Avaliação de riscos em fornecedores

Manual de controles de segurança da informação para personalizadoras de cartão de crédito e débito

DSC – Diretoria de segurança corporativa

SSI – Superintendência de Segurança da Informação

Itaú UNIBANCO

Índice

1. Objetivo

Este manual tem como objetivo informar aos fornecedores de serviços de personalização de cartões de crédito, débito e cartão segurança Itaú Unibanco Holding S. A. (CSI), sobre os controles de segurança da informação mínimos requeridos para reduzir os riscos de manuseio de dados do banco Itaú Unibanco Holding S. A.

2. Ciclo de vida das Informações

A informação é um ativo importante dentro da organização, e que deve ser protegido em todas as fases do seu ciclo de vida. No quadro abaixo demonstramos exemplos de meios físico e lógico durante o ciclo de vida da informação, onde a informação deve ser adequadamente protegida.

Ciclo de Vida	Meios	
	Físico	**Lógico**
Geração	Relatórios	Geração com dados de cartão
Transporte	Transporte dos cartões entre unidades internas do fornecedor	Link dedicado, FTP e qualquer tipo de conexão
Armazenamento	Cartões aguardando personalização	Arquivos com os dados de cartão
Manuseio	Embossing, envelopamento, conferência e despacho dos cartões	Transferência sistêmica de arquivos com dados de cartão para as diversas fases do processo (personalização, gráfica, berço, almoxarifado e outros)
Descarte	Destruição de papel, fitas de impressão e cartões impressos incorretamente	Limpeza dos dados de cartões após finalização do processo de personalização

3. Controles de segurança da informação e sua aplicabilidade

Introdução
A ISO 27002 é uma norma que trata das melhores práticas da segurança da informação. Os controles desse manual tiveram como base a ISO 27002, de modo que a numeração dos controles abaixo, seguem o mesmo padrão.

5.1.1 - Documento da política de segurança da informação - conjunto de princípios que norteia a gestão da segurança das informações corporativas. Esta política deve ser divulgada a todos os funcionários e partes externas relevantes para a proteção das informações do negócio da organização.
A política deve:

- ser aprovada pela administração;
- ser divulgada a toda organização;
- ser revisada anualmente;
- conter um escopo claramente definido;
- definir papéis e responsabilidades;
- classificação das informações.

6.1.2 - Coordenação da segurança da informação - representantes de diferentes partes da organização, com funções e papéis relevantes na coordenação das atividades operacionais de segurança da informação. A Coordenação deve:

- Definir e garantir a aderência da organização às diretrizes de segurança da informação;
- Identificar as ameaças significativas e a exposição da informação;
- Promover a conscientização pela segurança da informação;
- Monitorar os controles de segurança da informação e realizar uma análise crítica dos incidentes de segurança da informação;

6.1.5 - Acordos de confidencialidade - podem evitar a utilização indevida de informações sensíveis, no que diz respeito à questão de sigilo e condições de uso das informações confiadas aos funcionários, prestadores e partes externas relevantes.

7.1.1 - Inventário dos ativos – registro de identificação, localização e funcionalidade dos ativos de informação de valor relevante, para que a organização possa avaliar quais são os controles de segurança adequados. O inventário deve incluir uma identificação clara dos seguintes tipos de ativos: Informações, Software, Hardwares e Infra-estrutura.

7.2.1 - Recomendações para classificação – Elaboração de um esquema para classificar informações, que defina um conjunto apropriado de níveis de proteção e determine a necessidade de medidas especiais de tratamento para cada nível. A classificação deve:

- Ter como base os requisitos contratuais ou de conformidade legal,como o PCI;
- Abordar os principais ativos da organização;
- Designar responsável, custodiante e usuário das informações;
- Definir rótulos e regras para o tratamento seguro das informações durante todo o seu ciclo de vida.

8.2.2 - Conscientização, educação e treinamento em segurança da informação – sensibilização constante de funcionários e partes externas relevantes, por exemplo, prestadores de serviço, da necessidade de segurança da informação, a partir de programas de conscientização sobre segurança da informação, com foco nos dados sensíveis para a industria de cartões. O programa deve garantir que os colaboradores sejam conscientizados desde a sua contratação e periodicamente, e assegurar através de formalização o reconhecimento do conteúdo da política de segurança da informação.

8.3.2 - Devolução de ativos – definição de um processo para a proteção das informações e preservação do patrimônio organizacional no processo de encerramento ou transferência de

atividades. Os ativos que devem ser devolvidos incluem, mas não se restringem a: Equipamentos, Documentos corporativos, Softwares entregues à pessoa, Dispositivos de comunicação móvel, Cartões de crédito e Manuais.

