UNIVERSO AMERICANAS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Estabelecer os princípios, diretrizes e regulamentos que compõem a Política de Segurança da Informação, a fim de garantir o tratamento seguro das informações dos dados e comunicações do Universo Americanas.

2. Campo de Aplicação

Compreende o Universo Americanas, SEDE, Centros de Distribuição, Data Center, Lojas em âmbito nacional, seus associados, informações, ativos de informação e meios de comunicação, assim como seus processos administrativos, organizacionais e finalísticos bem como empresas parceiras.

3. Definições

- **Ativos**: Tudo aquilo que tem valor para o Universo Americanas.
- **Ativos de informação**: Todo e qualquer recurso que processe, manipule, armazene, transporte, transmita e descarte dados e informações que tenham valor para o Universo Americanas e precise ser protegido (por exemplo: computadores, servidores, banco de dados, smartphones, sistemas, ambientes e processos de trabalho, armários e arquivos).
- **Autenticidade**: Garantia da identificação do responsável por uma determinada ação. Desta forma é possível assegurar o não-repúdio quanto a ação executada, onde e quando a mesma foi ocorrida.
- **Ciclo de vida da informação**: É o ciclo formado desde a criação ou obtenção da informação, passando por seu uso, manipulação, compartilhamento, armazenamento, transporte e descarte.
- **Classificação da informação**: Processo caracterizado pela definição de um grau de sigilo da informação e os grupos de acesso à mesma. Visa assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização.
- **Associado**: Empregado, colaborador, estagiário, fornecedor, prestador de serviço, estatutário ou agente econômico, que tenha acesso a informações ou recursos do Universo Americanas.

- **Comissão Estratégica de Segurança da Informação**: Grupo de pessoas, do Universo Americanas, com a função de atuar como fórum para o debate, troca de informações e tomada de decisões.
- **Confidencialidade:** Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
- **Disponibilidade**: Propriedade de estar acessível e utilizável, sob demanda, por uma entidade autorizada, quando necessário.
- **Documento**: Conjunto de informações ou instruções dispostas de forma ordenada, podendo estar na forma física ou eletrônica. Quando em forma eletrônica é também chamado "Documento Digital".
- **Evento de segurança da informação**: Ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
- **Gestão documental**: Conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando sua eliminação ou recolhimento para guarda permanente.
- **Incidente de segurança da informação**: Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
- **Informação**: É o conjunto de dados relacionados entre si que levam à compreensão de algo e que trazem um determinado conhecimento, podendo estar na forma escrita, verbal ou de imagem e em meio digital ou físico. É considerada um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida.
- **Integridade**: Garantia de que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.
- **Nível de classificação**: Categoria a ser definida para cada informação ou classe de informação. Estabelece a sensibilidade da informação em termos da preservação de sua confidencialidade.
- **Proteção de dados pessoais (privacidade)**: Possibilidade que cada associado ou cliente determinar de forma autônoma a utilização que é feita de seus próprios dados pessoais em conjunto com o estabelecimento de garantias, para evitar que sejam utilizados de forma a causar discriminação, ou danos de qualquer espécie.

- **Proprietário da informação**: Pessoa responsável por assegurar que as informações e os ativos associados com os recursos de processamento da informação estejam adequadamente classificadas, realizando periodicamente análises críticas das classificações e restrições de acesso, levando em conta as políticas de controle de acesso aplicáveis.
- **Segurança da informação e comunicações**: Garantia de preservação da confidencialidade, disponibilidade, integridade e autenticidade da informação existente em quaisquer formas ou suportes, tais como impressa, armazenada ou transmitida por meio físico ou eletrônico, ou ainda, divulgada em meio áudio visual, ou falada em conversação.
- **Tratamento da informação**: Conjunto de ações referente ao estabelecimento de diretrizes de proteção da informação em função do seu nível de classificação, envolvendo: a produção, recepção, utilização, acesso, reprodução, transporte, transmissão, distribuição, destinação, arquivamento, armazenamento e eliminação da Informação.
- **Tratamento seguro da informação**: Tratamento da informação levando em consideração os critérios de Disponibilidade, Integridade, Confidencialidade e Autenticidade.
- **Universo Americanas**: Engloba Lojas Americanas, B2W Digital e todas as demais empresas a elas relacionadas, como controladas diretas e indiretas, e se aplica individualmente a qualquer das empresas que compõem o mesmo Grupo Econômico
- **Usuário**: Pessoa autorizada a interagir com a informação. A definição do acesso deve ter como base a necessidade de conhecer a informação para a adequada execução das tarefas inerentes ao seu cargo ou função.

