplicativo no qual ele está armazenado;
- Um processo automático deve existir para excluir permanentemente dados on-line, quando não for mais necessário;
- Todas as cópias impressas dos dados do titular do cartão devem ser destruídas manualmente quando não são mais necessárias para razões comerciais válidas e justificadas. Um processo trimestral deve ser executado para confirmar que todos os dados de um titular de cartão foram apropriadamente descartados em tempo hábil;
- A Elitravel terá procedimentos para a destruição de materiais impressos em papel. Isso exigirá que todos os materiais impressos sejam cortados transversalmente ou incinerados para que não possam ser reconstruídos;
- A Elitravel terá procedimentos documentados para a destruição de mídia eletrônica, onde estes exigirão que todos os dados do titular do cartão em mídia eletrônica devem ser tornados irrecuperáveis quando excluídos, seja através de desmagnetização ou limpeza eletrônica usando processos de eliminação segura ou a destruição física da mídia;
- Todas as informações do titular do cartão que aguardam destruição devem ser mantidas em recipientes de armazenamento bloqueáveis, claramente marcados como "para descarte" - o acesso a esses recipientes deve ser restrito.

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

6.9 CONSCIENTIZAÇÃO DE PROCEDIMENTOS DE SEGURANÇA

As políticas e os procedimentos descritos abaixo devem ser incorporados na prática da organização para manter um alto nível de conscientização de segurança:

- Revise os procedimentos de tratamento de informações confidenciais e mantenha reuniões periódicas de conscientização de segurança para incorporar esses procedimentos na prática diária da organização;
- Distribua este documento de política de segurança para todos os colaboradores da organização. É necessário que todos confirmem que entendem o conteúdo deste documento de política de segurança assinando um formulário de confirmação;
- Todos os colaboradores que manipulam informações confidenciais serão submetidos a verificações de antecedentes (como verificações de registros criminais e de crédito, dentro dos limites da lei local) antes de começarem suas atividades na organização;
- Todos os prestadores de serviços com acesso a números de conta de cartão de crédito estão obrigados contratualmente a cumprir as normas de segurança da associação de cartão (PCI / DSS);
- As políticas de segurança da organização devem ser revistas anualmente e atualizadas, conforme necessário.

6.10 SEGURANÇA DE REDES

- Os firewalls devem ser implementados em cada conexão à internet, qualquer zona desmilitarizada (DMZ) e a rede interna da organização;
- Um diagrama de rede detalhando todas as conexões de entrada e saída deve ser mantido e revisado a cada 6 meses;
- Um documento de configuração de firewall e roteador deve ser mantido, que inclui uma lista documentada de serviços, protocolos e portas, incluindo uma justificativa de negócios;
- As configurações de firewall e roteador devem restringir as conexões entre redes não confiáveis e quaisquer sistemas no ambiente de dados do titular do cartão;
- Os firewalls devem ser implementados para proteger os segmentos de redes locais e os recursos de TI que se conectam a esses segmentos, como a rede comercial e a rede aberta;
- Todo o tráfego de entrada e de saída deve ser restrito ao que é necessário para o ambiente de tratamento de dados do titular do cartão;
- Todo o tráfego de rede de entrada é bloqueado por padrão, a menos que seja explicitamente permitido e as restrições devem ser documentadas;
- Todo o tráfego de saída deve ser autorizado pelo gerenciamento (ou seja, qual é a categoria de sites que pode ser visitada pelos colaboradores) e as restrições devem ser documentadas;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- A organização terá firewalls entre qualquer rede sem fio e o ambiente de dados do titular do cartão;
- Uma topologia do ambiente de firewall deve ser documentada e deve ser atualizada de acordo com as mudanças na rede;
- As regras de firewall serão revistas a cada seis meses;
- Não serão permitidas conexões diretas da Internet para o ambiente de dados do titular do cartão. Todo o tráfego deve passar por um firewall.