8.3.3 - Retirada de direitos de acesso – remoção dos direitos de acesso de todos os funcionários, fornecedores e terceiros, a informações e aos recursos de processamento da informação após o encerramento de suas atividades, contratos ou acordos, ou ajustados após mudanças destas atividades.

9.1.2 - Controles de entrada física - acesso a áreas de segurança, como escritório, sala ou instalação de processamento e armazenamento de informações sensíveis ao negócio da organização, liberado somente para pessoas autorizadas, com entrada e saída controladas e registradas por meio de mecanismos apropriados. O controle deve incluir:

- Distinção das áreas de segurança. Perímetros que devem ser considerados: Administração, Personalização, Gráfica, Berço, Cofre, Almoxarifado, Datacenter, Operação, Expedição e outros;
- Alguma forma fácil de identificação, dentro das que tratem de informações críticas, que permita distinguir funcionários, fornecedores, e visitantes, através do CFTV;
- Registro de todos os acessos para fins de auditoria, incluindo o nome do visitante, a empresa representada, o funcionário que autoriza o acesso físico data e hora de entrada e saída;
- Armazenamento dos registros por pelo menos três meses.

9.1.3 - Segurança em escritórios, salas e instalações - informações e equipamentos precisam ficar protegidos de furtos, danos ou destruição por incidentes causados por pessoas que acessam a área sem autorização, ainda que estas áreas sejam equipadas com barreiras e controles de acesso. As seguintes diretrizes ou padrões técnicos devem ser aplicados:

- O ambientes críticos, como personalização, cofre, devem estar localizados de forma a evitar o acesso de pessoas não autorizadas e possuir monitoramento por circuito fechado de TV (CFTV);
- As portas e janelas devem ser mantidas fechadas quando não utilizadas e dotadas de proteções externas, principalmente quando estiverem localizadas no andar térreo;
- Evitar o impacto na instalação de serviços de suporte e equipamentos, por exemplo, fotocopiadoras e fax, em ambientes onde informações críticas possam ser comprometidas;
- Posicionar equipamentos de forma que o ângulo de visão seja restrito, de modo a reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante sua utilização;
- Instalar sistemas de detecção de intrusos, de forma a inibir o acesso por qualquer porta externa e janela acessível. As áreas desocupadas devem possuir um sistema de alarme que permaneça sempre ativado.

9.1.6 - Acesso do público, áreas de entrega e de carregamento - áreas públicas, tais como áreas de expedição, entrega e carregamento, devem possuir controles coerentes com os riscos. Construir as áreas de expedição, entrega e carregamento, incluindo:

- Acesso restrito somente ao pessoal identificado e autorizado à área de movimentação e suporte (carga e descarga) a partir do exterior do prédio, com utilização de portas tipo eclusa;
- Os materiais devem ser carregados ou descarregados sem que o pessoal responsável tenha acesso às outras partes da organização.

9.2.1 - Instalação e proteção do equipamento (riscos ambientais) - Os seguintes controles devem ser adotados:

- Dispositivos para minimizar o risco de: incêndio, explosões, fumaça, inundações, poeira, vibração, superaquecimento e outros;
- Adotar mecanismos de proteção contra relâmpagos, incluindo filtros de proteção nas linhas de comunicação.
- Estabelecer normas específicas para proibir alimentação, bebida e fumo nas proximidades das instalações de processamento da informação;
- Monitorar aspectos ambientais (temperatura, umidade, etc.) que evitem condições que possam afetar negativamente a operação.

9.2.2 – Infraestrutura de energia elétrica – Controles que evitem distúrbios, interrupções e oscilações no fornecimento de energia elétrica podem afetar o desempenho ou ainda causar danos aos equipamentos e interrupções de operações do negócio. Devem ser utilizados “No-breaks”, geradores reserva, aterramento das instalações elétricas, e técnicas de condicionamento de energia, em conformidade com as especificações dos fabricantes dos equipamentos.

9.2.6 - Reutilização e alienação segura de equipamentos – O descarte de dispositivos de armazenamento (discos rígidos, memórias "flash" e outros meios de armazenamento) que contenham informação sensível, principalmente dados de cartões de débito/crédito, deve ser realizado através da destruição física ou sobrescritos de forma segura.

9.2.7 - Remoção de propriedade - a ausência ou ineficácia do controle de retirada de equipamentos, "software" e dados armazenados traz riscos à segurança da informação. A remoção de ativo deve ser autorizada pelo seu responsável, possuir registros de retirada e devolução.

