Política Corporativa de Segurança da Informação

Presidente Executivo

24 novembro 2025

CONTROLO DE VERSÕES

Versão	Data	Alterações
V1	31/07/2020	versão inicial
V2	28/04/2023	Adaptação à ISO/IEC 27001:2013
V3	17/04/2024	Adaptação à ISO/IEC 27001:2022
V4	28/03/2025	Adaptação à ENS RD 311/2022
V5	24/11/2025	Estão incluídos comentários relativos ao âmbito da OT na secção 3.

CONTEÚDO

1. Objeto

A Política Corporativa de Segurança da Informação tem como objetivo estabelecer e regular as disposições gerais e os princípios orientadores das questões de segurança da informação que dizem respeito à Empresa.

A URBASER reafirma a sua posição como empresa orientada para a sustentabilidade através da sua missão de contribuir para o desenvolvimento adequado das cidades e territórios através de serviços eficientes e tecnologia inovadora. Por isso, desempenha um papel relevante na proteção da atividade tecnológica, industrial e comercial no desenvolvimento e operação de infraestruturas críticas que prestam serviços essenciais à sociedade e às entidades e instituições públicas governamentais.

A URBASER deve estar perfeitamente preparada para intervir, reagir e proteger os seus ativos de informação perante incidentes de segurança que possam afetá-la, bem como para que todas as suas atividades e serviços estejam alinhados com as mais exigentes diretrizes locais e internacionais de segurança da informação.

Com a aprovação desta Política, a URBASER manifesta a sua determinação e compromisso em alcançar um nível de segurança da informação adequado às necessidades do negócio, que garanta a proteção dos ativos de forma homogénea em todo o Grupo.

2. Âmbito de aplicação

Esta Política é aplicável a todas as entidades participadas (sociedades, UTEs, Joint Ventures ou qualquer outra fórmula associativa) nas quais a URBASER, S.A.U. seja o sócio maioritário ou tenha o controlo (doravante, «URBASER») e é de cumprimento obrigatório para todos os utilizadores que participem na gestão, utilização ou exploração da Informação da URBASER, incluindo, mas não se limitando a conselheiros, diretores, funcionários, colaboradores, gerentes e membros dos órgãos de governo.

Nas entidades participadas nas quais esta Política não seja aplicável, será promovida, através dos seus representantes nos órgãos de administração, a alinhamento das suas próprias políticas com as da presente Política.

3. Conteúdo

A segurança da informação, um dos pilares fundamentais sobre os quais se constrói a URBASER, deve ser entendida como um conceito integral que tem como objetivo preservar os ativos e proteger os interesses e objetivos estratégicos da Empresa. Da mesma forma, a segurança da informação deve contribuir para preservar a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade dos dados dos clientes e outras partes interessadas.

Nesse sentido, a URBASER assume os seguintes objetivos:

- Alinhar a estratégia de segurança da informação com a estratégia de negócios da URBASER.
- Estabelecer uma boa governança da segurança da informação para garantir a sua correta gestão

e operação, de acordo com os requisitos aplicáveis na matéria (a legislação aplicável em vigor em cada país, os requisitos contratuais e as necessidades das partes interessadas).

- Fornecer os recursos necessários para atingir os objetivos estabelecidos.
- Identificar e, quando apropriado, avaliar e categorizar os riscos e oportunidades inerentes às atividades, processos e serviços, planeando as ações necessárias para o seu tratamento, prevenindo os efeitos indesejados e potenciando os efeitos favoráveis dos mesmos.
- Garantir a cadeia de abastecimento do ponto de vista da segurança da informação.
- Garantir que todo o pessoal, incluindo os colaboradores externos com acesso aos sistemas de informação da organização, tenha a cultura, formação, sensibilização e capacitação adequadas para o desenvolvimento das suas atividades de forma segura para si próprios e para os outros, garantindo em todos os momentos a segurança da informação
- Implementar as medidas de segurança necessárias para garantir a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade da segurança da informação ao longo de todo o seu ciclo de vida
- Gerir os incidentes de segurança da informação para minimizar o impacto e a probabilidade de ocorrência dos mesmos.
- Alinhar a estratégia de gestão da segurança da informação com a estratégia de continuidade dos negócios de TI e OT.
- Melhorar continuamente o sistema de gestão da segurança da informação, incentivando a participação ativa de toda a organização para promover e adotar medidas que conformem processos mais seguros e otimizados.

