Política de Segurança da Informação

Objetivo

O Objetivo da Política de Segurança da Informação da Valecard é estabelecer as diretrizes para assegurar a integridade, confidencialidade, legalidade, autenticidade e disponibilidade das informações e definir as responsabilidades a serem seguidas para proteger os dados e informações da empresa.

Abrangência

As orientações desta Política aplicam-se a todos os colaboradores, estagiários e prestadores de serviços, pessoas físicas ou jurídicas que realizem qualquer tipo de tratamento dos dados e informações sensíveis à execução das atividades operacionais da organização.

Instruções Gerais

A Política de Segurança da Informação entra em vigor para implementar boas práticas de segurança e proteger os dados e informações da empresa de acordo com os requisitos normativos, legais e regulamentares aos quais estamos submetidos. Dessa forma esse documento é distribuído a todos os funcionários, prestadores de serviços e parceiros de negócios, de forma que todos estejam ativamente envolvidos na execução das diretrizes dessa política.

Diretrizes

Para garantir efetividade na proteção dos dados e informações, dispomos de programas e recursos que visam prevenir, detectar e reduzir as ameaças, constituindo matriz de riscos com suas respectivas classificações, tratamentos e acompanhamentos.
Prezamos pela qualidade e eficiência nos serviços internos de Recursos Humanos com regras voltadas para contratação consciente e humanizada, treinamentos e testes no processo de onboard de novos colaboradores, disseminação das políticas e código de conduta e ética bem como processos de controles de acessos físico e lógico.

Gestão de Ativos e Recursos de Tecnologia

Os dispositivos utilizados para as atividades diárias assim como os todos os recursos de infraestrutura são controlados e protegidos contra ataques, infecções e prevenção de vazamento de dados. Em todas as tecnologias de Software e Hardware são atribuídas regras de segurança com direitos e deveres de todos quanto ao seu uso correto.

Classificação e Gestão das Informações

A classificação da informação é realizada definindo os níveis de proteção que cada dado deve receber e é tratada e protegida seguindo critérios de confidencialidade, disponibilidade e integridade em conformidade com as leis regulamentos sobre o tema. As diretrizes de acesso às informações são definidas por essa política de forma que todos os colaboradores, terceiros e prestadores de serviço que acessam informações classificadas sigam as instruções de segurança e tratamento das informações.

Proteção de Dados e Privacidade

Estamos comprometidos em adequar continuamente nossas estruturas de forma a zelar e garantir a conformidade com as leis vigentes sobretudo à nova Lei Geral de Proteção de Dado

Gestão de Prestadores de Serviços de TI

As requisições de aquisição de produtos e serviços de processamento e armazenamento de dados e computação em nuvem seguem diretrizes de Política Específica e exigências regulamentares que garantem controle quanto à seleção de fornecedores bem como análise dos produtos e serviços oferecidos e da boa fé na conduta da execução dos serviços prestados.

Gestão de Identidade e Acessos Físicos e Lógicos

A Gestão de Identidade e Acessos (concessão, alteração, bloqueio, revogação e revisão), seguem as diretrizes de Política Específica que define os recursos, as permissões e regras de mínimo privilégio, e as operações que podem ser executadas mediante caracterização de perfis, identificação de área e cargo de atuação e a rastreabilidade efetiva dos acessos realizados.

A segurança física contempla mecanismos de proteção que abrangem desde o perímetro externo até o espaço interno de trabalho, bloqueando acessos não autorizados, danos furtos e interferências nas instalações.

Novos Projetos e Desenvolvimento

Ao longo de cada projeto desde sua concepção até sua entrega devem ser consideradas as regras de segurança para assegurar a proteção das informações processadas, conforme sua classificação e exposição a risco.

Segurança Operacional

As estações de trabalho, servidores, banco de dados, redes e sistemas devem ser administrados e monitorados de forma a reduzir riscos de ataques cibernéticos e proteger contra vazamento de informações.

Os processos de Backup e Contingência, assim como o de restore seguem regras de procedimento específico zelando pelo processo de salvaguarda dos dados a fim de atender aos requisitos operacionais e legais, garantir a continuidade do negócio em situações de incidentes ou falhas.

São também desenvolvidos e aplicados procedimentos se detecção de vulnerabilidades com o intuito de antever fragilidades e assim criar planos de ações de tratamento.

Os incidentes de Segurança são identificados, avaliados e comunicados, são aplicadas regras de segurança de forma a registrar os eventos e gerenciá-los com o objetivo de limitar os impactos e atuar de forma diligente garantindo a tomada de ação corretiva em tempo hábil.

Aculturamento

Para todos os colaboradores independente do regime de contrato de trabalho são ministrados cursos e treinamentos em plataforma educacional interna específico ao tema de Segurança da Informação em consonância com a Lei Geral de Proteção de dados, podendo ser aplicados testes direcionados ao desenvolvimento e conhecimento dos temas abordados nessa Política.

Auditorias, Penalidades e Sanções

A empresa se reserva no direito de executar auditorias internas, monitoramentos e registros de forma a garantir o cumprimento das diretrizes dessa política. As violações de segurança serão passíveis de aplicação de medidas disciplinares.