6.11 ANTIVÍRUS

- Todas as máquinas devem ser configuradas para executar o software antivírus, conforme aprovado pela organização. A aplicação deve ser configurada para baixar as atualizações mais recentes. O antivírus deve ter varredura periódica habilitada para todos os sistemas;
- O software antivírus em uso deve ser capaz de realizar a detecção de todos os tipos conhecidos de software malicioso (vírus, trojans, adware, spyware, worms e rootkits);
- Todas as mídias removíveis devem ser verificadas quanto a vírus antes de serem usadas;
- Todos os logs gerados a partir das soluções antivírus devem ser mantidos de acordo com os requisitos legais / regulatórios / contratuais;
- Instalações do software antivírus devem ser configuradas para atualizações automáticas e exames periódicos;
- Os usuários finais não devem ser capazes de modificar quaisquer configurações ou alterar o software antivírus;
- O e-mail com anexos provenientes de fontes suspeitas ou desconhecidas não deve ser aberto. Todos esses e-mails e seus anexos devem ser excluídos do sistema de correio, bem como do lixo. Ninguém deve encaminhar qualquer e-mail, que eles suspeitam que podem conter vírus.

6.12 GERENCIAMENTO DE PATCHES

- Todas as estações de trabalho, servidores, software, componentes do sistema, etc. de propriedade da organização devem ter patches atualizados de segurança instalados para proteger os recursos de vulnerabilidades conhecidas;
- Sempre que possível, todos os sistemas devem ter atualizações automáticas ativadas para os patches liberados de seus respectivos fornecedores. Os patches de segurança devem ser instalados no prazo máximo de um mês após a liberação do respectivo fornecedor e devem seguir o processo de gestão de mudanças;
- Qualquer exceção a este processo deve ser documentada.

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

6.13 ACESSO REMOTO

- É responsabilidade dos colaboradores com privilégios de acesso remoto para a rede corporativa da organização, garantir que sua conexão de acesso remoto tenha os mesmos requisitos de segurança exigidos quando da sua utilização pela rede local da organização;
- O acesso remoto seguro deve ser rigorosamente controlado;
- As contas de fornecedores com acesso à rede da organização só serão ativadas durante o período de tempo em que o acesso é necessário e serão desativados ou removidos assim que o acesso não for mais necessário;
- A conexão de acesso remoto será configurada para ser desconectada automaticamente após 30 minutos de inatividade;
- Todos os hosts conectados às redes internas da organização através de tecnologias de acesso remoto serão monitorados regularmente;
- Todas as contas de acesso remoto serão revisadas regularmente e revogadas se não houver mais justificativa para tal uso.

6.14 GESTÃO DE VULNERABILIDADES

- Todas as vulnerabilidades detectadas devem receber um ranking de risco, como Alto, Médio e Baixo, com base nas boas práticas recomendadas, como o score base CVSS;
- A Elitravel executará varreduras de vulnerabilidades de rede interna e externa pelo menos trimestralmente e após qualquer alteração significativa na rede (como novas instalações de componentes do sistema, mudanças na topologia de rede, modificações de regras de firewall, atualizações de produto, etc.);
- As varreduras de vulnerabilidades internas trimestrais devem ser realizadas pela Elitravel por equipe interna ou por um fornecedor capacitado e o processo de verificação deve incluir que as varreduras sejam feitas até que os resultados de aprovação sejam obtidos ou todas as vulnerabilidades definidas como altas sejam resolvidas;
- As varreduras de vulnerabilidades externas trimestrais devem ser realizadas por um ASV qualificado.

6.15 PADRÕES DE CONFIGURAÇÃO

Os sistemas de informação que processam transmissão ou os dados do suporte do cartão de armazenamento devem ser configurados de acordo com o padrão aplicável para essa classe de dispositivo ou sistema.