10.1.2 - Gestão de mudanças: a ausência ou o controle inadequado de modificações nos sistemas e recursos de processamento da informação podem ocasionar falhas operacionais ou de segurança. Por isso é necessário que a empresa tenha processos de gestão de mudança que aborde os seguintes itens:

- Identificação, registro e aprovação formal das mudanças significativas, como novos cartões ou alterações em cartões existentes;
- Planejamento, teste e avaliação de impactos operacionais e de segurança das mudanças;
- Comunicação dos detalhes das mudanças para todas as pessoas envolvidas;
- Procedimentos de recuperação em caso de insucesso ou ocorrência de eventos inesperados.

10.1.3 - Segregação de funções: é um princípio da segurança usado para impedir que uma única pessoa possa acessar modificar ou usar ativos sem a devida autorização ou detecção, reduzindo os riscos de uso acidental ou deliberado destes ativos, assim como a possibilidade de conluios nas fases de personalização de cartões. Assegurar que estágios críticos de um processo, como a do administrador do sistema e do auditor de segurança, aprovação da reimpressão de cartões defeituosos e outros, fiquem a cargo de dois ou mais indivíduos.

10.1.4 - Separação dos recursos de desenvolvimento, teste e de produção: as atividades de desenvolvimento e teste podem causar sérios problemas no ambiente de produção, como, por exemplo, modificações inesperadas ou falhas em arquivos ou em sistemas. Além da segregação dos ambientes, os seguintes procedimentos devem ser adotados:

- Estabelecer perfis diferentes de acesso de usuários para "software" em situação de desenvolvimento, de teste e de produção;
- Tornar inacessíveis compiladores, editores e outras ferramentas de desenvolvimento a partir dos sistemas operacionais do ambiente de produção (quando não forem necessários);
- Proteger e controlar os dados de teste, não utilizando os dados do Banco Itaú Unibanco Holding S. A. de produção nessa atividade.

10.2.2 - Monitoramento e análise crítica de serviços terceirizados: a monitoração e análise crítica dos serviços terceirizados garantem a aderência entre os termos de segurança da informação e as condições dos acordos, além de permitir o gerenciamento adequado de problemas e incidentes de segurança. Os seguintes procedimentos devem ser adotados:

- Atribuir a um indivíduo ou a equipe de gerenciamento de serviço a responsabilidade pelo gerenciamento do relacionamento com o terceiro.
- Atribuir ao terceiro a responsabilidade pela verificação de conformidade e reforço aos requisitos dos acordos em seu ambiente.
- Disponibilizar habilidades técnicas suficientes e os recursos necessários para monitorar se os requisitos dos acordos, em particular os requisitos de segurança da informação, estão sendo atendidos.
- Executar regularmente auditorias nos serviços de terceiros

10.4.1 - Controles contra códigos maliciosos: "softwares" maliciosos, tais como vírus de computador, cavalos de Tróia, "worms" de rede e bombas lógicas, são agentes potencialmente graves à segurança da informação, pois possibilitam o roubo de informações sigilosas e a paralisação dos serviços. Os seguintes procedimentos devem ser adotados:

- Estabelecer política formal de uso de "software";
- Manter atualizado o "software" de anti-vírus.

10.5.1 - Cópias de segurança das informações: a ocorrência de desastres, erros operacionais ou falhas nos recursos de processamento da informação podem fazer com que dados e "software" essenciais ao negócio da organização sejam perdidos, assim, os seguintes procedimentos devem ser adotados:

- Gerar e testar regularmente as cópias de segurança das informações;

- Armazenar cópias de segurança a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;
- Usar criptografia para situações onde a confidencialidade das cópias de segurança precisa ser mantida, como dados de cartões.

10.6.1 - Controles de redes: a comunicação entre as localidades de uma organização (matriz e filiais, por exemplo), bem como entre a organização e o meio externo (Internet, por exemplo), normalmente faz uso de redes de computadores. Uma rede de computadores representa um potencial ponto de risco à segurança da informação, visto que pode possuir inúmeras brechas ou vulnerabilidades que permitem o acesso indevido aos sistemas, serviços e recursos de processamento da informação e, portanto, requer controles de segurança adequados em sua administração, tais como:

- Segregar a responsabilidade operacional pela operação dos recursos computacionais;
- Utilizar criptografia robusta e protocolos de segurança como SSL/TLS ou IPSEC para proteger os dados confidenciais do portador do cartão durante a transmissão em redes sem fio e públicas;
- Monitorar a presença de pontos de acesso sem fio;
- Usar sistemas de detecção de invasão e/ou sistemas de prevenção contra invasão para monitorar todo o tráfego no ambiente de dados do portador do cartão e alertar as equipes sobre comprometimentos suspeitos;
- Formalizar, justificar, aprovar e testar todas as conexões de rede, serviços, protocolos e portas de comunicação permitidas e alterações às configurações do firewall e do roteador;
- Analisar os conjuntos de regras do firewall e do roteador pelo menos a cada seis meses;
- Manter diagrama da rede atualizado com todas as conexões com relação aos dados do portador do cartão, incluindo quaisquer redes sem fio.
- Controle rigido sobre equipamentos e/ou softwares com capacidade para analisar tráfego de rede

