INFORMATION SECURITY AND CYBERSECURITY POLICY

OBJECTIVE

To the extent applicable to Nomad's activities, the Information Security and Cybersecurity Policy is in line with the requirements and controls of the ISO/IEC 27001 standard, and the guidelines of the Central Bank of Brazil ("BCB"), the Brazilian Securities and Exchange Commission ("CVM") and the U.S. Securities and Exchange Commission ("SEC"), and its main objective is to define the guidelines adopted by Nomad to protect its data and the information of its customers, employees and stakeholders. These guidelines also address the proper treatment of risks and threats related to Information Security and Cybersecurity, in addition to the ability to identify, protect, detect, respond to and quickly recover from a cyber threat, in order to protect technological assets and information by helping Nomad to comply with current regulations and best practices.

To successfully achieve its objective, this policy is guided by the following principles:

- **Confidentiality:** ensures that the information processed is exclusively known by authorized persons;
- **Integrity:** ensures that the information remains intact, without undue modifications (accidental or purposeful);
- **Availability:** allows information systems and associated data to be accessible and usable when necessary by the authorized persons.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

OBJETIVO

A Política de Segurança da Informação e Cibersegurança está alinhada com os requisitos e controles da norma ISO/IEC 27001 e as diretrizes do Banco Central do Brasil ("BCB"), da Comissão de Valores Mobiliários ("CVM") e da Securities and Exchange Commission ("SEC"), na medida aplicável às atividades da Nomad, e tem como objetivo central definir as diretrizes que a Nomad adota para proteção dos seus dados e das informações de seus clientes, colaboradores e partes interessadas. Essas diretrizes também abordam o devido tratamento dos riscos e ameaças relacionadas à Segurança da Informação e Segurança Cibernética, além da capacidade de identificar, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger os ativos tecnológicos e informações auxiliando a Nomad a cumpir as regulamentações vigentes e com base nas melhores práticas.

Para alcançar com êxito seu objetivo, essa política é norteada pelos princípios:

- **Confidencialidade:** que garantirá que todas as informações tratadas sejam de conhecimento exclusivo de pessoas autorizadas;
- **Integridade:** que garantirá que as informações permaneçam íntegras sem modificações indevidas (acidentais ou propositais);
- **Disponibilidade:** que permitirá que os sistemas de informações e os dados associados estejam acessíveis e utilizáveis quando necessário por pessoas autorizadas.

In order to achieve this objective, Nomad has an Information Security and Cybersecurity Policy and a Business Continuity Policy that address information system security and business continuity issues with interests aligned with best practices.

Para contribuir para o alcance desse objetivo, a Nomad possui uma Política de Segurança da Informação e Segurança Cibernética e Política de Continuidade dos Negócios para lidar com as com as questões de segurança do sistema de informação e a continuidade de negócios com interesses alinhados às melhores práticas

The Information Security and Cybersecurity Policy ensures and establishes standards, procedures, and controls in order to ensure the integrity, availability and confidentiality of information contained in the Group's environments, reducing possible impacts and vulnerabilities, and the occurrence of security incidents that may affect Nomad's businesses. The document also presents the measures adopted by the Group to manage, report, and escalate Information Security and Cybersecurity risks (including important assets, information, systems and third parties).

A Política de Segurança da Informação e Cibersegurança assegura e estabelece padrões, procedimentos e controles de modo a garantir a integridade, disponibilidade e a confidencialidade das informações contidas nos ambientes do Grupo, minimizando possíveis impactos e vulnerabilidades, reduzindo a ocorrência de incidentes de segurança que afetem os negócios da Nomad. O documento ainda busca apresentar a forma adotada pelo Grupo para gerenciar, reportar e escalar riscos de Segurança da Informação e Cibersegurança (incluindo ativos relevantes, informações, sistemas e terceiros).