- Um padrão de configuração de sistemas deve ser desenvolvido com base nos padrões reconhecidos , tais como SANS, NIST, ISO, etc;
- As configurações de sistemas devem ser atualizadas à medida que novos problemas são identificados;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- As configurações de sistemas devem incluir configurações comuns de parâmetros de segurança;
- Todas as contas e senhas padrão do fornecedor para os sistemas devem ser alteradas no momento de provisionar o sistema / dispositivo na rede da Elitravel e todos os serviços desnecessários e as contas do usuário / sistema devem ser desabilitadas;
- Todas as contas padrão desnecessárias devem ser removidas ou desativadas antes de instalar um sistema na rede;
- As configurações de parâmetros de segurança devem ser configuradas adequadamente nos componentes do sistema;
- Todas as funcionalidades desnecessárias (scripts, drivers, recursos, subsistemas, sistemas de arquivos, servidores web etc.) devem ser removidas;
- Todos os serviços desnecessários, protocolos, daemons etc., devem ser desativados se não forem utilizados pelo sistema;
- Qualquer protocolo inseguro, daemons, serviços em uso devem ser documentados e justificados;
- Todos os usuários com acesso aos dados do titular do cartão devem ter uma ID exclusiva;
- Todo usuário deve usar uma senha para acessar a rede da organização ou qualquer outro recurso eletrônico;
- Todas as ID de usuário que tiveram seu uso encerrado devem ser desativadas ou removidas imediatamente.
- O ID do usuário será bloqueado se houver mais de 5 tentativas mal sucedidas. Essa conta bloqueada só pode ser ativada pelo administrador do sistema. As contas de usuário bloqueadas serão desativadas por um período mínimo de 30 minutos ou até que o administrador ative a conta;
- Todas as senhas do sistema e do nível de usuário devem ser alteradas pelo menos trimestralmente;
- Uma senha exclusiva deve ser configurada para novos usuários e os usuários solicitados a alterar a senha no primeiro login;
- O grupo, a conta de usuário compartilhada ou genérica ou a senha ou outros métodos de autenticação não devem ser usados para administrar quaisquer componentes do sistema;
- Todo o acesso administrativo não-console usará tecnologias apropriadas como ssh, vpn, ssl etc. antes da senha do administrador ser solicitada;
- Os serviços e parâmetros do sistema serão configurados para evitar o uso de tecnologias inseguras, como o telnet e outros comandos de login remoto inseguros;
- O acesso de administrador às interfaces de gerenciamento baseadas na web deve ser criptografado usando criptografia forte;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Todas as configurações de dispositivos de rede devem respeitar os padrões exigidos pela Elitravel antes de serem colocados na rede;
- Antes de ser implantado na produção, um sistema deve ser certificado para atender ao padrão de configuração aplicável;
- Todas as configurações de dispositivos de rede devem ser verificadas anualmente contra o gabarito de configuração para garantir que a configuração continue a atender aos padrões exigidos;
- Sempre que possível, um software de gerenciamento de configuração de rede será usado para automatizar o processo de confirmação da aderência à configuração da plataforma.

6.16 GESTÃO DE MUDANÇAS

- As mudanças nos recursos de informação devem ser gerenciadas e executadas de acordo com um processo formal de controle de mudanças. O processo de controle assegurará que as mudanças propostas sejam revisadas, autorizadas, testadas, implementadas e divulgadas de forma controlada; e que o status de cada mudança proposta seja monitorado;
- O processo de controle de mudanças deve ser formalmente definido e documentado. Um processo de controle de mudanças deve ser implementado para controlar mudanças em todos os recursos críticos de informações da organização (como hardware, software, documentação do sistema e procedimentos operacionais). Este processo documentado deve incluir responsabilidades e procedimentos de gerenciamento. Sempre que possível, os procedimentos de controle de mudanças operacionais e de aplicativos devem ser integrados;
- Todos os pedidos de mudança devem ser registrados, sejam aprovados ou rejeitados, em um sistema padronizado e central. A aprovação de todos os pedidos de mudança e seus resultados devem ser documentados. Uma trilha de auditoria, contendo informações relevantes, deve ser mantida em todos os momentos. Isso deve incluir documentação do pedido de mudança, alteração de autorização e o resultado da alteração. Nenhuma pessoa deve ser capaz de efetuar mudanças nos sistemas de informação de produção sem a aprovação de pessoal autorizado;
- Uma avaliação de risco deve ser realizada para todas as mudanças e dependendo do resultado, deve ser realizada uma avaliação de impacto;
- A avaliação de impacto deve incluir o efeito potencial sobre outros recursos de informação e possíveis implicações de custos. A avaliação de impacto deve, quando aplicável, considerar a conformidade com os requisitos e padrões legislativos;
- Todos os pedidos de mudança devem ser priorizados em termos de benefícios, urgência, esforço exigido e impacto potencial nas operações;
- As mudanças devem ser testadas em um ambiente isolado, controlado e representativo (onde esse ambiente é viável) antes da implementação para minimizar