10.7.1 - Gerenciamento de mídias removíveis - fitas, discos, cartuchos, "flash disks", CD, DVD e mídia impressa, dentre outras mídias removíveis, costumam conter dados e informações confidenciais do portador do cartão, portanto, requer controles de segurança adequados em sua administração, tais como:

- Habilitar unidades de mídias removíveis somente se houver uma necessidade do negócio;
- Registrar, inventariar e classificar a informação das mídias removíveis para limitar a oportunidade de perda de dados;
- Obter aprovação da gerência e registrar a remoção de qualquer mídia da organização;
- Tornar o PAN, no mínimo, ilegível em qualquer local onde ele esteja armazenado em mídia digital portátil, mídia de back-up e outros.

10.7.2 - Descarte de mídias - mídias óticas e eletrônicas, tanto as fixas como as removíveis, contêm dados e informações confidenciais para o negócio da organização. Quando não forem mais utilizadas, requerem os seguintes cuidados no descarte:

- Identificar e registrar as mídias que requerem descarte seguro, tais como cartões e cartas impressos incorretamente, fitas TOP e outros;
- Triturar, incinerar ou amassar as mídias para que os dados do portador do cartão não possam ser recuperados;
- Os serviços terceirizados de coleta e descarte de papel, de equipamentos e de mídias magnéticas, deve ser efetuado por fornecedor com experiência e controles de segurança adequados.

10.8.3 - Mídias em trânsito - o transporte físico de mídias externas aos limites da organização é um potencial ponto de risco à segurança da informação, visto que as torna vulneráveis a acessos não autorizados, danos ou adulterações, principalmente quando realizado por terceiros, assim, os seguintes procedimentos devem ser adotados:

- Utilizar transporte ou serviço de mensageiro confiável;
- Enviar a mídia via mensageiro identificado e seguro ou outro método de entrega que pode ser monitorado com precisão;
- Adotar controles especiais, para proteger informações críticas, tais como: recipientes lacrados, entrega em mãos, lacres específicos de pacotes (que revele qualquer tentativa de acesso), divisão do conteúdo em mais de uma remessa, transporte de cada uma das mídias por rotas distintas e assinatura digital com criptografia;
- Cartões (personalizados ou não) transportados entre as diferentes unidades, devem ser acondicionados em cofres com as chaves em poder da empresa responsável pelos cartões (nunca do mensageiro), com escolta e monitoramento do itinerário.

10.8.4 - Mensagens eletrônicas - mensagens eletrônicas como correio eletrônico, "Eletronic Data Interchange" (EDI) e sistemas de mensagens eletrônicas instantâneas cumprem um papel cada vez mais importante nas comunicações das organizações. Os seguintes procedimentos devem ser adotados para transmissão:

- Proteger os dados do portador do cartão contra acessos não autorizados, modificação ou negação de serviço e utilizar mecanismos de criptografia, quando necessário;
- Nunca enviar PANs não criptografadas através das tecnologias de envio de mensagens de usuário final (por exemplo, e-mail, sistemas de mensagens instantâneas, bate-papo);

10.10.1 - Registros de auditoria - Os "logs" de eventos dos sistemas contêm informações que ajudam na identificação de ataques, fraudes e outros eventos de segurança, assim, os seguintes procedimentos devem ser adotados:

- Padronizar os registros ("logs") de auditoria para as atividades de usuários, exceções e outros eventos de segurança da informação, incluindo: identificação dos usuários, datas e horários como detalhes de eventos-chave, identidade e localização da estação de trabalho, registros das tentativas de acesso aceitas e rejeitadas e outras informações relevantes;
- Os administradores de sistemas não devem ter permissão de exclusão ou desativação dos registros ("log") de suas próprias atividades, seguindo as orientações estabelecidas nas regras de segregação de funções;

- Definir, para cada conjunto de registros ("logs") de auditoria, uma periodicidade de retenção baseada em determinações de órgãos reguladores;
- Manter um histórico da trilha de auditoria por pelo menos um ano, com um mínimo de três meses imediatamente disponível para análise (por exemplo, online, arquivado ou recuperável a partir do back-up);
- Armazenar os registros ("log") de auditoria em locais adequados, providos de controle de acesso, pelos períodos definidos;
- Ter uma atenção especial à mídia de armazenamento dos registros, que deve ter validade superior ao período de retenção definido, de forma que a qualidade das evidências seja mantida.