4. Conteúdo do Padrão

4.1. Atribuições e responsabilidades

4.1.1. Comissão Estratégica de Segurança da Informação (CESI)

O Comissão Estratégica de Segurança da Informação das Lojas Americanas e Comissão Estratégica de Segurança da Informação da B2W Digital são coordenadas pelas respectivas áreas de segurança de cada Companhia e constituído minimamente por associados nomeados das áreas como: Gerente Executivo de Segurança da Informação de Lojas Americanas e B2W Digital e Diretores Estatutários de Tecnologia das Companhias, podendo ainda utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

4.1.1.1. Deverá a CESI reunir-se formalmente pelo menos uma vez a cada seis meses, sendo que reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o Universo Americanas.

Cabe à CESI (Comissão Estratégica de Segurança da Informação):

4.1.1.2. Propor atualizações deste documento, revisar e validar os documentos complementares, que tratem da segurança da informação, buscando a melhoria contínua das diretrizes sobre segurança da informação no Universo Americanas;

4.1.1.3. Propor investimentos relacionados à segurança da informação visando a redução de riscos de segurança e conscientização dos associados;

4.1.1.4. Decidir sobre os incidentes de segurança, reportados pelo gestor de segurança da informação;

4.1.1.5. Prestar suporte na elaboração de documentos complementares a esta Política, sobre classificação, guarda e manutenção da informação;

4.1.1.6. Definir as medidas cabíveis nos casos de descumprimento da Política;

4.1.1.7. Difundir a cultura de Segurança da Informação no Universo Americanas;

4.1.1.8. Reportar ao Comitê de Auditoria formalmente, pelo menos uma vez ao ano, sobre o resultado das reuniões da CESI.

4.1.2. Comitê de Auditoria

O Comitê de Auditoria é responsável por:

4.1.2.1. Acompanhar periodicamente a atuação e resultados da CESI;

4.1.2.2. Definir as diretrizes e propor melhorias na Política de Segurança da Informação;

4.1.2.3. Reportar ao Conselho de Administração sobre as questões de Segurança da Informação pelo menos uma vez ao ano.

4.1.3. Conselho de Administração

O Conselho de Administração é responsável por:

4.1.3.1. Aprovar a Política de Segurança da Informação das Lojas Americanas e B2W Digital;

4.1.4. Diretoria Executiva e Estatutária

A Diretoria é responsável por:

4.1.4.1. Prover os recursos humanos, materiais e financeiros necessários à segurança da informação e comunicações;

4.1.4.2. Acompanhar periodicamente a evolução dos indicadores e resultados de segurança da informação.

4.1.5. Gestor de Segurança da Informação

O Gestor de segurança da informação é responsável por:

4.1.5.1. Responder, perante a Diretoria, por todos os aspectos de segurança e gestão de riscos da Companhia em relação à Segurança das Informações;

4.1.5.2. Responder por todos os eventos de segurança da informação (físicos ou eletrônicos) e todas as perdas resultantes dos riscos não geridos ou não previstos;

4.1.5.3. Liderar a elaboração da Política Corporativa de Segurança da Informação, bem como os anexos necessários para a adequação dos ativos ao nível de Segurança pertinente ao bom desenvolvimento do negócio;

4.1.5.4. Buscar e apoiar iniciativas de Segurança da Informação aplicáveis a todo o Universo Americanas, como, por exemplo, o programa de conscientização de segurança, governança da informação e gestão de identidades digitais;

4.1.5.5. Garantir que a segurança seja parte do processo de planejamento da informação;

4.1.5.6. Apoiar e validar as auditorias externas de Segurança da Informação realizadas por clientes ou órgãos reguladores;

4.1.5.7. Manter contatos apropriados com autoridades relevantes, grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais;

4.1.5.8. Coordenar as reuniões de trabalho do grupo técnico/operacional no tratamento de incidentes de segurança;

4.1.5.9. Avaliar os incidentes de segurança da informação e propor ações corretivas, incluindo o direcionamento dos mesmos para a Comissão Estratégica de Segurança da Informação, quando aplicável;

4.1.6. Gestor de área

O Gestor de área é responsável por:

4.1.6.1. Assegurar que Política de Segurança, regulamentos e procedimentos do Universo Americanas sejam implantadas e mantidas de acordo com os preceitos definidos para a sua área de atuação.

