Visão Geral da Segurança da Informação

Mar/2024

Serasa Experian

A Serasa Experian é líder na América Latina em serviços de informações para apoio na tomada de decisões das empresas. No Brasil, é sinônimo de solução para todas as etapas do ciclo de negócios, desde a prospecção até a cobrança, oferecendo às organizações as melhores ferramentas. Com profundo conhecimento do mercado brasileiro, conjuga a força e a tradição do nome Serasa com a liderança mundial da Experian. Criada em 1968, uniu-se à Experian Company em 2007. Responde on-line/real-time a 6 milhões de consultas por dia, auxiliando 500 mil clientes diretos e indiretos a tomarem a melhor decisão em qualquer etapa de negócio. A Experian plc está listada na Bolsa de Valores de Londres (EXPN) e compõe o índice FTSE 100.

Constantemente orientada para soluções inovadoras, a Serasa Experian vem contribuindo para a transformação do mercado de soluções de informação, com a incorporação contínua dos mais avançados recursos de inteligência e tecnologia.

Procedimentos e Processos de gestão

A Serasa Experian mantém um abrangente programa de segurança da informação que contém controles adequados de acordo com o risco e a sensibilidade da informação. Tais controles são desenhados para:

- Garantir que a segurança e a confidencialidade das informações de clientes
- Proteger contra ameaças e riscos previstos que impactam a segurança da informação
- Proteger contra acesso não autorizado ou usar qualquer informação que possa resultar em prejuízos para clientes

Somos certificados ISO27001 – Vide o link
https://www.serasaexperian.com.br/cadastro-positivo-seguranca-da-informacao/
Política de Privacidade link.

Política de Segurança e ciclo de atualização

A Serasa Experian possui um Programa de Segurança da Informação abrangente, incluindo controles administrativos, técnicos e físicas adequadas à complexidade, natureza e alcance das nossas atividades e a sensibilidade de seus ativos de informação. Esses controles são projetados para:

(1) alcançar a segurança e a confidencialidade das nossas Informações;
(2) proteger contra ameaças, riscos de segurança ou integridade da Informação;
(3) proteger contra acesso não autorizado ou uso indevido de informações;
(4) fornecer eficácia contínua dos controles.

Nossa Política Global de Segurança da Informação é baseada na norma ISO 27001 (International Organization for Standization). A ISO 27001 disponibiliza um modelo para estabelecer, implantar, operar, monitorar, revisar manter e melhorar um Sistema de Gerenciamento de Segurança da Informação. Como parte do gerenciamento de políticas, um fórum da alta direção é usado para revisar e aprovar todas as novas políticas e mudanças para políticas existentes.

Para mais informações, vide nosso site.

Classificação da Informação

Temos uma abordagem gerenciada de segurança para garantir que as nossas informações sejam protegidas durante todo o ciclo de vida, desde a criação, transformação e uso, armazenamento e destruição. Controles específicos são implementados de acordo com a classificação das informações para garantir que possam ser gerenciadas de forma adequada, incluindo controles de acesso, criptografia, rotulagem, divulgação para partes internas e externas, envio e manuseio e destruição/descarte.

Utilizamos Sistema para prevenção de perda de dados (DLP) configurado para identificar, monitorar e proteger dados em uso, dados em movimento e dados em repouso através de inspeção de conteúdo e regras específicas.

Treinamento e Conscientização

Todos os colaboradores possuem NDA e participam de treinamentos anuais mandatório de segurança da informação, Desenvolvimento de Sofware Seguro, Gestão de Riscos, Compliance, Controles Internos e demais áreas de especialização, reciclando seus conhecimentos de acordo com a legislação em vigor. Adicionalmente, mantemos campanhas regulares de conscientização abordando temas como práticas seguras, engenharia social, phishing e outros.

Gerenciamento de operações

Nosso ambiente de aplicações usa um modelo de rede de três camadas para servidores voltados ao assinante e usa diversas camadas para os nossos servidores de aplicação com uma abordagem em camadas com redundância de firewalls e sistemas de proteção contra intrusos (IDS/IPS). Os Firewalls são configurados para permitir apenas o tráfego de rede necessário para realizar negócios e as regras são validadas periodicamente.
Todas as conexões da rede são aprovadas, documentadas e rastreadas. Nossa rede foi desenhada para assegurar uma arquitetura segura, com segregação e redundância adequada. Os componentes da rede são configurados de forma segura (hardening) e implementados com serviços desabilitados, componentes removidos e senhas padrão alteradas.

