Extrato da Política de Segurança da Informação

Público
Versão Extrato 1.0 (EV1.0)

Histórico de revisões

Versão	Data	Autor	Alterações

1. Visão geral e Objetivo

1. Introdução

A Seabras Group, LLC e suas subsidiárias (coletivamente, "**Seaborn**", "nós", "nosso", "nossos"), incluindo a Seabras 1 USA, LLC ("SB US"), a Seabras 1 Brasil Ltda. ("SB BR") e a Seaborn Management, LLC ("SB Management"), mantêm um Programa de Segurança da Informação ("**Programa de SI**") abrangente projetado para proteger nossos ativos de dados e tecnologia em ambientes operacionais e de backoffice ("**Ativos DIT**"). Construído em uma abordagem de "segurança por design", o programa é baseado na Política de Segurança da Informação ("**ISP")** da Seaborn e documentos relacionados.

A ISP se aplica a todos os empregados e consultores independentes e se alinha com normas técnicas reconhecidas (por exemplo, NIST CSF e ISO/IEC 27001), ao mesmo tempo em que aborda as leis e regulamentos aplicáveis de proteção de dados e telecomunicações nos Estados Unidos e no Brasil, incluindo a Lei Geral de Proteção de Dados ("**LGPD**") do Brasil (Lei Federal nº 13.709/2018) e as regras relevantes da Federal Communications Comission ("**FCC**") e da Agência Nacional de Telecomunicações ("**ANATEL**").

Este Extrato da Política de Segurança da Informação ("**Extrato**") fornece informações importantes sobre as práticas de segurança da informação e segurança cibernética da Seaborn, a fim de promover a confiança entre a Seaborn e seus clientes.

A qualquer momento a Seaborn pode atualizar a ISP e este Extrato para refletir as mudanças em suas práticas e/ou em requisitos legais.

2. Objetivo

O objetivo da Política de Segurança da Informação é definir os princípios e controles que regem a segurança da informação e a segurança cibernética nas operações da Seaborn. Ela estabelece medidas para proteger nossos Ativos DIT, preservando a confidencialidade, integridade e disponibilidade das informações, incorpora uma abordagem de segurança por design com melhoria contínua e define processos e responsabilidades para identificar, avaliar e responder a Incidentes e riscos de segurança da informação. A Política apoia a conformidade com as leis de proteção de dados aplicáveis, incluindo a LGPD, e as obrigações relevantes de telecomunicações, incluindo os regulamentos do FCC e da ANATEL.

3. Aplicabilidade

A ISP se aplica a todos os empregados da Seaborn e a todos os consultores independentes contratados, que devem ler, entender e cumprir a ISP e relatar violações reais ou suspeitas por meio dos canais estabelecidos pela Seaborn. A Política também se aplica a todos os Ativos DIT da Seaborn entre os ambientes operacionais e corporativos.

4. Referências

- Framework de Segurança Cibernética 2.0 do NIST (NIST CSF).
- ABNT NBR ISO/IEC 27001:2022 — Sistemas de Gestão de Segurança da Informação (SGSI).
- Lei Geral de Proteção de Dados (LGPD) do Brasil.
- Resolução ANATEL nº 740/2020, alterada pela Resolução nº 767/2024.

- Regras da Comissão Federal de Comunicações dos EUA relacionadas à Lei de Licença de Aterrissagem de Cabos (*Cable Landing License Act*).
- Publicação Especial NIST 800-88 Revisão 1 - Diretrizes para Sanitização de Mídia.

A ISP pode ser atualizado para refletir as alterações nessas fontes e nos requisitos legais ou regulamentares aplicáveis.

5. Responsabilidades

O Comitê de Gerenciamento de Riscos Corporativos ("**ERMC**") da Seaborn supervisiona o Programa de Segurança da Informação, definindo e mantendo políticas, coordenando a identificação e avaliação de riscos, garantindo controles e auditorias apropriados e governando a segurança do fornecedor e da cadeia de suprimentos.

A Equipe de Resposta a Incidentes de Segurança da Informação (**"ISIR")** coordena a prontidão e o tratamento de Incidentes, incluindo avaliação, correção e comunicações com as partes interessadas de acordo com os deveres legais e regulamentares.