4.1.7. Associados

Os associados são responsáveis por:

4.1.7.1. Conhecer e cumprir as diretrizes estabelecidas nesta Política, bem como as boas práticas que contribuem para a segurança da informação e comunicações no Universo Americanas.

4.1.7.2. Administrar os recursos, processos de negócios e informações sob sua responsabilidade conforme as diretrizes desta Política.

4.2. Princípios de segurança da informação e comunicações

As ações de Segurança da Informação e Comunicações no Universo Americanas são norteadas pelos seguintes princípios:

4.2.1. **Alinhamento estratégico**: deve haver um alinhamento entre a Política, regulamentos e ações de Segurança da Informação e Comunicações do Universo Americanas com a missão das Companhias e seu planejamento estratégico.

4.2.2. **Diversidade organizacional**: a elaboração de regulamentos, controles e da Política de Segurança da Informação e Comunicações do Universo Americanas deve levar em consideração a diversidade das atividades de cada Companhia, respeitando a natureza e finalidade de cada Unidade Organizacional.

4.2.3. **Propriedade da informação**: toda informação produzida ou armazenada no Universo Americanas são de sua propriedade e não de seus Associados, Estatutários e Prestadores de Serviço, exceto os casos onde a Companhia atua como custodiante da informação, devendo seu uso ser destinado, exclusivamente, a atender os interesses do Universo Americanas.

4.3. Diretrizes de segurança da informação e comunicações

Para fins desta Política ficam estabelecidas as seguintes diretrizes gerais:

4.3.1. A Segurança da Informação do Universo Americanas deve ser apoiada por um Sistema de Gestão da Segurança da Informação e Comunicações (SGSI).

4.3.2. Devem ser definidas métricas e indicadores que permitam controlar, auditar e elevar o nível de maturidade e conformidade do Universo Americanas em segurança da informação.

4.3.3. Comprometimento: Todos os Associados, Estatutários e Prestadores de Serviço do Universo Americanas, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda dos ativos tecnológicos e informações de que sejam usuários, dos ambientes físicos e computacionais a que tenham acesso, respeitando as Políticas e mecanismos de controle e proteção implantados.

4.3.4. Gestão de Riscos: Todos os processos, produtos e serviços desenvolvidos, que possam comprometer a segurança da informação, devem ser submetidos a um processo formal de análise, avaliação e tratamento de riscos, antes da sua aquisição, implementação e disponibilização, visando atingir o grau de segurança adequado para o Universo Americanas.

4.3.5. Gestão de Continuidade de Negócio: o Universo Americanas deve estabelecer um conjunto de estratégias e planos de ação documentados, testados e revisados periodicamente, de maneira a garantir que os seus serviços essenciais sejam devidamente identificados, preservados e entregues, mesmo diante da ocorrência de um desastre até o retorno à situação normal de funcionamento da Companhia.

4.3.6. Classificação e Tratamento da Informação: Todas as informações e os respectivos recursos tecnológicos que as suportam devem ser classificadas de acordo com seu grau de sigilo e receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida.

4.3.7. Gestão de Acessos: O acesso aos ambientes físicos e lógicos do Universo Americanas deve ser controlado, registrado e monitorado, com base nos princípios da necessidade de conhecer e do privilégio mínimo para o desempenho das atividades profissionais.

4.3.8. Gestão de Incidentes: Os Associados, Estatutários e Prestadores de Serviço do Universo Americanas têm a obrigação de reportar imediatamente quaisquer incidentes de segurança que tomaram conhecimento, de modo que possam ser registrados, avaliados e tratados.

4.3.9. Auditoria e Conformidade: O Universo Americanas reserva-se o direito de auditar periodicamente a prática de segurança da informação e comunicações, de forma a avaliar a conformidade das ações de seus Associados e Prestadores de Serviço em relação ao estabelecido pela Política de Segurança da Informação e Comunicações do Universo Americanas e pela legislação aplicável.

4.3.10. Monitoramento: O Universo Americanas reserva-se o direito de monitorar o acesso e utilização de seus ambientes físicos, assim como dos ambientes, equipamentos e sistemas tecnológicos, de forma que ações indesejáveis ou não autorizadas sejam detectadas proativamente.

4.3.11. Treinamento e Conscientização: Todos os Associados, Prestadores de Serviço e Estatutários devem conhecer esta Política e serem capacitados anualmente por meio de campanhas de conscientização e treinamentos de acordo com suas funções. Devem ter ciência desta Política e assinar o respectivo termo de aceite, garantindo assim maior efetividade e eficácia das ações de segurança da informação no Universo Americanas.