Programa de Desenvolvimento Seguro

A Serasa Experian possui controles para reduzir as vulnerabilidades em aplicações e construí-las de maneira segura. Todos os desenvolvedores são obrigados a realizar treinamentos de segurança de aplicações. Todas as nossas aplicações passam por avaliações de segurança adequadas ao seu perfil de risco antes de entrar em produção. Essas avaliações incluem teste estático (teste do código em si), teste dinâmico (a aplicação é sujeita a tentativas de exploração através de teste de penetração) e teste manual (uma pessoa age como um hacker para garantir que a aplicações não está sujeita a invasão/abuso).

Os testes de aplicações consistem em testes de segurança de aplicações estáticas (SAST), análise de composição de software (SCA), testes dinâmicos de segurança de aplicações (DAST) e testes de penetração de aplicações (APT).

Com base no risco, a Experian realiza:
• Teste de segurança de aplicações estáticas (Static Application Security Testing, SAST).
• Análise da composição do software (Software Composition Analysis, SCA).
• Teste dinâmico de segurança de aplicações (Dynamic Application Security Testing, DAST).
• Teste de penetração de aplicação (Application Penetration Testing, APT).
• Varredura de infraestrutura.
• Teste de penetração de rede (Network Penetration Testing, NPT).
Problemas identificados são relatados ao negócio para garantir que sejam fechados dentro dos prazos acordados para reduzir o risco de acesso não autorizado a dados e sistemas.

Os ambientes de desenvolvimento, testes e produção são segregados e controlados através de processos documentados de Gestão de Mudanças, que inclui aprovação de todas as partes interessadas, avaliação de impacto das mudanças e controle de versões.

Gerenciamento de Vulnerabilidades

Nosso ambiente é avaliado periodicamente baseado na Política de Segurança Global da Experian. Todas as vulnerabilidades identificadas são classificadas de acordo com a sua criticidade e possuem um prazo limite para correção (de acordo com as melhores práticas de mercado). Firewalls, roteadores, servidores, PCs e todos os outros recursos serão mantidos atualizados com os patches de segurança apropriados.
Realizamos regularmente teste de penetração na nossa infraestrutura e todas as vulnerabilidades de detectadas são gerenciadas em um sistema específico (datawarehouse). O

resultado do processo é apresentado nos comitês executivos de risco local e global para acompanhamento das ações e gerenciamento dos riscos.

Controle de Acesso

A Serasa Experian possui controles robustos para restringir o acesso aos nossos sistemas e proteger os dados dos nossos clientes. Todos os usuários possuem um identificador exclusivo (ID) que possibilita a identificação e rastreabilidade individual. Nossos sistemas possuem recursos para Identificação, autenticação e autorização integrada. O nível de autenticação necessário para acessar qualquer recurso é proporcional à sensibilidade dos dados e ao nível de permissão de acesso autorizado, sendo eles solicitados por meio do IDC (Identity Central), plataforma onde é feito o gerenciamento de acesso a ferramentas e softwares dentro da companhia. O acesso a contas privilegiadas é restrito apenas aos usuários que administram os recursos, bem como as senhas, que são gerenciadas através de solução PAM (Privileged Access Management). Utilizamos do princípio "privilégio mínimo", onde apenas o pessoal autorizado possui o nível de acesso aos recursos necessários para desempenhar suas funções de trabalho.

Todos os acessos que se conectam na nossa rede possuem MFA (Fator duplo de autenticação) – Cisco Anyconnect Secure Mobility Client e Token via OKTA.

As senhas dos usuários são configuradas com regras de complexidade e, todos os acessos são revisados periodicamente e monitorados através de ferramentas especificas, considerando controles de segregação de funções e comportamento.

Integridade de Dados

A Serasa Experian protege a confidencialidade e a integridade dos dados de nossos clientes que são transmitidos através de sua rede. Todas as informações Experian são criptografadas com técnicas de criptografia forte (onde a criptografia em repouso é utilizado o padrão AES-256 e a criptografia em transito utilizamos o protocolo TLS 1.2+) e implementamos um programa de prevenção de vazamento de dados baseado em ferramenta DLP que controla todas as saídas de dados (internet, e-mail, cloud, portas USB e demais end-points) através de regras definidas por comitês locais e globais para proteção das informações de acordo com a Política de Segurança da Informação.