This document establishes and supervises the correct application of the local cybersecurity strategy, in line with the Group's global strategy and regulatory requirements. It supports business areas in driving the correct cybersecurity behaviors; performing security assessments and imposing corrections for cybersecurity risks and vulnerabilities; managing electronic fraud protection activities; and collaborating with, coordinating and communicating cybersecurity events to the business areas, regulators, government agencies and other third parties.

Este documento estabelece e supervisiona a correta aplicação da estratégia de segurança cibernética local, em linha com a estratégia global e requisitos regulatórios do Grupo. Garantindo o respaldo as áreas de negócio para impulsionar os comportamentos corretos de segurança cibernética, realizar avaliações de segurança e impor correções para os riscos e vulnerabilidades de segurança cibernética, gerir atividades de proteção contra fraude eletrônica, colaborar, coordenar e comunicar eventos de segurança cibernética com as áreas de negócio, reguladores, agências públicas e qualquer outro terceiro.

TARGET AUDIENCE

This Information Security and Cybersecurity Policy (“Policy”) is applicable to all employees, partners and suppliers, third parties and service providers of the entities of Nomad’s Economic Group (together referred to as "Nomad," to the extent applicable to their activities and according to:

PÚBLICO ALVO

Esta Política de Segurança da Informação e Cibersegurança (“Política”) aplica-se aos colaboradores, parceiros e fornecedores, terceiros e prestadores de serviço das entidades do Grupo Econômico da Nomad (referidas em conjunto como "Nomad", na medida aplicável para as suas atividades e conforme:

i) **partners and suppliers** who access Nomad's Systems and Information, and/or their own Systems, if they are integrated with Nomad's systems or if they store or process the Group's information and data;

ii) **third-party employees who build**, operate or use Nomad's information systems, whether inside or outside the Group's facilities;

iii) **service providers** involved in information technology projects, but also to other suppliers, including commercial vendors, particularly when they manage personal data;

iv) Nomad's **internal employees.**

Nomad requires compliance with all security rules of its information systems by third-party companies and their representatives.

Thus, our main attributions are as follows:

- Information Security Governance and Management;
- Access Management (Definition of Rules and Criteria);
- Certification of Information Security and Cybersecurity Internal Controls;
- Definition of Requirements and Security Analysis in Projects;
- Management and Detection of Vulnerabilities;
- Penetration Testing;
- Search and Anticipation of Cyber Threats and Attacks;
- Response to Information Security and Cybersecurity Incidents;
- Application Security.

i) **parceiros e fornecedores**, que acessam os Sistemas e Informações da Nomad, e/ou seus próprios Sistemas se estiverem integrados aos da Nomad ou se armazenarem ou processarem informações e dados do Grupo;

ii) **colaboradores de terceiros que constroem**, operam ou utilizam sistemas de informação da Nomad, bem como dentro e fora das instalações do Grupo;

iii) **prestadores de serviço** envolvidos em projetos de tecnologia da informação, mas também a outros fornecedores, incluindo fornecedores comerciais, em particular quando são capazes de gerir dados pessoais;

iv) **colaboradores internos** da Nomad.

A Nomad exige o cumprimento de todas as regras de segurança de seus sistemas de informação, por empresas terceiras e seus representantes.

Desta forma, temos as principais atribuições:

- Governança e Gestão de Segurança da Informação;
- Gestão de Acessos (Definição de Regras e Critérios);
- Certificação de Controles Internos de Segurança da Informação e Cibersegurança;
- Definição de Requisitos e Análise de Segurança em Projetos;
- Gestão e Detecção de Vulnerabilidades;
- Testes de Invasão;
- Busca e Antecipação de Ameaças e Ataques Cibernéticos;
- Resposta a Incidentes de Segurança da Informação e Cibersegurança;
- Segurança de Aplicações.