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

o efeito sobre o processo comercial relevante, avaliar o impacto sobre as operações e a segurança e verificar que apenas foram feitas alterações aprovadas;

- Qualquer mudança de software e / ou atualização deve ser controlada com controle de versão. As versões antigas devem ser mantidas de acordo com as políticas de gerenciamento de armazenamento e armazenamento corporativo;
- Todas as alterações devem ser aprovadas antes da implementação. A aprovação das mudanças deve basear-se em critérios de aceitação formal, ou seja, o pedido de alteração foi feito por um usuário autorizado, a avaliação de impacto foi realizada e as alterações propostas foram testadas;
- Todos os usuários, afetados de forma significativa por uma alteração, devem ser notificados da alteração. O representante do usuário deve assinar a mudança. Os usuários devem ser obrigados a fazer envios e comentários antes da aceitação da alteração;
- A implementação só será realizada após testes e aprovação apropriados pelas partes interessadas. Todas as principais mudanças devem ser tratadas como uma nova implementação do sistema e devem ser estabelecidas como um projeto. As principais mudanças serão classificadas de acordo com o esforço necessário para desenvolver e implementar as referidas mudanças;
- Procedimentos para abortar e recuperar de mudanças infrutíferas devem ser documentados. Se o resultado de uma alteração for diferente do resultado esperado (conforme identificado no teste da alteração), os procedimentos e as responsabilidades devem ser observados para a recuperação e continuidade das áreas afetadas. Os procedimentos de rollback serão estabelecidos para garantir que os sistemas possam voltar ao que eram antes da implementação das mudanças;
- A documentação dos recursos de informação deve ser atualizada após a conclusão de cada alteração e a documentação antiga deve ser arquivada ou descartada de acordo com as políticas de documentação e retenção de dados;
- Procedimentos específicos para assegurar o bom controle, autorização e documentação de mudanças de emergência devem estar em vigor. Parâmetros específicos serão definidos como um padrão para classificar mudanças, como mudanças de emergência;
- Todas as alterações serão monitoradas uma vez que tenham sido implementadas para o ambiente de produção. Os desvios das especificações de projeto e os resultados dos testes serão documentados e escalados para o proprietário da solução para ratificação.

6.17 AUDITORIA E ANÁLISE DE LOGS

Este procedimento abrange todos os logs gerados para sistemas dentro do ambiente de dados do titular do cartão, com base no fluxo de dados do titular do cartão na rede da organização, incluindo os seguintes componentes:

- Registros do sistema operacional;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Registros de auditoria de banco de dados;
- Firewalls & Network Logs;
- Antivírus Logs;
- Registros de sistema de monitoramento de integridade de arquivos;
- Os logs de auditoria devem ser mantidos por um mínimo de 3 meses on-line (disponível para análise imediata) e 12 meses de backup;
- A revisão dos logs deve ser realizada por meio do sistema de monitoramento de rede da Elitravel;
- Os seguintes eventos do sistema operacional são configurados para registro e são monitorados pelo console:
    - Qualquer adição, modificação ou exclusão de contas de usuário;
    - Qualquer tentativa fracassada ou não autorizada no logon do usuário;
    - Qualquer modificação nos arquivos do sistema;
    - Qualquer acesso ao servidor, ou aplicativo em execução no servidor, incluindo arquivos que detêm dados do titular do cartão;
    - Ações tomadas por qualquer pessoa com privilégios root ou administrativos;
    - Qualquer usuário acesso a trilhas de auditoria;
    - Qualquer criação / exclusão de objetos no nível do sistema instalados pelo sistema operacional.
- Os seguintes eventos de firewall são configurados para registro e são monitorados pelo sistema de monitoramento de rede:
    - Violações ACL;
    - Invasões de autenticação de usuário inválidas;
    - Logon e ações tomadas por qualquer pessoa usando contas privilegiadas;
    - Mudanças de configuração feitas no firewall (por exemplo, políticas desativadas, adicionadas, excluídas ou modificadas);
    - Tentativas de autenticação de usuário inválidas;
    - Logon e ações tomadas por qualquer indivíduo usando contas privilegiadas;
    - Mudanças de configuração feitas no dispositivo (por exemplo, configuração desabilitada, adicionada, excluída ou modificada).
- Os seguintes eventos de detecção de invasão devem ser configurados para registro e são monitorados pelo sistema de monitoramento de:
    - Qualquer vulnerabilidade listada no banco de dados Common Vulnerability Entry (CVE);
    - Qualquer ataque genérico não listado no CVE;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Qualquer ataque conhecido de negação de serviço;
- Todos os padrões de tráfego que indicaram o reconhecimento de uma tentativa de ataque;
- Qualquer tentativa de explorar erros de configuração relacionados à segurança;
- Qualquer falha de autenticação que possa indicar um ataque;
- Qualquer tráfego para ou de um programa de backdoor;
- Qualquer tráfego típico de ataques secretos conhecidos.

o Os seguintes eventos de integridade de arquivos devem ser configurados para registro e monitorado:

- Qualquer modificação nos arquivos do sistema;
- Ações tomadas por qualquer pessoa com privilégios administrativos;
- Qualquer usuário que acessar trilhas de auditoria;
- Qualquer criação / exclusão de objetos no nível do sistema instalados pelo sistema operacional.

6.18 DESENVOLVIMENTO SEGURO DE APLICAÇÕES

o A política de desenvolvimento seguro de aplicações é um plano de ação para orientar as decisões e ações dos desenvolvedores durante o ciclo de vida do desenvolvimento de software (SDLC) para garantir a segurança do software. Esta política visa ser independente de linguagem e plataforma para que seja aplicável em todos os projetos de desenvolvimento de software;

o A aderência e o uso da política de codificação de desenvolvimento seguro de aplicativos é um requisito para todo o desenvolvimento de software nos sistemas de tecnologia da informação de prestadores de serviços que processam os dados da organização;

o Cada fase do SDLC é mapeada com atividades de segurança, conforme explicado abaixo:

- Design
  - Identificar os requisitos de design sob a perspectiva de segurança;
  - Arquitetura e design review;
  - Modelagem de ameaças.
- Codificação
  - Melhores práticas de codificação de Melhores Práticas;
  - Análise de performance.
- Teste

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

        - Análise de Vulnerabilidade.
    - Implantação
        - Revisão de configurações do servidor;
        - Revisão de configurações de rede.
- O desenvolvimento do código deve ser verificado e validado com as versões mais atualizadas dos Padrões de Codificação da organização para o Desenvolvimento Seguro de Aplicações. Todos os desenvolvedores de código devem verificar se seu código está em conformidade com as normas e diretrizes de codificação mais recentes e aprovadas;
- Somente o código validado deve ser implementado no ambiente de produção da organização. Uma revisão e validação garante que o código exiba propriedades de segurança fundamentais para incluir correção, previsibilidade e tolerância de ataque;
- Desenvolvedores de código devem:
    - Certificar-se de que o código atende ao nível de confiança e que o software está livre de vulnerabilidades exploráveis;
    - Certificar-se de que o código fornece uma execução previsível ou uma confiança justificável e que o software, quando executado, fornecerá a funcionalidade de segurança conforme o previsto;
    - Devem levar em consideração as técnicas de codificação e as vulberabilidades listadas no OWASP TOP 10;
    - Nunca confiar em dados recebidos no sistema, aplicar verificações a esses dados;
    - Nunca confiar no cliente para armazenar dados confidenciais, independentemente da trivialidade;
    - Desativar mensagens de erro que retornam qualquer informação sensível ao usuário;
    - Useara herança de objetos, encapsulamento e polimorfismo sempre que possível;
    - Usar variáveis de ambiente de forma prudente e sempre verifique os limites e os buffers;
    - Validar a entrada de dados para garantir que estejam bem formados e significativos.