Os empregados devem conhecer e seguir a ISP, proteger os Ativos DIT da Seaborn, manter suas credenciais seguras, usar apenas ferramentas autorizadas e prontamente relatar Incidentes suspeitos ou reais, bem como pontos fracos; os Consultores Independentes têm obrigações equivalentes quando contratados pela Seaborn. Todos os empregados são legalmente obrigados a cumprir a ISP.

Os Encarregados de Proteção de Dados ("**DPOs**") atuam como canal de comunicação com os titulares dos dados e autoridades e orientam o cumprimento das leis de proteção de dados aplicáveis.

[DPO Global/USA: Lin Gentemann

DPO Brasil: Beatriz Miranda].

6. Contato

Para assuntos urgentes relacionados à conformidade regulatória, entre em contato com: ISP@seabornnetworks.com.

Incidentes suspeitos de segurança da informação devem ser comunicados a: incident@seabornnetworks.com.

7. Treinamento e Conscientização

A Seaborn realiza treinamentos obrigatórios de segurança da informação e proteção de dados para todos os empregados e consultores independentes, com módulos adicionais para funções que exigem conhecimento técnico ou jurídico mais profundo. O treinamento pode ser ministrado pessoalmente ou online e aborda a importância da segurança, requisitos aplicáveis de privacidade e telecomunicações, ameaças comuns (incluindo *phishing* e engenharia social), as responsabilidades de cada indivíduo, entre outros. O treinamento é realizado de forma recorrente e os registros de conclusão podem ser fornecidos às autoridades quando necessário.

8. Notificação de Incidentes de Segurança

O ISIR da Seaborn coordena notificações para partes interessadas internas e externas quando um Incidente é identificado, de acordo com as leis aplicáveis de proteção de dados e telecomunicações. A equipe do ISIR trabalha com o ERMC, o departamento jurídico e a equipe de privacidade do Brasil para garantir relatórios oportunos às autoridades e outras partes interessadas, conforme exigido pelas leis de proteção de dados e telecomunicações, e mantém um registro de Incidentes. Empregados e consultores independentes devem

prontamente relatar Incidentes suspeitos por meio dos canais estabelecidos e não devem divulgar informações sobre Incidentes a terceiros, a menos que autorizados.

9. Informações Importantes sobre Processos de Segurança

A ISP da Seaborn estabelece processos e procedimentos de segurança da informação para garantir que os Ativos DIT estejam devidamente protegidos. Eles incluem, sem limitação:

- **Conformidade de empregados e consultores independentes.** Procedimentos de ciclo de vida para admissão de pessoal, mudanças de função e rescisões, incluindo verificação de antecedentes, conforme aplicável. Garante que o acesso seja alinhado às alterações de função e removido na saída.
- **Uso aceitável de Ativos DIT.** Requisitos de uso aceitável para Ativos de DIT da empresa, incluindo conformidade com a lei e com contratos de licenciamento, incluindo proibições de uso indevido. Estabelece normas para o uso responsável do e-mail e outras comunicações eletrônicas.
- **Classificação e Organização de Ativos.** Procedimentos sobre como os ativos de informação e tecnologia são identificados, classificados e organizados em toda a empresa. Oferece suporte à proteção consistente em todo o ciclo de vida dos dados/ativos.
- **Tipos de Dados e Níveis de Confidencialidade.** Classificação de categorias de dados como Dados Confidenciais, Dados Pessoais e Dados Públicos, com expectativas de tratamento em alto nível.
- **Funções e Responsabilidades para Ativos de TI e Propriedade de Dados.** Definições sobre proprietários de dados e grupos de dados para esclarecer as responsabilidades de propriedade (classificação, expectativas de retenção/disponibilidade e governança relacionada).
- **Registro de Atividades de Processamento (ROPA).** Requer a manutenção de uma mapeamento de dados ou ROPA em conformidade com a LGPD e a manutenção de diagramas de rede e fluxo de dados atuais.
- **Controles de Acesso à Informação.** Implementa acesso baseado em privilégios mínimos e função, aprovações documentadas para acesso a Dados Confidenciais, revisões periódicas de acesso e auditabilidade de alterações.
- **Coleta, Manuseio e Transmissão de Dados.** Requer minimização de dados, coleta de fontes confiáveis, manuseio cuidadoso e transmissão limitada de Dados Confidenciais/Pessoais, aplicando criptografia quando transmitidos eletronicamente. Incentiva canais seguros e práticas de comunicação seguras quando necessário.
- **Prevenção de Perda de Dados**. Estabelece controles técnicos e processuais para prevenir e detectar a exfiltração de dados (por exemplo, proteções e monitoramento de dispositivos/mídias).
- **Política de E-mail.** Define regras internas sobre autenticidade do remetente de e-mail e de uso de e-mail para reduzir a falsificação e o uso indevido.
- **Filtragem da Web.** Define controles de filtragem da Web para restringir o acesso a sites inseguros ou inadequados e reduzir o risco de malware.
- **Senhas.** Estabelece práticas de criação e proteção de senha, desencorajando sua reutilização ou seu compartilhamento. Enfatiza que os sistemas devem ser bloqueados quando não estejam em uso.
- **Gerenciamento de Configurações.** Estabelece procedimentos de gerenciamento de mudanças e interconexão para que as mudanças sejam autorizadas, testadas e auditáveis.