PRINCIPLES AND GUIDELINES

A. Information Protection:

Any product or information generated, processed, transmitted, and stored by any employee constitutes an asset and intellectual property that is essential to the conduct of Nomad's businesses. Regardless of its form, which may be physical, electronic, written or spoken, or how it is shared, stored or transmitted, the information should be used solely for the purpose for which it was collected, and it should not be used in non-authorized means.

The information owned by Nomad should be protected, so that its confidentiality, integrity or availability is not compromised.

B. Access Management and Control:

Access to and use of all information systems, network directories, databases, instant messaging, internet access and other resources must be limited to people authorized by the manager and the owner of the information, following the principle of least necessary privilege to fulfill their functions. Access is periodically reviewed and revoked in a timely manner at the end of the employee's or service provider's contract, or when there is a change in a function.

Critical and/or sensitive information processing equipment and facilities are kept in secure areas, with appropriate access control and protection against any threats.

PRINCÍPIOS E DIRETRIZES

A. Proteção da Informação:

Todo produto ou informação gerada, processada, transmitida, armazenada por qualquer colaborador constitui ativo e propriedade intelectual da Nomad, essencial à condução de seus negócios. Independentemente da forma apresentada que pode ser de forma física, eletrônica, escrita ou falada ou da forma como ela é compartilhada, armazenada ou transmitida, a informação deve ser utilizada unicamente para a finalidade para a qual foi coletada e não deve ser utilizada em meios não autorizados.

É diretriz que toda informação de propriedade da Nomad seja protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade.

B. Gestão e Controle de Acessos:

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bases de dados, mensagens instantâneas, acesso à internet e demais recursos devem ser restritos a pessoas autorizadas pelo gestor e pelo proprietário da informação, seguindo o princípio do menor privilégio necessário ao cumprimento de suas funções. Os acessos são revisados periodicamente e revogados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço ou quando ocorrer mudança de função.

Os equipamentos e instalações de processamento de informação crítica e/ou sensível são mantidos em áreas seguras, com controle de acesso apropriado e proteção contra quaisquer ameaças.

C. Access Credentials:

Each employee is responsible for actions performed using their credentials, which are unique, personal and non-transferable. Access to confidential information, including personal data, that are collected and stored by Nomad is limited to authorized professionals.

D. Traceability:

Each information asset must be protected proportionally to its respective value, sensitivity, criticality and associated risk of loss or compromise, generating the need, for internal systems, to have automated audit trails for internal system components, with the purpose of reconstructing the following events:

- User authentication (valid and invalid attempts);
- Access to information;
- Actions performed by users, including creating or removing objects from the system.

The audit trails of external systems are conducted in accordance with the control rules available for each system.

E. Network Segmentation:

The segmentation of the network in separate zones, based on security criteria, is applied to protect information assets and reduce risks, ensuring the confidentiality, integrity and availability of information.

The network is divided into security perimeters, with the aim of controlling traffic between them, and based on business needs.

Computers connected to the corporate network should not be accessible remotely,

C. Credenciais de Acesso:

Todo colaborador é responsável pelos atos executados com suas credenciais, que é única, pessoal e intransferível. O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pela Nomad é restrito aos profissionais autorizados.

D. Rastreabilidade:

Todo ativo da informação deve ser protegido de forma proporcional à seu respectivo valor, sensibilidade, criticidade e risco associado de perda ou comprometimento, gerando a necessidade de, para sistemas internos, serem implementadas trilhas de auditoria automatizadas para os componentes de sistema internos, com a finalidade de reconstruir os seguintes eventos:

- Autenticação de usuários (tentativas válidas e inválidas);
- Acesso a informações;
- Ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

Sistemas externos terão as trilhas de auditoria executadas de acordo com as regras de controle disponíveis por cada sistema.

E. Segmentação de Rede:

É utilizada a prática de segmentar a rede em zonas separadas, com base em critérios de segurança, para proteger ativos de informação e minimizar riscos, garantindo a confidencialidade, integridade e disponibilidade das informações.

