RANDONCORP

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Estabelecer diretrizes de comportamentos relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

2. APLICAÇÃO E ABRANGÊNCIA

Esta Política aplica-se a todos os funcionários, estagiários, fornecedores, prestadores de serviço ou quaisquer outras pessoas que sejam usuários de informações da Randoncorp.

3. REFERÊNCIAS

- Código de Conduta Ética da Randoncorp.
- Política de Consequências.
- ABNT NBR ISO/I EC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos.
- CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil.
- NIST – *National Institute of Standards and Technology*.
- Legislações vigentes.

4. DEFINIÇÕES

Ativos de Informação: qualquer informação que tenha valor para a organização, contemplando equipamentos, informações e dados.

Backup: é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Dispositivos Móveis: notebooks, tablets, smartphones, entre outros.

Incidente de Segurança: evento que pode acarretar prejuízos a empresa ou mesmo violar as regras de segurança.

5. DIRETRIZES

A Política de Segurança da Informação da Randoncorp considera a segurança da informação através dos seguintes aspectos:

- Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas;
- Integridade: salvaguarda da exatidão e inteireza da informação e dos métodos de processamento;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

A segurança da informação é obtida a partir da implementação de uma série de controles, que podem ser tecnológicos, físicos ou administrativos.

Esta política está alinhada com os objetivos estratégicos da Randoncorp.

5.1 Diretrizes Específicas

- **Uso de recursos e informações:** é compromisso de todos assegurar que as informações e os recursos sejam utilizados apenas para fins profissionais, fazendo uso adequado dos recursos de TI (tecnologia da informação), físicos (hardware) ou lógicos (software). Os funcionários, estagiários, fornecedores, prestadores de serviço devem observar e respeitar os direitos de propriedade intelectual, sejam informações de propriedade da Randoncorp ou de terceiros. Estes direitos recaem tanto sobre ativos tangíveis quanto intangíveis, incluindo as marcas, as patentes, os códigos-fonte e os contratos de licenciamento, entre outros.

- **Classificação e tratamento da informação:** todas as informações encontradas nos ambientes físicos e lógicos da Randoncorp, inclusive aquelas relacionadas aos seus fornecedores, parceiros e clientes, devem ser classificadas de acordo com a sua criticidade e sensibilidade. É um compromisso de todos os funcionários, estagiários, fornecedores, prestadores de serviço assegurar que as informações recebam os rótulos condizentes com a sua classificação, divididos nos seguintes níveis:
    i. **Pública:** na classificação pública não há confidencialidade na informação, é aberta tanto para o público interno quanto externo;

ii. **Interna:** a classificação de uso interno possui baixo nível de confidencialidade. Esta informação estará disponível para todos os administradores, funcionários e estagiários da Randoncorp, mas o público externo não poderá ter acesso a estas informações;

iii. **Restrita:** a classificação restrita possui médio nível de confidencialidade. Somente pessoas autorizadas poderão ter acesso a informação;

iv. **Confidencial:** a classificação confidencial tem o mais alto nível de confidencialidade. A informação tem alto valor para organização.

- **Usuários e Senhas:** será concedido acesso físico e lógico, somente aos recursos e informações necessários e indispensáveis ao desempenho das atividades e em conformidade com os interesses da Randoncorp considerando o princípio do menor privilégio. As senhas e outras formas de autenticação são individuais, secretas, intransferíveis e são protegidas com grau de segurança compatível com a informação associada. É responsabilidade do funcionário zelar pelo uso correto de sua identificação e pelo sigilo de sua senha.

- **Internet:** é uma ferramenta de trabalho e deve ser utilizada como método de pesquisa e complemento às atividades profissionais. O acesso às páginas e web sites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdo impróprio, como pornografia, games, apostas, entre outros.

- **E-mail:** é uma ferramenta de trabalho e deve ser utilizada como apoio ao desenvolvimento das atividades funcionais. O funcionário é totalmente responsável pela utilização do serviço, cabendo a ele total responsabilidade por qualquer ação ou dano realizado, respondendo por qualquer ato lícito ou ilícito. Os endereços e as caixas postais disponibilizadas aos usuários são de propriedade da empresa.

- **Dispositivos móveis:** é um compromisso de o funcionário utilizar de acordo com os interesses da Randoncorp e zelar pela sua guarda, cuidando de sua integridade física e pela inviolabilidade das informações contidas no mesmo, bem como devolvê-los quando requisitados pela empresa.

- **Gestão e proteção dos recursos de TI:** a aquisição, instalação, configuração, movimentação e manutenção dos recursos de Tecnologia da Informação da Randoncorp são de responsabilidade

exclusiva da área de TI. Somente é permitida a utilização de recursos de TI devidamente licenciados e homologados, mediante a análise dos riscos.

