

SEGURANÇA DA INFORMAÇÃO – Destaques 2023

A segurança da informação é parte fundamental para a condução estratégica e operacional dos nossos negócios a fim de reduzir qualquer exposição aos riscos atrelados ao tema.

Nossa preocupação se estende aos negócios, dado que um ataque cibernético sobre o serviço de abastecimento de gás, por exemplo, pode afetar o fornecimento para clientes, hospitais e indústrias, causando grandes danos a sociedade.

Por isso, dedicamos um grande esforço no desenvolvimento de mecanismos de proteção dos dados e dos sistemas que gerem nossas operações.

A gestão dessa temática foi estruturada para integrar todas as nossas empresas.

O *Chief Information Security Officer* (CISO) atua de maneira matricial, reportando-se simultaneamente à Vice-Presidência Financeira e de Relações com Investidores enquanto colabora com os gerentes de Segurança da Informação (*Business Information Security Officer* - BISO) de cada uma das controladas.

A governança no tema consiste no reporte e no alinhamento frequente dos riscos identificados e na melhoria de processos juntos às empresas do portfólio em caráter tático. **Os reportes estratégicos são realizados mensalmente à Diretoria Executiva e trimestralmente apresentados ao Conselho de Administração, contribuindo para uma melhor gestão da segurança de informação e cibernética das nossas operações e para a proteção de dados, colocando a temática no centro da discussão estratégica da Companhia.**

O modelo atual de governança e operação consolida trazendo vários benefícios às empresas do grupo Cosan, como por exemplo, sinergia de custos operacionais, centro de inteligência de ameaças unificado, equipe multidisciplinar (técnicos, especialistas e interações com o negócio) e tecnologias. Nesse sentido, desenvolvemos estratégias, políticas, normas, formas de gerenciar risco e programas de educação (Programa Guardiã), de forma padronizada, que seja compatível e replicável para todas as empresas do portfólio.

Programa Guardiã

uma iniciativa institucional que traz a agenda da segurança da informação para o centro da empresa. Sua proposta é apresentar, discutir e introjetar conceitos e hábitos relacionados à segurança da informação em todas as pessoas que trabalham no Grupo.

Seguimos, em 2023, com nosso planejamento iniciado em 2021 com projeções estratégicas até 2025, com revisão anual buscando alinhamento as melhores práticas de mercado.

12

Testes de phishing

16

simulações de ataques cibernéticos e gestão de crise

98%

de adesão na Trilha de Conhecimento aplicada para todos os colaboradores

Nos últimos três anos não foram registrados incidentes e casos de vazamento de dados internos e por parte de terceiros.

Consolidamos nos negócios a operação de segurança da informação e cibernética para nossos ambientes operacionais e industriais (OT Security) junto com a implantação da fase 2 (expansão industrial). Também, com grande destaque no ano, o projeto de proteção de banco de dados teve sua primeira fase concluída, elevando a segurança e monitoramento 24x7 com foco em sistemas críticos que afetam as operações. **Conseguimos superar a nossa meta de 2023 e elevar a nossa maturidade para nível 3,3 (régua de 0 a 5 baseada no CMMI e Framework NIST), o que significa uma expressiva governança, com mais processos e controles críticos, testes e simulações de crises cibernéticas e gestão de vulnerabilidades com inteligência tecnológica, com aperfeiçoamento constante do monitoramento 24x7 com respostas à incidentes e ataques mais sofisticados.**

O Programa de Maturidade de Segurança prevê a avaliação independente anualmente.

A evolução no rating de maturidade de segurança é, inclusive, uma meta atrelada a remuneração variável de todos os colaboradores, incluindo as lideranças e executivos. Esse programa contempla os principais frameworks internacionais, tais como NIST-CSF, ISO 27001/2 e CIS Controls.

Guardião

A conscientização dos times e a identificação de possíveis tentativas de ataques são premissas fundamentais para suportar nossas medidas de proteção. **Ao longo do ano, foram realizadas ações e práticas de educação continuada, conscientização e engajamento para verificar o comportamento dos colaboradores em relação a links maliciosos e para munir o time de informação e cuidados com o tema, abrangendo situações do cotidiano (vida pessoal) e as ameaças mais conhecidas e direcionadas aos ambientes corporativos.**

O novo Guardião iniciou no segundo semestre de 2023 se estendendo como parte estratégica até 2025. Essa estratégia nasce com o propósito de inserir a iniciativa na agenda executiva, além de posicionar o Guardião como narrativa institucional e parte integral da segurança dos negócios, tendo os CEOs e executivos seniores dos negócios como os principais porta-vozes.