A rede é dividida em perímetros de segurança, com objetivo do controle de tráfego entre eles e com base nas necessidades de negócios.

Computadores conectados à rede corporativa não devem ser acessíveis

with one exception: being a remote-first company, Nomad's IT Infrastructure & Support team is allowed to connect remotely, when necessary, to carry out procedures at workstations. Furthermore, direct connection to a third-party network using any network protocol is not allowed.

In order to request the creation, change and exclusion of rules relating to firewalls and network assets, a request should be sent to the Operational and Corporate Security area or the Reliability area, which will carry out the analysis, assessment of the approval, and execution.

F. Classification of Information and protection of personal data:

Data and information are categorized according to their relevance, criticality and sensitivity for the business and customers. Nomad values the privacy of information within the scope of the Brazilian General Data Protection Law ("LGPD") and the Privacy and Data Protection Policy. The information security and information technology structure include the relevant aspects to ensure the protection of personal data and its integrity, availability and confidentiality.

G. Prevention Against Viruses, Files and Malware:

Nomad has controls in place to block traffic from malicious websites, and uses a detection solution and policy to prevent viruses and other types of malicious files and software from entering and spreading on its systems and servers. All assets (computers, servers, among other devices) that are connected to the corporate network, or use Nomad's information, are protected with a malware protection solution determined by the Operational Security area.

remotamente, com uma exceção, sendo a Nomad uma empresa remote-first, o time de IT Infrastructure & Support tem permissão para conectar remotamente, quando necessário, para realizar procedimentos nas estações de trabalho. Além disso, não é permitida a conexão direta de rede de terceiros utilizando-se qualquer protocolo de rede.

Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de Segurança Operacional e Corporativa ou área de Confiabilidade, que fará a análise, avaliação da aprovação e execução.

F. Classificação de Informações e proteção de dados pessoais:

Os dados e as informações são classificados quanto a sua relevância, criticidade e sensibilidade para o negócio e para os clientes. a Nomad preza pela privacidade das informações no âmbito da Lei Geral de Proteção de Dados ("LGPD") e da Política de Privacidade e Proteção de Dados. A estrutura de segurança da Informação e tecnologia da informação contempla aspectos pertinentes para assegurar a proteção dos dados pessoais e sua integridade, disponibilidade e confidencialidade.

G. Prevenção Contra Vírus, Arquivos e Softwares Maliciosos:

A Nomad possui controles para bloqueio de tráfego de sites maliciosos e utilização de solução e política de detecção para prevenir que vírus e outros tipos de arquivos e software maliciosos entrem e espalhem-se nos sistemas e servidores. Todos os ativos (computadores, servidores, entre outros dispositivos) que estejam conectados à rede corporativa ou façam uso de informações da Nomad são protegidos com uma solução de proteção contra malware determinada pela área de Segurança Operacional.

H. Maintenance and Backups:

The backup execution process is carried out periodically for Nomad's information assets, in order to avoid or reduce data loss in the event of incidents, including cyber incidents. Nomad has specific policies and procedures to ensure data and information recovery.

I. Secure Development and Encryption:

Nomad maintains a set of principles for developing systems in a safe manner, ensuring that information security, cybersecurity and privacy protection are designed and implemented in the systems development lifecycle. Specific procedures relating to secure systems development and encryption are also in place.

J. Assessment of Providers and Suppliers:

Providers and suppliers that store, transmit and process data, or offer cloud services that can be contracted by Nomad, are assessed from the point of view of Information Security and Cybersecurity, and in accordance with the Supplier Management Policy.

When contracting data processing and storage services, Nomad will comply with the rules set out in current regulations. Therefore, the procedures to be adopted include:

I. adoption of corporate governance, information security and management practices proportional to the importance of the service to be contracted and the risks to which they are exposed; and

II. verification of the potential service provider's ability to ensure:

H. Manutenção e Cópias de Segurança:

O processo de execução de backups é realizado periodicamente para os ativos de informação da Nomad, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes, incluindo cibernéticos, a Nomad possui política e procedimentos específicos para garantir a recuperação de dados e informações.