- **Acordos de confidencialidade e termos de responsabilidade:** todo funcionário da Randoncorp deve atestar o conhecimento da Política de Segurança da Informação por meio do Termo de Responsabilidade, o qual descreve de modo sucinto as condições de utilização dos recursos de TI e das informações da Randoncorp.

- **Incidentes de Segurança da Informação:** são considerados incidentes quaisquer eventos que afetem negativamente a confidencialidade, a integridade e a disponibilidade dos ativos de informação. É compromisso de todos comunicar imediatamente, através do e-mail si@randoncorp.com, qualquer incidente de Segurança da Informação. Qualquer incidente ocorrido onde o causador seja um funcionário, o mesmo pode sofrer sanções previstas na Política de Consequências.

- **Controles de Segurança da Informação:** para reduzir as vulnerabilidades e incidentes de segurança da informação, a Randoncorp dispõem de controles tais como, gerenciamento de equipamentos e dispositivos móveis, antivírus, filtros de e-mail e filtros para acesso à internet.

- **Monitoramento:** a Randoncorp poderá,
  i. Monitorar os recursos tecnológicos para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
  ii. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, caso exigido judicialmente e disponibilizá-las aos gestores, conforme solicitação;
  iii. Realizar inspeção física e lógica nas máquinas de sua propriedade;
  iv. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

- **Trabalho Remoto / Home Office:** é uma modalidade que a Randoncorp dispõem aos seus funcionários para que eles possam trabalhar de fora do ambiente corporativo (ex. residência, coworking, hotel, etc.). O funcionário é responsável por zelar os equipamentos fornecidos pela empresa, bem como a informação que está acessando.

- **Inteligência Artificial:** O uso de Inteligência Artificial pelos funcionários da Randoncorp deve ser analisado e homologado pelas áreas de Segurança da Informação, Tecnologia da Informação e Privacidade de Dados. A inserção de dados sensíveis deve ser evitada sem devida autorização. A colaboração com a equipe de tecnologia da informação é necessária para desenvolver e supervisionar processos, garantindo a segurança e conformidade com a política de segurança da informação.

6. RESPONSABILIDADES

Conselho de Administração

- Aprovar a política.

Área de Gestão de Riscos e Compliance

- Revisar e aprovar as definições gerais das estratégias de segurança da informação;
- Identificar por tipo de exposição, avaliar quanto à probabilidade de incidência e quanto ao impacto, todos os riscos que possam comprometer a realização dos objetivos da Randoncorp.

Área de Segurança da Informação

- Monitorar os recursos e os ambientes sob a sua responsabilidade com o objetivo de garantir a proteção contra as possíveis ameaças e o uso inadequado, assim como mantê-los em dia com as suas atualizações e com as mudanças na legislação e/ou nos requisitos do negócio;
- Gerenciar os controles e as ferramentas de Segurança da Informação, assim como tratar os incidentes, problemas, mudanças e quaisquer requisições e/ou reportes relacionados à Segurança da Informação;
- Promover a cultura em Segurança da Informação.

Área da Tecnologia de Informação

- Garantir a disponibilidade do ambiente Randoncorp estando em conformidade com a política e procedimentos de segurança da informação.

Gestores

- Disseminar a cultura em Segurança da Informação por meio do exemplo, verificando o cumprimento dos controles, bem como orientando os funcionários e estagiários sob sua gestão;

- Definir os privilégios de acesso dos funcionários e estagiários sob sua gestão de acordo com as atividades que desempenham.

Funcionários e estagiários

- Conhecer e cumprir a Política de Segurança da Informação, bem como os demais controles, especialmente os procedimentos relacionados à mesma e aplicáveis às atividades desempenhadas.

7. DISPOSIÇÕES GERAIS

A proteção de informações deve ser parte da conduta dos funcionários. Divulgações indevidas podem causar desvantagens, perdas financeiras e/ou danos à imagem da Randoncorp. Sempre que tiver conhecimento sobre o vazamento de informações sigilosas, tal fato deverá ser reportado por meio do Canal de Ética, para que sejam tomadas as providências cabíveis.

8. INFORMAÇÕES DE CONTROLE

Esta Política foi aprovada pelo Conselho de Administração na data de 07 de novembro de 2017, entrando em vigência a partir da mesma data.

Responsáveis pelo documento:

Elaboração	Revisão	Aprovação
Tecnologia da Informação	Gestão de Riscos e Compliance	Conselho de Administração

Versão	RCA	Data	Vigência
1ª	841	07/11/2017	07/11/2017
2ª	869	14/03/2019	14/03/2019
3ª	940	10/11/2021	10/11/2021
4ª	955	04/07/2022	04/07/2022
5ª	981	14/12/2023	14/12/2023
6ª | vigente	999	12/12/2024	12/12/2024

Última revisão:

Data: 12/12/2024

ID

RANDONCORP