POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Na **iDISC INFORMATION TECHNOLOGIES, S.L.** as informações devem ser sempre protegidas, independentemente de como são compartilhadas, comunicadas ou armazenadas.

Introdução

As informações existem em várias formas: impressas ou escritas em papel, armazenadas eletronicamente, transmitidas por correio ou meios eletrônicos, exibidas em projeções ou faladas em conversas.

A iDISC depende dos sistemas de TIC para alcançar seus objetivos.
Esses sistemas devem ser gerenciados para proteger contra ameaças e vulnerabilidades que possam afetar a disponibilidade, a integridade ou a confidencialidade das informações processadas ou dos serviços prestados, a fim de garantir a continuidade dos negócios, minimizar os riscos comerciais e maximizar o retorno sobre o investimento e as oportunidades comerciais.

Escopo

Esta diretriz apóia a política geral do sistema de gerenciamento integrado da organização e se aplica a todos os sistemas TIC da iDISC, portanto, deve ser seguida por todas as pessoas que trabalham e colaboram com a empresa, sem exceções.

Objetivos de segurança da informação

- Evitar ou prevenir incidentes de segurança avaliando e tratando os riscos.
- Detectar anomalias na prestação de serviços por meio de mecanismos de monitoramento e análise.
- Responder de maneira eficaz a incidentes de segurança.
- Garantir a disponibilidade de serviços essenciais por meio de planos de continuidade e recuperação.
- Proteger a confidencialidade dos dados pessoais de acordo com o RGPD 2016/679.

Princípios de segurança da informação

- Esta organização avalia e tolera ou trata os riscos que, com base na avaliação, precisam ser controlados ou tratados.
- Todos os funcionários devem ser informados sobre as políticas de segurança da informação relevantes para o desempenho de seu trabalho.
- O financiamento estará disponível para o gerenciamento operacional dos controles relacionados à segurança da informação.
- As possibilidades de fraude relacionadas ao mau uso dos sistemas de informação devem ser levadas em conta no gerenciamento geral dos sistemas de informação.
- Os riscos à segurança da informação devem ser monitorados e medidas relevantes devem ser tomadas diante de mudanças que impliquem um nível inaceitável de risco.
- Os critérios para classificação e aceitação de riscos são mencionados na documentação do SGSI.
- Situações que possam expor a organização a violações de leis e regulamentos legais não serão toleradas.

Estrutura regulatória

- Esquema Nacional de Segurança (*ENS, Esquema Nacional de Seguridad*) – *Disposição 7191 do Real Decreto 311/2022*, de 3 de maio, que regulamenta o Esquema Nacional de Segurança (ENS).
- Regulamento geral de proteção de dados pessoais (RGPD – UE*) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*.
- Lei Orgânica de Proteção de Dados Pessoais e Garantia dos direitos digitais (LOPDGDD) – *Lei 3/2018 de 5 de dezembro*.

Responsabilidades

- A equipe de gestão é responsável por garantir que a segurança das informações seja gerenciada adequadamente em toda a organização.
- A equipe de gestão nomeia as pessoas responsáveis que formam o Comitê de Segurança, de acordo com o procedimento estabelecido em conformidade com o Esquema de Segurança Nacional.
- Cada chefe de departamento é responsável por garantir que as pessoas que trabalham sob seu controle protejam as informações de acordo com os padrões definidos pela organização.
- O responsável pela segurança aconselha a equipe de gestão, fornece suporte especializado à equipe da organização e garante que os relatórios de status de segurança da informação estejam disponíveis.
- Cada membro da equipe tem a responsabilidade de manter a segurança das informações em suas atividades relacionadas ao trabalho.

Políticas e padrões relacionados

- Política do sistema de gerenciamento integrado (SGI)
- Política de uso aceitável
- Dispositivos móveis e política de teletrabalho
- Política BYOD – Traga seu próprio dispositivo
- Política de classificação de informações
- Política de backup de segurança
- Declaração interna da equipe sobre a proteção de dados pessoais – RGPD
- Acordo de confidencialidade – NDA

Essas políticas/padrões/procedimentos devem ser comunicados aos funcionários e às partes interessadas externas.

Olesa de Montserrat, 22 de maio de 2023

A Direção