I. Desenvolvimento Seguro e Criptografia:

A Nomad mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança da informação, cibersegurança e proteção à privacidade sejam projetadas e implementadas no ciclo de vida de desenvolvimento de sistemas e possui procedimentos específicos relativos à prática de desenvolvimento seguro de sistemas e criptografia.

J. Avaliação de Provedores e Fornecedores:

Provedores e fornecedores que armazenam, transmitem e processam dados, ou oferecem serviços alocados em nuvem, que possam ser contratados pela Nomad são avaliados sob o ponto de vista de Segurança da Informação e Cibersegurança e de acordo com a Política de Gestão de Fornecedores.

Na contratação de serviços de processamento e armazenamento de dados a Nomad obedecerá às regras previstas na regulamentação vigente, com isso, serão adotados procedimentos que contemplem:

I. a adoção de práticas de governança corporativa, segurança da informação e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

II. a verificação da capacidade do potencial prestador de serviço de assegurar:

a) compliance with current legislation and regulations;

b) the institution's access to data and information to be processed or stored by the service provider;

c) the confidentiality, integrity, availability and recovery of data and information processed or stored by the service provider;

d) compliance to the certifications required by the institution to provide the service to be contracted;

e) when applicable, access by the contracting institution to the reports prepared by an independent specialized audit company hired by the service provider, regarding the procedures and controls used in the provision of the services to be contracted;

f) provision of information and management resources suitable for monitoring the services to be provided;

g) the identification and segregation of the institution's customer data through physical and/or logical controls;

h) the quality of access controls aimed at protecting the data and information of the institution's customers; and

i) inclusion of Nomad's standard draft contract, which has a clause on the supplier's obligation to respect the Group's policies.

a) o cumprimento da legislação e da regulamentação em vigor;

b) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

e) quando aplicável, acesso pela instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente, contratada pela prestadora de serviço, a respeito dos procedimentos e controles utilizados na prestação dos serviços a serem contratados;

f) provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos e/ ou lógicos; e

h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

i) inclusão da minuta padrão de contrato da Nomad que possui cláusula sobre a obrigação do fornecedor de respeitar as políticas do Grupo.

K. Security Incident and Cyber Incident Management:

In order to guarantee the security of Nomad's information, assets and technological infrastructure, management is carried out through monitoring, assessment, treatment and responses to incidents, with the aim of minimizing the risk of failures and providing secure administration of communications networks. The activities of the Security and Cybersecurity Incidents Response Team include mapping possible attacks through detection controls implemented in the environment. The controls include a content filter, malicious behavior detection tool, antivirus, antispam, and other important tools. The incidents identified follow the incident response process and are communicated to the Privacy, Data Protection and Information Security Committee, and the Governance, Risk and Compliance Committee.

L. Preventing information leakage:

In order to prevent information leakage, specific tools to prevent data loss are used with the purpose of ensuring that confidential information is not misused, lost, stolen or leaked to the web by unauthorized users.

M. Information Security and Cybersecurity Awareness:

Employees and third parties linked to Nomad are trained annually through an effective program that raises awareness and disseminates an information security and cybersecurity culture with the aim of transmitting information security concepts.

Control and anti-phishing campaigns are carried out with all employees and third parties.

K. Gestão de Incidentes de Segurança e Incidentes Cibernéticos:

Visando garantir a segurança da informação, ativos e infraestrutura tecnológica da Nomad, é feito um gerenciamento efetivo através de monitoramento, avaliação, tratamento e respostas aos incidentes, com o intuito de minimizar o risco de falhas e prover uma administração segura de redes de comunicações. As atividades da Equipe de Resposta a Incidentes de Segurança e Cibersegurança englobam o mapeamento de possíveis ataques por meio de controles de detecção implementados no ambiente. Os controles contam com filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, antivírus, antispam, e outras ferramentas relevantes. Os incidentes identificados seguem o processo de resposta a incidentes e são comunicados ao Comitê de Privacidade, Proteção de Dados e Segurança da Informação e Comitê de Governança, Riscos e Compliance.