- **Segurança de Rede**. Requer proteção de perímetro, segregação de conexão de rede sem fio (wireless) de convidados e autenticação forte para qualquer conexão de rede interna sem fio.
- **Gestão de Ativos.** Requer identificação, classificação e inventário de Ativos DIT, incluindo aqueles hospedados por terceiros.
- **Registro e Monitoramento.** Requer a manutenção e a revisão da auditoria de logs de atividades dos usuários, exceções e eventos de segurança.
- **Hardware/Software Não Autorizado (Shadow IT).** Proíbe a instalação ou o uso de software ou hardware não aprovado e requer aprovação centralizada para solicitações de software e aceitação de termos de licença.
- **Resposta de Alerta.** Define o processo para triagem e resposta a alertas de segurança e escalonamento para tratamento de Incidentes quando apropriado.
- **Auditoria de Segurança e Testes de Rede.** Prevê auditorias periódicas de segurança, varredura de vulnerabilidades e testes de penetração, bem como monitoramento para detectar atividades maliciosas e para acompanhamento de correção.
- **Gestão de Riscos dos Dados Pessoais do Titular dos Dados do Brasil e Privacidade por Design.** Estabelece avaliação de risco para o processamento de Dados Pessoais no Brasil e articula as expectativas de privacidade por design em projetos e operações.
- **Ativos de TI Hospedados/Em Nuvem.** Define controles de linha de base para serviços hospedados na nuvem (por exemplo, registro/monitoramento, privilégios mínimos, autenticação multifator, proteção de dados, proteção, aplicação de patches, avaliação de vulnerabilidade).
- **Proteção de Dispositivos Móveis e Laptops.** Requer inventário de dispositivos, registro de gerenciamento de dispositivos móveis, criptografia de disco completo, bloqueios de inatividade e proteções em pontos de extremidade (*endpoint*) relacionadas.
- **Proteções de Estação de Trabalho.** Requer proteções de *endpoint* em estações de trabalho corporativas, proíbe o uso de dispositivos pessoais para o trabalho da empresa e exige *patches* e defesas contra malware.
- ***Patching*.** Define o processo para aplicar correções de segurança e estabilidade a sistemas e aplicativos de maneira oportuna e controlada.
- **Segurança Física.** Estabelece requisitos para controle de acesso físico a instalações e pontos de presença, incluindo procedimentos de visitantes e áreas restritas.
- **Segurança em Viagens.** Estabelece as expectativas de segurança de viagem e faz referência ao procedimento de aviso de viagem para viagens internacionais.
- **Solicitações do Titular dos Dados.** Exija que qualquer solicitação recebida do Titular dos Dados seja imediatamente encaminhada ao DPO dos EUA ou ao DPO BR, conforme aplicável; os Empregados não devem responder diretamente.
- **Uso Aceitável de Ferramentas de IA Generativa**. Proíbe o uso de dados da empresa com ferramentas públicas Inteligência Artificial Generativa (GenAI) sem aprovação prévia por escrito e define o que fazer/não fazer para uso seguro; reforça que os resultados do GenAI devem ser verificados e não tratados como privados.