4.3.12. Gestão de exceções/procedimentos de escalação: As necessidades válidas do Universo Americanas decorrentes das suas operações podem eventualmente conflitar com algumas diretrizes estabelecidas nesta Política. Os procedimentos de gestão de exceções reconhecem que os conflitos de Políticas são naturais e que a Companhia tem maturidade suficiente para poder geri-los. Ao estabelecer procedimentos de gestão de exceções, os associados são encorajados a trabalhar com o sistema em vez de contorná-lo. Os gestores das áreas deverão ser consultados sobre os casos omissos para que sejam estabelecidos novos procedimentos para adequar as exceções.

4.3.13. Gestão de Mudanças: O Gerenciamento de Mudança deve garantir que os métodos e procedimentos sejam aplicados de forma correta para avaliar, aprovar, implantar e revisar todas as Mudanças de acordo com escopo estabelecido, de maneira eficiente, a fim de minimizar o risco e o potencial impacto de tais Mudanças para o negócio. Os processos e controles estabelecidos devem permitir a rastreabilidade das mudanças ocorridas em ambientes críticos do Universo Americanas.

4.3.14. Desenvolvimento Seguro: As aplicações desenvolvidas ou adquiridas pelo Universo Americanas, devem em todo o ciclo de desenvolvimento de sistemas utilizar metodologias que garantam a segurança das informações.

4.4. Privacidade

4.4.1. O Universo Americanas respeita a privacidade dos dados pessoais dos seus associados e clientes.

4.4.2. Em proteção à Privacidade, apenas dados necessários conforme finalidade ou legalmente exigidos para o desempenho eficaz da Companhia e cumprimento de obrigações legais são solicitados e retidos ou eventualmente divulgados em atendimento à legislação específica.

4.4.3. O Universo Americanas se reserva o direito de monitorar o uso de computadores, telefones fixos, smartphones, tablets, celulares, rádios e outros equipamentos disponibilizados e atividades de rede, incluindo, mas não se limitando a e-mail, correio de voz, uso da Internet e de qualquer informação armazenada em tais equipamentos, sistemas ou servidores, em circunstâncias apropriadas e com vista à proteção das informações e da segurança do tráfego de informação e conteúdo.

4.5. Aprovações, revisões e análises críticas

4.5.1. O conjunto de documentos que compõe a Política de Segurança da Informação e Comunicações do Universo Americanas deve passar por revisões anuais e análises críticas periódicas, ou sempre que ocorrer fato ou evento relevante que motive sua revisão antecipada.

4.6. Violações da política corporativa de segurança da informação

4.6.1. Em caso de violação desta Política, a área de Segurança da Informação deve ser imediatamente notificada e em segunda instância à Comissão Estratégica de Segurança da Informação.

4.6.2. O descumprimento das diretrizes previstas nesta Política é passível de sanções administrativas, conforme regimento interno da área de Recursos Humanos, e legais, conforme legislação vigente.

4.6.3. Nota: O não cumprimento pelo associado das diretrizes e regras estabelecidas (Políticas e Regulamentos de Segurança do Universo Americanas), seja isolada ou cumulativamente, poderá ensejar, de acordo com a infração cometida.

5. Referências

- ABNT NBR ISO/IEC 27001:2013
- ABNT NBR ISO/IEC 27002:2013
- CCS CSC 16
- COBIT 5
- ISA 62443-2-1:2009 e ISA 62443-3-3:2013
- NIST SP 800-53 Rev. 4
- Código de Ética e Conduta
- LGPD (Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018)

- PCI DSS

6. Anexos

6.1. Termo de Ciência Individual de Compromisso e Confidencialidade

- LASA-TER-SI-01 - Termo - Segurança da Informação

6.2. Regulamentos de Segurança da Informação:

- LASA-REG-SI-001 Acesso à Internet
- LASA-REG-SI-002 Classificação e Tratamento da Informação
- LASA-REG-SI-003 Controle de Acesso
- LASA-REG-SI-004 Desenvolvimento Seguro
- LASA-REG-SI-005 Gestão de Incidentes de SI
- LASA-REG-SI-006 Gerenciamento de Risco
- LASA-REG-SI-007 Uso de dispositivo móvel
- LASA-REG-SI-008 Utilização do Correio Eletrônico
- LASA-REG-SI-009 Auditorias Internas de SI
- LASA-REG-SI-010 Gestão de Mudança

7. VIGÊNCIA

Esta política entra em vigor na data da sua publicação.