6.19 TESTES DE INVASÃO

- Os testes de invasão externa serão realizados remotamente nas instalações do fornecedor. Os testes internos de intrusão serão realizados no escritório da Elitravel. A equipe de auditoria deve ter acesso à rede da organização;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Todos os testes serão realizados a partir do equipamento de propriedade da equipe de auditoria, portanto, nenhum equipamento para a execução dos testes é necessário. O único requisito a este respeito será ter uma conexão de rede ativa para cada membro da equipe de auditoria. Essas conexões devem fornecer acesso ao segmento de rede alvo em todos os casos;
- Se ocorrer um incidente durante a execução dos testes que tenham impacto nos sistemas ou serviços da organização, o incidente deve ser imediatamente levado à atenção dos responsáveis pelo gerenciamento de incidentes no projeto;
- Para todas as descobertas ou vulnerabilidades identificadas durante os testes realizados serão gerados e documentados evidências suficientes para provar a existência do mesmo. O formato da evidência pode ser variável em cada caso, captura de tela, saída bruta de ferramentas de segurança, fotografias, documentos em papel, etc;
- Como resultado de testes realizados deve gerar um documento contendo pelo menos as seguintes seções: Introdução, Sumário executivo, Metodologia, Vulnerabilidades identificadas, Recomendações para corrigir vulnerabilidades, Conclusões, Evidências.

6.20 PLANO DE RESPOSTA A INCIDENTES

Entende-se como incidente de segurança, qualquer incidente (acidental ou intencional) relacionado aos seus sistemas de comunicação ou de processamento de informações. O invasor pode ser um estranho mal-intencionado, um concorrente ou um colaborador descontente, e sua intenção pode ser roubar informações ou dinheiro, ou apenas prejudicar a organização.

O plano de resposta ao incidente deve ser testado uma vez por ano. As cópias deste plano de resposta a incidentes devem ser disponibilizadas a todos os membros da equipe relevantes e tomar medidas para garantir que eles entendam o que se espera deles.

Os colaboradores da organização deverão informar ao responsável quaisquer problemas relacionados à segurança.

O plano de resposta do incidente de segurança PCI da organização é o seguinte:

- Cada departamento deve reportar um incidente à Alta Direção;
- A Alta Direção coordenará a investigação do incidente e ajudará o departamento potencialmente comprometido a limitar a exposição dos dados do titular do cartão e a mitigar os riscos associados ao incidente;
- A Alta direção atuará para resolver o problema de forma satisfatória para todas as partes envolvidas, inclusive reportando o incidente e as descobertas às partes apropriadas (associações de cartão de crédito, processadores de cartão de crédito, etc.), conforme necessário;
- A Alta direção determinará se as políticas e os processos precisam ser atualizados para evitar um incidente semelhante no futuro e se são necessárias salvaguardas adicionais no ambiente onde ocorreu o incidente ou para a instituição;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Se um ponto ou dispositivos de acesso sem fio não autorizados forem identificados ou detectados como parte do teste trimestral, estem devem ser imediatamente escalados para a Alta Direção ou alguém por ela designado com que tenha autoridade para parar, cessar, desligar e remover o dispositivo ofensivo imediatamente;
- Um departamento que acredita razoavelmente que pode ter uma violação da conta, ou uma violação das informações do titular do cartão ou dos sistemas relacionados ao ambiente PCI em geral, deve informar à Alta Direção. Depois de ser notificado de um incidente, a Alta Direção, juntamente com outros colaboradores designados, implementará o Plano de Resposta ao Incidente do PCI para auxiliar e aumentar os planos de resposta dos departamentos.

Em resposta a um comprometimento de sistemas, a Alta Direção e os colaboradores designados irão:

- Certificar-se de que o sistema comprometido esteja isolado na rede;
- Reunir, rever e analisar os registros e informações relacionadas de várias salvaguardas centrais e locais e controles de segurança;
- Realizar análises forenses apropriadas do sistema comprometido;
- Entrar em contato com departamentos e entidades internos e externos, conforme apropriado;
- Fazer a análise forense e de registro disponível para o pessoal apropriado de segurança da lei ou do setor de cartões, conforme necessário;
- Atender o pessoal de segurança da lei e do setor de cartões em processos de investigação, incluindo em processos judiciais.