10.10.3 - Proteção das informações dos registros – Os registros ("logs") de auditoria podem ser adulterados por falhas técnicas ou por meio de ação deliberada para encobrir atividades não autorizadas, assim, os seguintes procedimentos devem ser adotados:

- Os servidores de "log" devem estar localizados em uma área de segurança, contendo uma console de gerenciamento e uma impressora conectada localmente;
- Os servidores de "log" devem estar em uma rede segmentada da rede local, com proteção de dispositivos de segurança ("Firewall" e VLAN);
- Os relógios dos servidores de "log" devem estar sincronizados;
- Registrar todas as atividades executados nos servidores de "log";
- Devem-se aplicar medidas de segregação de funções para assegurar que as pessoas autorizadas que realizam atividades nos servidores de "log" sejam diferentes daquelas que realizam a auditoria;
- O acesso remoto aos servidores de "log" deve ser feito através de utilização de protocolos seguros (por exemplo: SSL/SSH);
- Documentar todos os procedimentos dos servidores de "log", tais como: configuração e instalação, administração e operação, backup e manutenção, acessos a todas as trilhas de auditoria, inicialização dos registros de auditoria.

10.10.6 - Sincronização dos relógios - O correto estabelecimento dos relógios dos computadores é importante para garantir a exatidão dos registros ("log") de auditoria, que podem ser requeridos por investigações ou apresentação de evidências em casos legais ou disciplinares. Os seguintes procedimentos devem ser adotados:

- Implementar mecanismo que permita a sincronização dos relógios de computadores a um padrão de tempo confiável, por exemplo, o tempo coordenado universal ("Coordinated Universal Time" - UTC) ou um padrão de tempo local (Observatório Nacional - ON);
- Definir rotina para a verificação de inconsistências e correção das variações de tempo significativas.

11.2.1 - Registro de usuário - a concessão indiscriminada de contas de acesso a sistemas e serviços, assim como a não obrigatoriedade de revogação de contas não utilizadas (por exemplo, de ex-funcionários), favorece a ocorrência de acessos indevidos, assim, os seguintes procedimentos devem ser adotados:

- Estabelecer procedimentos que orientem a concessão e revogação de contas de acesso;
- Identificação de usuário (ID) única para assegurar a responsabilidade de cada usuário por suas;
- Permissão do uso de grupos de ID somente onde existe necessidade para o negocio ou por razões operacionais;
- Autorização do proprietário do sistema para liberação do acesso para usuários;
- Declaração por escrito dos direitos de acesso a ser fornecida aos usuários;
- Assinatura do usuário em declaração indicando que as condições de acesso foram entendidas;
- Liberar acesso aos usuários somente após conclusão dos procedimentos de autorização;
- Registro formal de todas as pessoas com direito de acesso concedido;
- Remoção imediata, ou bloqueio dos direitos de acesso, de usuários que mudaram de cargos, funções ou deixaram a organização.

11.2.2 - Gerenciamento de privilégios - o uso inapropriado de privilégios especiais de acesso pode ser um grande fator de contribuição para falhas ou violações, permitindo a divulgação ou modificação imprópria de informações, fraudes e sabotagens, assim, os seguintes procedimentos devem ser adotados:

- Identificar e registrar os privilégios especiais de acesso associados a cada componente relacionado ao uso de sistemas e aplicações (sistema operacional, gerenciador de banco de dados, etc.);
- Identificar e registrar as categorias e perfis de usuários para os quais os privilégios especiais de acesso precisam ser concedidos;
- Conceder privilégios especiais de acesso a usuários conforme sua necessidade de uso e em concordância com a política de acesso;
- Conceder privilégios especiais de acesso somente após a conclusão dos procedimentos de autorização formal;
- Registrar as concessões e alterações de privilégios especiais de acesso (como, por exemplo, no remanejamento de funcionários e prestadores de serviço) para posterior análise crítica;
- Autenticar todos os acessos para qualquer banco de dados que contenha dados do portador do cartão, incluindo acesso por meio de aplicativos, administradores e todos os outros usuários.