Ambiente Cloud

A Experian utiliza uma solução de segurança nos seus ambientes de nuvens centralizados chamados Experian Express Cloud (EEC). Todos os ambientes em Cloud são configurados em conformidade com padrões rígidos de segurança e são monitorados. Essa ferramenta possibilita o monitoramento, criação e correção automática de configurações incorretas em todas as contas vinculadas ao EEC. O EEC possui imagens de servidores em nuvem já configuradas e prontas para serem criadas de acordo com os requerimentos de segurança padrão da Experian, permitindo aos usuários, modelar, provisionar e gerenciar recursos da AWS e de terceiros tratando a infraestrutura como código.

Através do EEC, controlamos diversos recursos, entre eles: criptografia ativa no EBS das instâncias EC2, MFA para usuários root, acesso de somente leitura ao bucket S3, acesso ao banco de dados RDS, AWS CloudTrail e CloudTrail Lake habilitado. Regras de segurança e acesso também são configuradas por padrão no EEC, algumas delas são relacionadas ao nível de acesso via RBAC, exemplos: acesso de somente leitura as informações sensíveis no S3 e banco de dados, acesso somente de visualização aos serviços e recurso, recursos de acesso ao RDS restrito ao time de Banco de Dados (infraestrutura). Além disso seguimos todos os requerimentos de segurança padrão recomendados pelos principais provedores do mercado.

Na Experian, a segurança em nuvem tem estado na vanguarda para manter nossos ambientes em nuvem em conformidade com os padrões corporativos de Segurança e disponibilidade.

Registro e Monitoramento das Operações

Todos os sistemas possuem mecanismos de registro ativos de log para identificar comportamentos suspeitos, acessos não autorizados, eventos relacionados ao sistema (alteração e/ou inclusão de contas) entre outros, que permitam estabelecer responsabilidade e reconstruir eventos.

Os logs de auditoria são mantidos em um estado protegido e seguro com revisão periódica para detectar quaisquer ações que possam comprometer a segurança dos nossos sistemas (SIEM Splunk). Os registros são mantidos por um período mínimo determinado por lei ou definidos em contrato.

Proteção contra vírus

A Serasa Experian possui sistemas antivírus/antimalware para proteger todos os computadores da nossa rede, além de sistemas de detecção de vírus em todos os mecanismos de troca de dados. A atualização de assinaturas de antivírus é realizada diariamente.

Segurança Física

Os Datacenters são protegidos e monitorados 24/7, com monitoramento de imagens do interior, estacionamentos e todo perímetro. O acesso às instalações é restrito com controle de acesso eletrônico. Os acessos são restritos apenas a pessoas autorizadas e com justificativa de acesso. Áreas altamente restritas são protegidas com controles de acesso adicionais tais como CFTV, leitoras de cartão magnético e controle de acesso biométrico. Todos os acessos são registrados em trilhas de auditoria e são revisados periodicamente.

Gestão de Resposta a Incidentes

A Serasa Experian possui processos e procedimentos para responder a violações de segurança, eventos e incidentes incomuns ou suspeitos limitando danos aos ativos de informações e que, permitem a identificação e processos de investigação forense.

Nosso plano de resposta a incidentes, procedimentos e normas estão de acordo as melhores práticas de mercado. Temos processo de monitoramento dos controles de segurança, correlacionando as informações apresentadas e tratando os incidentes tão logo sejam detectados. Também contamos com um canal para reporte de incidentes que passam por um processo de triagem, avaliação e tratamento.

Continuidade de Sistemas e recuperação de desastres

Possuímos um Plano Continuidade de Negócios que inclui estratégias, planos e procedimentos de recuperação documentados para garantir que os produtos e serviços estejam disponíveis dentro dos prazos definidos em contrato.
A estratégia de recuperação e infraestrutura é testada e revisada regularmente para assegurar a eficiência do Plano e que novas tecnologias são constantemente incorporadas no planejamento.

Os procedimentos de backups dos diversos sistemas são executados ao final de cada ciclo de processamento, obedecendo a frequência de cada ciclo. O prazo de retenção é definido para cada aplicação de acordo com o contrato, legislação vigente e seguindo as melhores práticas confirme orientação do fabricante. Os backups são realizados de forma online e incremental.
Os backups de databases atualmente são executados de forma Online, Offline, Full, Diferencial e Incremental. Realizamos backups de diversas plataformas incluindo: Oracle, Microsoft SQL Server e IBM DB. Os backups de máquinas virtuais serão realizados através do software de backup - IBM Spectrum Protect Plus