As empresas de cartão têm requisitos específicos individuais que a Alta Direção deve abordar ao tratar violações suspeitas ou confirmadas dos dados do titular do cartão.

Notificações de resposta de incidente a várias empresas de cartão:

- No caso de uma violação de segurança suspeita, avise imediatamente a Alta Direção;
- A Alta Direção coordenará uma investigação inicial da violação de segurança suspeita;
- Após a confirmação de que ocorreu uma violação de segurança, a Alta Direção começará a informar todas as partes relevantes que podem ser afetadas pelo incidente.

6.21 ACESSO DE TERCEIROS AO TITULAR DO CARTÃO

- Todas as empresas terceirizadas que prestam serviços críticos à Elitravel devem fornecer um Contrato de Nível de Serviço acordado;
- Todas as empresas terceirizadas que fornecem instalações de hospedagem devem cumprir com a Política de Segurança Física e Controle de Acesso da Empresa;
- Todas as empresas terceiras que tenham acesso à informação do titular do cartão devem:

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Aderir aos requisitos de segurança PCI DSS;
- Reconhecer a responsabilidade por garantir os dados do titular do cartão;
- Reconhecer que os dados do titular do cartão só devem ser usados para ajudar a conclusão de uma transação, apoiando um programa de fidelidade, fornecendo um serviço de controle de fraude ou para uso especificamente exigido por lei;
- Ter disposições adequadas para a continuidade do negócio em caso de grande destruição, desastre ou falha;
- Fornecer plena cooperação e acesso para realizar uma revisão de segurança completa após um incidente de segurança para um representante da indústria de cartões de pagamento ou um terceiro aprovado pelo setor de cartão de pagamento.

6.22 GERENCIAMENTO DE ACESSOS DE USUÁRIOS

- O acesso à organização é controlado através de um processo formal de registro de usuário, começando com uma notificação formal do RH ou responsável pelo departamento;
- Cada usuário é identificado por uma ID única para que possam ser vinculados e responsáveis por suas ações. O uso de IDs de grupo só é permitido quando eles são adequados para o trabalho realizado;
- A função de trabalho do usuário decide o nível de acesso do colaborador aos dados do titular do cartão;
- Uma solicitação de acesso deve ser feita por escrito (e-mail ou cópia impressa) pelo responsável do departamento do recém-chegado ou pelo RH. O pedido é de formato livre, mas deve indicar:
  - Nome da pessoa que faz o pedido;
  - Função de trabalho dos recém-chegados e do grupo de trabalho;
  - Data de início;
  - Serviços necessários para o desempenho das atividades.
- Cada usuário receberá uma cópia de seu novo formulário de usuário para fornecer uma declaração escrita dos seus direitos de acesso, assinada por um representante de TI após o procedimento de indução. O usuário assina o formulário indicando que eles entendem as condições de acesso;
- O acesso a todos os sistemas da organização é fornecido pela TI e só pode ser iniciado após a conclusão dos procedimentos adequados;
- Assim que um indivíduo deixa a organização, todos os logons do sistema devem ser imediatamente revogados.