11.2.3 - Gerenciamento de senha do usuário - senhas são um meio comum de verificar automaticamente a identidade dos usuários antes que acessos a sistemas e serviços sejam liberados conforme os níveis de autorização concedidos, podendo se tornar vulneráveis sem o devido gerenciamento, assim, os seguintes procedimentos devem ser adotados:

- Forçar a troca obrigatória de senhas temporárias, no primeiro acesso ao sistema;
- Restrição de reutilização de senhas;
- Criação de máscaras de senhas;

- Forçar a troca periódica de senhas;
- Verificar a identidade do usuário antes de fornecer uma senha temporária, de substituição ou nova;
- Obter assinatura do usuário em declaração solicitando a manutenção da confidencialidade das senhas fornecidas;
- Fornecer inicialmente aos usuários senhas seguras e temporárias com troca obrigatória no primeiro acesso realizado;
- Os usuários devem acusar o recebimento das senhas;
- Manter senhas gravadas somente em computadores protegidos;
- Remover/desativar as contas dos usuários inativos pelo menos a cada 90 dias;
- Ativar as contas usadas pelos fornecedores somente para a manutenção remota durante o período necessário.

11.3.1 - Uso de senhas - senhas são um meio comum de verificar automaticamente a identidade dos usuários antes que acessos a sistemas e serviços sejam liberados conforme os níveis de autorização concedidos, podendo se tornar vulneráveis sem o devido tratamento, assim, os seguintes procedimentos devem ser adotados:

- Orientar usuários na formação de senhas fortes;
- Orientar usuários a manter a confidencialidade das senhas;
- Evitar a utilização da mesma senha para uso com finalidades profissionais e pessoais.

11.3.3 - Política de mesa limpa - uma política de "mesa limpa" é uma forma eficaz para reduzir os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho, assim, os seguintes procedimentos devem ser adotados:

- Papéis e mídias de computador devem ser guardados, quando não estiverem sendo utilizados, em lugares adequados, com fechaduras ou outras formas seguras de mobiliário, especialmente fora do horário normal de trabalho;
- Informações sensíveis ou críticas ao negócio, quando não requeridas, devem ser guardadas em local distante, de forma segura e fechada, de preferência em um cofre ou arquivo resistente a fogo, especialmente quando o escritório estiver vazio;
- Pontos de recepção e envio de correspondências e máquinas de fax e telex não assistidas devem ser protegidos;
- Equipamentos de reprodução (fotocopiadoras, "scanners" e máquinas fotográficas digitais) devem ser travadas ou de alguma forma protegidas contra o uso não autorizado fora do horário de trabalho;
- Informações sensíveis e classificadas, quando impressas, devem ser imediatamente retiradas da impressora e fax.

11.3.3 - Política de tela limpa - uma política de "tela limpa" é uma forma eficaz para reduzir os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho, assim, os seguintes procedimentos devem ser adotados:

- Os computadores pessoais, terminais de computador e impressoras devem ser desligados quando desassistidos;
- Equipamentos devem ser protegidos por mecanismo de travamento de tela e teclado controlados por senhas, chaves ou outros mecanismos de autenticação quando não estiverem em uso;
- Se uma sessão estiver ociosa por mais de 15 minutos, exigir que o usuário redigite a senha para reativar o terminal.

11.4.2 - Autenticação para conexão externa do usuário - as conexões externas, por exemplo, realizadas por meio de acesso discado ("dial-up"), geralmente não possuem o mesmo nível de segurança que a rede de comunicação, dotada de controles de segurança específicos, assim, os seguintes procedimentos devem ser adotados:

- Técnicas baseadas em criptografia, "hardware tokens" ou protocolo de desafio/resposta;
- Procedimentos e controles de discagem reversa ("dial-back") para prover proteção contra conexões não autorizadas e não desejadas;
- Autenticação do nó da rede com base em certificados de máquina;
- Incorporar a autenticação com dois fatores para o acesso remoto (acesso no nível da rede que se origina fora dela) à rede pelos funcionários, administradores e terceiros. Usar tecnologias como a autenticação remota e o serviço dial-in (RADIUS); sistema descontrole de acesso ao controlador de acesso do terminal (TACACS) com tokens; ou VPN (baseado em SSL/TLS ou IPSEC) com certificados individuais.

11.4.4 - Proteção e configuração de portas de diagnóstico remotas - computadores e sistemas de comunicação possuem instalados recursos remotos de diagnóstico e configuração para uso dos engenheiros de manutenção, para dar suporte aos sistemas mais complexos e críticos do negócio, assim, os seguintes procedimentos devem ser adotados:

- Implementar uma chave de bloqueio e procedimentos para controlar o acesso físico às portas;
- Estabelecer um procedimento que garanta que essas portas sejam acessíveis somente através de um acordo entre o gestor dos serviços e o pessoal de suporte que solicitou o acesso;
- Desabilitar ou remover dos equipamentos portas, serviços e recursos similares que não são especificamente requeridos para a funcionalidade do negócio.