10. Controle e Monitoramento

- **Governança e Controles Internos.** O ERMC estabelece, supervisiona e melhora continuamente os controles de segurança, coordenando testes, auditorias, correções e monitoramento de conformidade em todas as funções de risco e tecnologia. Também organiza equipes de apoio e fornece atualizações e recomendações para a liderança sênior.
- **Registro e Monitoramento.** O ERMC mantém registros de auditoria de atividades do usuário, exceções e eventos de segurança em Ativos DIT, capturando itens como atividade de autenticação, carimbos de data/hora, origem/local, acesso a ativos/dados, uso de privilégios elevados e parâmetros de rede relevantes. Os logs e relatórios de ativos voltados para o perímetro (*perimeter-facing assets*) são revisados periodicamente para detectar atividades suspeitas (por exemplo, acesso incomum, contas inativas, tentativas de login não autorizadas).
- **Revisão de Acessos e Alteração de Rastreabilidade**. O acesso a Dados Confidenciais/Pessoais segue o privilégio mínimo com aprovações documentadas; acesso privilegiado requer autorização reforçada. Revisões periódicas de acesso são executadas e as alterações de acesso devem ser auditáveis e relatadas por meio do processo de gerenciamento de alterações.
- **Triagem e Escalonamento de Alertas**. Os alertas de segurança dos controles de proteção são submetidos a triagem e, quando necessário, escalados para o tratamento de Incidentes. O processo considera possíveis invasões e impactos em Ativos de TI, dados, pessoal, clientes e fornecedores.

Auditorias de segurança, avaliação de risco e testes de rede. O ERMC realiza avaliações de risco de segurança e auditorias de Ativos DIT usando critérios definidos para avaliar ameaças, vulnerabilidades e a suficiência de controles, aplicando tratamento de risco (reduzir, reter, evitar, transferir, monitorar) e promovendo melhorias no Programa de SI. O ERMC também realiza testes de rede (incluindo varreduras internas/externas), verifica a correção de violações anteriores e usa os resultados para aprimoramento do processo.

11. Principais Definições

Os termos em maiúsculas usados neste Extrato têm o significado estabelecido abaixo, a menos que definido de outra forma pela lei de proteção de dados aplicável.

Termo	Definição
Ativos DIT	Todos os dados, sistemas, redes, aplicativos, equipamentos, infraestrutura e recursos tecnológicos utilizados pela Seaborn em seus ambientes corporativos e operacionais.
Comitê de Gerenciamento de Riscos Corporativos (ERMC)	O comitê responsável por supervisionar o Programa de Segurança da Informação da Seaborn, incluindo definição de políticas, identificação e mitigação de riscos, auditoria e segurança da cadeia de suprimentos.
Dados Confidenciais / Dados Pessoais / Dados Públicos	Categorias de classificação de informações que definem os requisitos de manuseio, armazenamento e transmissão de acordo com os níveis de confidencialidade e sensibilidade.

Termo	Definição
Encarregado de Proteção de Dados (DPO)	O indivíduo designado responsável por garantir a conformidade com as leis de proteção de dados aplicáveis, servindo como ponto de contato com os titulares dos dados e autoridades supervisoras e orientando as práticas relacionadas à privacidade.
Equipe de Resposta a Incidentes de Segurança da Informação (ISIR)	A equipe encarregada de preparar e responder a Incidentes de segurança da informação, incluindo avaliação de Incidentes, correção, comunicação e notificações regulatórias.
Incidente	Qualquer evento que comprometa, ou tenha o potencial de comprometer, a confidencialidade, integridade ou disponibilidade das informações da Seaborn ou dos Ativos DIT, incluindo acesso não autorizado, vazamento de dados, infecção por malware ou falha operacional.
Política de Segurança da Informação (ISP)	A política abrangente da Seaborn que define os princípios, controles e procedimentos que regem o gerenciamento de informações e segurança cibernética para preservar a confidencialidade, integridade e disponibilidade dos Ativos DIT.
Registro de Atividades de Processamento (ROPA)	Um registro exigido pela LGPD que documenta o processamento de Dados Pessoais, incluindo finalidades, bases legais, categorias de dados, compartilhamento e medidas de segurança aplicadas.