L. Prevenção a vazamento de informações:

Na busca por prevenir o vazamento de informações é estabelecida a utilização de ferramentas específicas para prevenção de perda de dados, com a finalidade de garantir que informações confidenciais não sejam mal utilizadas, perdidas, roubadas ou vazadas na web por usuários não autorizados.

M. Conscientização em Segurança da Informação e Segurança Cibernética:

Os colaboradores e terceiros ligados a Nomad são treinados anualmente através de um programa efetivo de conscientização e disseminação da cultura de segurança da informação e cibersegurança com objetivo de disseminar os conceitos de segurança da informação.

Campanhas de controle e antiphishing são realizadas com todos os colaboradores e terceiros.

N. Operational and non-financial risks:

Nomad maintains its business continuity plan, which identifies alternative procedures and infrastructure to protect its people, reputation, values and commitments to related audiences.

To manage crises, there is pre-established governance, with previously defined members. The objective is to manage special situations if an exceptional situation occurs, different from what was expected, or which should arise from ordinary business management.

The target is to identify what could compromise the development of activities or lead to a serious deterioration of the financial situation of the entity or group, for involving a significant distancing from the risk appetite and defined limits.

Nomad has mechanisms to activate business continuity plans in the event of disasters, both cyber and operational.

SECURITY RECOMMENDATIONS AND THREAT DEFINITIONS

Nomad lists the definition of some threats and guides information security and cybersecurity practices:

A. Authentication and password:

With the aim of identifying and authenticating access to information, the employees and/or third parties, as well as customers will receive a login and password and will be responsible for all actions carried out with this information. Therefore, everyone must follow information security practices:

N. Risco Operacionais e não financeiros:

A Nomad mantém seu plano de continuidade de negócios, que identifica procedimentos e infraestrutura alternativa para proteger as pessoas, a reputação, os valores e os compromissos com os públicos relacionados.

Para administrar crises, há uma governança pré-estabelecida, com membros previamente definidos. A responsabilidade é de administrar situações especiais, caso ocorra uma situação de excepcionalidade, diferente da esperada ou que deva derivar da gestão ordinária dos negócios.

O objetivo é identificar o que possa comprometer o desenvolvimento das atividades ou acarretar uma deterioração grave na situação financeira da entidade ou do grupo, por conjecturar um afastamento significativo do apetite ao risco e dos limites definidos.

A Nomad possui mecanismos de acionamento dos planos de continuidade de negócios em caso de desastres, tanto de origem cibernética como operacional.

RECOMENDAÇÕES DE SEGURANÇA E DEFINIÇÕES DE AMEAÇAS

A Nomad lista a definição de algumas ameaças e orienta como práticas de segurança da informação, cibersegurança:

A. Autenticação e senha:

Tendo como objetivo a identificação e autenticação no acesso à informação, o colaborador e/ou terceiro, assim como cliente receberá um login e uma senha e será responsável por todos os atos executados com essas informações. Com isso, todos devem seguir as práticas de segurança da informação:

- Always maintain the confidentiality of information;
- If storing logins and access passwords is required, keep them in a safe place with restricted access;
- Change your password periodically or immediately, whenever there is any suspicion that it has been compromised;
- Create quality passwords, so that they are complex and difficult to guess;
- Do not authorize the use of your equipment by others while it is connected/"logged in" with your identification;
- Lock the equipment whenever you are away;
- Whenever possible, enable a second authentication factor (such as SMS, Token, email login confirmation etc.).