11.4.5 - Segregação de redes - as redes se estendem cada vez mais além dos limites tradicionais da organização, à medida que as parcerias de negócio são formadas, e podem requerer a interligação ou compartilhamento dos recursos de rede e de processamento de informações, assim, os seguintes procedimentos devem ser adotados:

- Implementar os perímetros de segurança com a instalação de um "gateway" seguro entre as redes, considerando os seguintes perímetros: rede administrativa, produtiva, transferência de arquivos com o banco e outras;
- Restringir o tráfego de entrada e saída ao necessário para o ambiente de dados do portador do cartão;

- Posicionar o banco de dados em uma zona da rede interna, separada da DMZ;
- Proibir o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do portador do cartão;
- Implementar o mascaramento de IP para impedir que endereços internos sejam traduzidos e revelados na Internet, usando o espaço de endereço RFC 1918. Usar as tecnologias NAT (network address translation).
- Se aplicável, subdividir os domínios internos em grupos de serviços de informação, usuários e sistemas de informação;
- Segregar as redes sem fio das redes internas ou privadas, visto que os perímetros de redes sem fio não são bem definidos e necessitam uma análise/avaliação de riscos para identificar controles adicionais de segurança (por exemplo, autenticação forte, métodos criptográficos e seleção de freqüência).

11.5.1 - Procedimentos seguros de entrada no sistema – logon - a identificação de um usuário válido é o ponto de partida para uma invasão ou ataque à rede, colocando em risco informações sensíveis, sistemas e serviços, assim, os seguintes procedimentos devem ser adotados:

- Não mostrar identificadores de sistema ou de aplicações até que o processo de entrada no sistema tenha sido concluído com sucesso;
- Mostrar um aviso geral informando que somente pessoas autorizadas devem obter acesso ao computador;
- Não fornecer mensagens de ajuda durante o procedimento de entrada no sistema que poderiam auxiliar um usuário não autorizado;
- Validar a informação de entrada no sistema apenas quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não deve indicar que parte do dado de entrada está correta ou incorreta;
- Limitar o número de tentativas de entrada no sistema sem sucesso, para um máximo de 3 tentativas;
- Limitar o tempo máximo e mínimo para o procedimento de entrada no sistema. Se excedido, o sistema deverá encerrar o procedimento;
- Mostrar data e hora da última entrada no sistema com sucesso e detalhes de qualquer tentativa sem sucesso de entrada no sistema desde o último procedimento efetuado com sucesso;
- Não mostrar a senha que está sendo informada ou ocultar os caracteres da senha com símbolos;
- Tornar todas as senhas ilegíveis durante a transmissão e o armazenamento em todos os componentes usando a criptografia robusta.

11.6.2 - Isolamento de sistemas sensíveis - os sistemas de aplicação possuem requisitos de negócio e de proteção diferenciados, que devem ser observados para a adoção dos controles de segurança adequados, assim, os seguintes procedimentos devem ser adotados:

- Separar física e logicamente o sistema de aplicação sensível dos demais, por exemplo, utilizando um computador dedicado e um "gateway" que isole logicamente o segmento da

rede de computadores, servidor de recebimento do arquivo para personalização exclusivo, pastas no servidor de arquivos dedicado (não compartilhado) para o cliente;

- Garantir que o sistema de aplicação sensível compartilhe recursos somente com outros sistemas confiáveis.

12.3.1 - Política para o uso de controles criptográficos - conjunto de regras que garantem a padronização das técnicas criptográficas, a aplicação adequada das mesmas e responsabilidades, para garantir a segurança no transporte ou armazenamento das informações, sem afetar o negócio da organização. Esta política deve:

- Definir as técnicas de criptografia e a adequada aplicação das mesmas;
- Definir o uso de criptografia, conforme a classificação das informações (ex. confidencial, etc.), no transporte e/ou armazenamento, independente do meio utilizado (linha de comunicação, mídias e dispositivos fixos, removíveis ou móveis, etc.);
- Ter um procedimento para Gerenciamento das Chaves Criptográficas para garantir a proteção das chaves e a recuperação das informações criptografadas caso as chaves sejam perdidas, expostas ou danificadas;
- Definir os responsáveis pela implementação e atualização da Política e pelo Gerenciamento das Chaves Criptográficas em todo o seu ciclo de vida.