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

6.23 CONTROLE DE ACESSO

- A Elitravel fornecerá a todos os colaboradores as informações de que precisam para desempenhar suas responsabilidades da forma mais efetiva e eficiente possível;
- As identificações genéricas ou de grupo normalmente não são permitidas, mas podem ser concedidas em circunstâncias excepcionais, se houver outros controles suficientes sobre o acesso;
- A alocação de direitos de privilégio (por exemplo, administrador local, administrador de domínio, superusuário, acesso raiz) deve ser restrita e controlada, e autorização fornecida conjuntamente pelo proprietário do sistema e pelos Serviços de TI. As equipes técnicas devem se proteger contra a emissão de direitos de privilégio para equipes inteiras para evitar a perda de confidencialidade;
- Os direitos de acesso serão concedidos seguindo os princípios de menor privilégio e necessidade de saber;
- Todo usuário deve tentar manter a segurança dos dados em seu nível classificado mesmo se os mecanismos técnicos de segurança falharem ou estiverem ausentes;
- Os usuários que optam por colocar informações em mídia digital ou dispositivos de armazenamento ou mantendo um banco de dados separado devem apenas fazê-lo, onde tal ação está de acordo com a classificação dos dados;
- Os usuários são obrigados a reportar instâncias de não conformidade à Alta Direção;
- A emissão de senha, os requisitos de força, a mudança e o controle serão gerenciados através de processos formais;
- O acesso a informações confidenciais, restritas e protegidas será limitado a pessoas autorizadas cujas responsabilidades de trabalho exigem, conforme determinado pelo proprietário dos dados ou pelo representante designado. Os pedidos de permissão de acesso a serem concedidos, alterados ou revogados devem ser feitos por escrito;
- Espera-se que os usuários se familiarizem e respeitem as políticas, padrões e diretrizes da organização, para o uso apropriado e aceitável das redes e sistemas;
- O acesso para usuários remotos deve estar sujeito a autorização dos Serviços de TI e ser fornecido de acordo com a Política de Acesso Remoto e a Política de Segurança da Informação. Não é permitido nenhum acesso externo descontrolado a qualquer dispositivo de rede ou sistema em rede;
- O acesso aos dados é variado e adequadamente controlado de acordo com os níveis de classificação de dados descritos na Política de Segurança da Informação;
- Os métodos de controle de acesso incluem direitos de acesso de logon, privilégios de conta de usuário, direitos de acesso de servidor e estação de trabalho, permissões de firewall, direitos de autenticação de intranet / extranet, direitos de banco de dados, redes isoladas e outros métodos, conforme necessário;

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

- Um processo formal deve ser conduzido regularmente por proprietários de sistemas e proprietários de dados em conjunto com os Serviços de TI para revisar os direitos de acesso dos usuários..

6.24 REDE SEM FIO

- É proibida a instalação ou o uso de qualquer dispositivo sem fio ou rede sem fio destinado a ser usado para se conectar a qualquer uma das redes ou ambientes da empresa;
- Um teste trimestral deve ser executado para descobrir quaisquer são os pontos de acesso sem fio conectados à rede da organização;
- O uso de testes adequados deve ser realizado trimestralmente para garantir que qualquer dispositivo que suporte comunicação sem fio permanece;
- Se qualquer violação da Política de Rede sem Fio for descoberta como resultado dos processos de auditoria normais, a Alta Direção poderá parar, cessar, desligar e remover o dispositivo ofensivo imediatamente.

Se for necessário utilizar a tecnologia sem fio pela empresa , as seguintes orientações devem ser cumpridas:

- Seqüências de caracteres e senhas padrão, frases de senha, chaves de criptografia / padrões de fornecedores relacionados com segurança (se aplicável) devem ser alteradas imediatamente após a instalação do dispositivo e se alguém com conhecimento destes deixar a organização;
- O firmware nos dispositivos sem fio deve ser atualizado de acordo com o cronograma de lançamento dos vendedores;
- O firmware nos dispositivos sem fio deve suportar criptografia forte para autenticação e transmissão em redes sem fio;
- Qualquer outro padrão de segurança do fornecedor de serviços relacionados à segurança deve ser alterado, se aplicável;
- As redes sem fio devem implementar práticas recomendadas do setor (IEEE 802.11i) e criptografia forte para autenticação e transmissão de dados do titular do cartão.

6.25 MONITORAÇÃO E CONTROLE

Os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da Elitravel, não podendo ser interpretados como de uso pessoal. Todos os colaboradores da Elitravel devem ter ciência de que o uso das informações e dos sistemas de informação da organização podem ser monitorados, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

7. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000

Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos criminais, se aplicáveis.

www.elitravel.com.br
Av. Pastor Martin Luther King Jr., 126 - Bloco 9 - Torre Office 3000
Grupo 1317 - Shopping Nova América, Rio de Janeiro – RJ
CEP: 20.765-000