B. Antivirus

The installation and update of an antivirus in the equipment that is used for accessing the services offered by Nomad is highly recommended. Additionally, the operating system must be up to date.

Nomad lists and defines some security and cybersecurity threats, which can cause damage to the integrity, confidentiality and availability of data and information:

A. Social engineering

This is a technique used by criminals by which one person seeks to persuade another, often based on the latter's naivety or trust, with the aim of deceiving, scamming or obtaining confidential information.

- Sempre mantenha a confidencialidade das informações;
- Caso seja necessário o armazenamento dos logins e senhas de acesso, manter em lugar seguro e com restrição de acesso;
- Altere a senha com certa periodicidade e imediatamente sempre que existir qualquer suspeita de comprometimento da mesma;
- Elabore senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
- Não autorize o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloqueie o equipamento sempre que se ausentar;
- Sempre que possível, habilitar um segundo fator de autenticação (como SMS, Token, confirmação de login por e-mail etc.).

B. Antivírus

É extremamente recomendável que seja mantido um antivírus instalado e atualizado, no equipamento utilizado para acesso aos serviços oferecidos pela Nomad. Além disso, deve possuir um sistema operacional atualizado.

A Nomad lista e define algumas ameaças de segurança e cibersegurança, que podem causar danos a integridade, confidencialidade e disponibilidade de dados e informações:

A. Engenharia social

É uma técnica empregada por criminosos pela qual uma pessoa procura persuadir outra, muitas vezes abusando da ingenuidade ou confiança, com o objetivo de ludibriar, aplicar golpes ou obter informações sigilosas.

B. Phishing

Technique used by virtual criminals with the aim of deceiving users by sending malicious emails and messages,
with the purpose of obtaining personal information from customers and users, such as passwords, credit card numbers, tax ID numbers, bank account numbers, and other data.

C. Spam

These are unsolicited emails, generally sent to a significant number of people, with typically advertising content, with the purpose of committing illegal actions. Spam is directly linked to security attacks, being one of the main vehicles for the spread of malicious codes and illegal sale of products.

D. Fake Telephone Contact

Technique used for getting information such as personal data, passwords, tokens, cell phone identification code (IMEI) or any other type of information to commit fraud.

E. False Electronic Contact and Social Media

This is also a phishing technique used by virtual criminals to deceive users by sending messages with the intention of selling, or offering new business opportunities and new jobs, with the purpose of obtaining personal information from employees, in order to have access to internal and confidential data, with a focus on stealing data.

B. Phishing

É uma técnica utilizada por criminosos virtuais, com objetivo de enganar os usuários, por meio do envio de e-mails e mensagens maliciosas,
tendo como finalidade obter informações pessoais de clientes e usuários, como senhas, número de cartão de crédito, CPF, número de contas bancárias, entre outros dados.

C. Spam

São e-mails não solicitados, geralmente enviados para um número significativo de pessoas, com conteúdo tipicamente publicitário, utilizados para a prática de atos ilícitos. Os Spams estão diretamente associados a ataques de segurança, sendo eles um dos principais responsáveis pela propagação de códigos maliciosos e venda ilegal de produtos

D. Falso Contato telefônico

É uma técnica utilizada para conseguir informações como dados pessoais, senhas, token, código de identificação do aparelho celular (IMEI) ou qualquer outro tipo de informação para a prática da fraude.

E. Falso Contato Eletrônico e Redes Sociais

Também é uma técnica de phishing utilizada por criminosos virtuais, para enganar os usuários, por meio do envio de mensagens com a intenção de venda, oportunidade de novos negócios e buscando ofertar novos empregos, tendo como finalidade obter informações pessoais de colaboradores, que facilitem o acesso a dados internos e confidenciais, com foco em sequestro de dados.

This Information Security and Cybersecurity Policy was last updated on May 17th,2024.

Esta Política de Segurança da Informação e Cibersegurança foi atualizada pela última vez em 17 de maio de 2024.