12.3.2 – Gerenciamento de chaves – procedimento para garantir a proteção das Chaves Criptográficas em todas as etapas do processo: Geração, Custódia, Armazenamento, Backup, Recuperação, Distribuição, Utilização, Revogação, Renovação e Procedimento para Destruição das Chaves. Os controles devem:

- Garantir a geração de chaves robustas, conforme padrões da indústria financeira, incluindo: geração dentro de hardware seguro homologado FIPS, geração de número aleatório e primo, registro em ata de cerimônia de geração de chave, ambiente segregado para a geração de chaves;
- Definir sobre a geração e obtenção de certificados de chave pública;
- Definir a forma de distribuição (se manual ou eletrônica) com controles que garantam a proteção das chaves e o procedimento para ativação após recebimento;
- Definir o armazenamento seguro das chaves: se “em claro” dentro da memória protegida de hardwares criptográficos, se criptografadas em outras formas de armazenamento, se dois ou mais componentes criptografados ou “em claro” em dupla custódia. Além do uso de cofre que garanta integridade e controle de acesso às chaves, mantendo o menor número possível de locais e formatos das chaves;
- Definir a atualização periódica das chaves, incluindo tempo e o procedimento para atualização;
- Definir as situações em que são necessárias Revogação ou Destruição das chaves, por exemplo, quando houver comprometimento das chaves ou saída de colaborador da equipe (neste caso as chaves também devem ser guardadas), bem como o procedimento para execução;

- Definir sobre a Recuperação de Chaves, incluindo: procedimento (cerimônia, recuperação através do backup) e situações em que deve ocorrer (ex. quando corrompidas, perdidas), com o intuito de garantir a continuidade do negócio, nos casos de recuperação de informações criptografadas;
- Definir o Procedimento de Backup das Chaves para reserva ou acesso a informações arquivadas, sendo que as chaves devem ser armazenadas em arquivos criptografados e ter cópia de seus componentes em papel armazenada em local diferente do original;
- Definir sobre a Destruição das Chaves, incluindo quando se aplica e procedimento (comunicado aos envolvidos, cerimônia, destruição de todos os documentos ou dispositivos magnéticos relacionados, registro em ata, etc.);
- Manter registro (log) de todas as ações que envolvam o Gerenciamento das Chaves, bem como Auditorias internas ou externas para verificação do cumprimento das normas relacionadas a esta gestão;
- Manter assinatura de Termo de Responsabilidade pelos colaboradores responsáveis pela custódia e proteção das chaves criptográficas;
- Restringir o acesso às chaves criptográficas ao menor número possível de colaboradores.

12.6.1 – Controle de Vulnerabilidades Técnicas – procedimento que garanta a eliminação ou minimização da ação de códigos maliciosos ou falhas nos sistemas através da atualização de patches. Os seguintes procedimentos devem ser adotados:

- Inventariar todos os ativos e componentes de tecnologia;
- Definir responsáveis pela monitoração das vulnerabilidades, análise de riscos e implementação de “patches”;
- Identificar vulnerabilidades recentes, por exemplo, através de um serviço de alertas;
- Definir a frequência e limite de tempo para atualização dos patches, devendo ser instalado em até 1 mês após a descoberta os patches de segurança críticos;
- Avaliar e testar os patches em ambiente isolado e controlado antes da aplicação em ambiente de produção;
- Priorizar a aplicação das correções em sistemas mais críticos ou de alto risco;
- Assegurar que todos os componentes dos sistemas e softwares estão com os patches de segurança recomendados e disponibilizados pelos fornecedores instalados;
- Manter registro de auditoria de todos os procedimentos realizados para atualização dos patches;
- Estabelecer configuração padrão para todos os componentes do sistema (blindagem) que abranja as vulnerabilidades conhecidas, as melhores práticas recomendadas para o negócio em questão, desativando os protocolos, serviços, funcionalidades inseguras e/ou desnecessárias e paramentrização padrão do fornecedor;
- Realizar testes de penetração externos e internos, pelo menos 1 vez por ano ou após modificações significativas no ambiente.

13.2.1 – Responsabilidades e Procedimentos (Incidentes de Segurança da Informação)– procedimento para tratamento a incidentes de segurança da informação e resposta rápida, efetiva e ordenada. Deve abranger os seguintes controles:

- Definir o tipo, quantidade, volume e custo de incidentes;
- Definir as responsabilidades no tratamento aos incidentes;
- Planos de respostas a cada um dos tipos de incidentes (violação de confidencialidade, negação de serviço, código malicioso, etc.);
- Manter documentação de análise e causa dos incidentes;
- Planejar e implementar medidas para prevenir a reocorrência;
- Proteção das trilhas de auditoria e evidências relacionadas ao incidente;
- Comunicar o incidente de segurança envolvendo o Banco Itaú Unibanco Holding S. A. (gestor do fornecedor).

13.2.2 – Aprendendo com os incidentes de Segurança da Informação – As análises críticas dos incidentes de segurança da informação podem indicar a necessidade de melhorias ou controles adicionais para limitar a freqüência, os danos e os custos de incidentes semelhantes no futuro. Além disso, as análises críticas são previstas no processo de revisão da política de segurança da organização.