Para que as ameaças existentes na URBASER não se concretizem ou, caso se concretizem, não afetem gravemente nem as informações que ela gere nem os serviços prestados, as atividades de segurança da URBASER serão orientadas pelos seguintes princípios:

- **Eficiência:** será dada prioridade ao conhecimento das potenciais ameaças e dos riscos delas decorrentes, com o objetivo de antecipar a sua ação e evolução e preservar a Empresa dos seus potenciais efeitos prejudiciais, mitigando-os até um nível aceitável para o negócio.
- **Responsabilidade:** os utilizadores devem preservar a segurança dos ativos que a URBASER coloca à sua disposição, em conformidade com os critérios, requisitos, procedimentos e tecnologias de segurança definidos.
- **Legalidade:** será observado em todos os momentos o necessário cumprimento das leis e regulamentos em matéria de segurança, em vigor em cada momento em todos os territórios em que a URBASER opera.
- **Cooperação e Coordenação:** será dada prioridade à cooperação e coordenação entre todas as unidades de negócio e pessoal, para gerar as sinergias adequadas e reforçar as capacidades conjuntas.
- **Prevenção:** para prevenir e evitar que as informações ou os serviços sejam prejudicados por incidentes de segurança, a URBASER implementará as medidas de segurança determinadas pela normativa de segurança atualmente em vigor em cada país, bem como qualquer outro controlo adicional identificado através de uma avaliação de ameaças e riscos.

- **Deteção:** a operação dos sistemas e serviços será monitorizada continuamente para detetar anomalias nos níveis de prestação e agir em conformidade.
- **Resposta:** serão estabelecidos mecanismos para responder eficazmente a incidentes de segurança da informação.
- **Recuperação:** serão desenvolvidos planos de continuidade dos sistemas de Tecnologias da Informação e Comunicação (TIC) e dos sistemas de Tecnologias de Operação (OT).

A fim de cumprir a presente norma, as funções e responsabilidades em matéria de segurança da informação estão definidas na Normativa de Funções e Responsabilidades (NS-19-CORP), onde está definido o Comité de Segurança da Informação, órgão diretor da presente Política.

4. Formação

Serão promovidas as ações de formação e sensibilização necessárias para o conhecimento, implementação e acompanhamento da presente Política em matéria de segurança da informação.

5. Dúvidas, comunicações ou reclamações

As consultas no âmbito desta Política devem ser dirigidas à Área Corporativa de Cibersegurança da URBASER.

Qualquer incidente relacionado com o incumprimento do estabelecido nesta Política e procedimentos relacionados, ou a sua conformidade com o estabelecido no Código de Conduta do Grupo, deve ser dirigido ao órgão de conformidade regulamentar correspondente através do Canal Ético constante da página web do Grupo (https://www.urbaser.com/canal-etico/).

6. Incumprimentos

A presente Política é considerada uma norma de cumprimento obrigatório, pelo que a sua violação constituirá uma infração da mesma e a Empresa adotará as medidas disciplinares, contratuais ou legais que forem pertinentes, sem prejuízo de outras responsabilidades em que o infrator possa ter incorrido. Da mesma forma, a URBASER reserva-se o direito de adotar as medidas que considerar oportunas contra os parceiros comerciais que a infringirem. Qualquer exceção ou isenção, seja por motivos organizacionais, legais, contratuais, tecnológicos ou de outra natureza, a esta Política ou a qualquer norma, procedimento ou instrução técnica da qual ela dependa, será gerida de acordo com os documentos internos definidos para tal.

7. Revisão e atualização

O Comité de Segurança da Informação irá rever anualmente ou sempre que houver uma alteração substancial no contexto da organização, assegurando-se de que inclui as recomendações e melhores práticas internacionais de acordo com os requisitos normativos e a legislação aplicável. Também irá propor ao Órgão de Administração as modificações e atualizações que contribuam para o seu desenvolvimento e melhoria contínua.

www.urbaser.com