EXTRATO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Objetivo

Esse extrato tem como propósito reafirmar o compromisso da Unifique com a proteção de seus sistemas, redes e dados. Nosso objetivo é garantir que os serviços prestados operem com segurança e resiliência frente a ameaças internas e externas, sempre em conformidade com as legislações e normas aplicáveis.

Definições

Para melhor compreensão deste extrato de Cibersegurança, seguem abaixo os significados dos principais termos utilizados:

- **Cibersegurança:** Conjunto de práticas, processos e tecnologias voltadas à proteção de sistemas, redes, dispositivos e dados contra-ataques ou acessos não autorizados.
- **Segurança da Informação:** Princípios e medidas adotadas para garantir a confidencialidade, integridade e disponibilidade das informações.
- **Backup:** Cópia de segurança das informações, realizada regularmente para garantir sua recuperação em caso de falhas, erros ou incidentes.
- **Criptografia:** Técnica de codificação de dados para que apenas pessoas autorizadas possam acessá-los, tornando-os ilegíveis a terceiros não autorizados.
- **Vulnerabilidade:** Fragilidade ou falha em um sistema que pode ser explorada para comprometer a segurança da informação.
- **Teste de Intrusão (Pentest):** Simulação controlada de ataque a sistemas com o objetivo de identificar vulnerabilidades e aprimorar os mecanismos de proteção.
- **Malware:** Software malicioso criado para causar danos, roubar informações ou comprometer sistemas.
- **Rastreabilidade (Logs):** Registros automáticos das ações realizadas por usuários em sistemas e ativos, permitindo monitoramento e auditoria.
- **Segmentação de Rede:** Divisão da rede corporativa em diferentes zonas de segurança, com o objetivo de controlar e restringir o tráfego de dados entre elas.
- **Incidente de Segurança:** Qualquer evento que comprometa ou possa comprometer a segurança da informação ou a proteção de dados pessoais.
- **Gestão de Riscos Cibernéticos:** Processo de identificação, análise e mitigação de riscos relacionados a ameaças digitais e vulnerabilidades tecnológicas.
- **Baseline de Configuração:** Conjunto de configurações mínimas recomendadas para garantir a segurança de ativos tecnológicos.
- **Dados Pessoais:** Qualquer informação que identifique ou possa identificar uma pessoa natural, conforme definido pela Lei Geral de Proteção de Dados Pessoais (LGPD).

Conscientização em Segurança Cibernética

A Unifique investe continuamente em ações de conscientização e capacitação voltadas à segurança da informação e à cibersegurança. Nosso compromisso é garantir que colaboradores e parceiros estejam preparados para agir de forma segura e responsável.

Realizamos treinamentos práticos, campanhas educativas e simulações, como exercícios sobre segurança digital e testes de phishing, com o objetivo de fortalecer a cultura de segurança em todos os níveis da organização.

Além disso, estendemos essas ações ao público em geral. Nossos clientes também recebem orientações e dicas para se protegerem de ameaças digitais, por meio de campanhas informativas e conteúdos educativos.

Um exemplo é a página Segurança e boas práticas (https://unifique.com.br/portal-da-privacidade/seguranca-e-boas-praticas), onde disponibilizamos recomendações úteis para promover uma navegação segura e consciente.

Diretrizes de Segurança:

Autenticação e Senhas

A Unifique adota práticas rigorosas de controle de acesso para proteger seus ambientes digitais. Todos os colaboradores, fornecedores, prestadores de serviços e parceiros utilizam credenciais individuais, pessoais e intransferíveis para acessar os sistemas da empresa.

Essas credenciais seguem padrões definidos em nossa Política de Segurança da Informação, garantindo maior proteção contra acessos não autorizados e reforçando o compromisso com a segurança dos dados e das operações.

Gestão e Controle de Acessos

Na Unifique, o acesso a informações, sistemas e ambientes corporativos é restrito a pessoas devidamente autorizadas. Todos os acessos são concedidos com base em critérios técnicos e mediante aprovação formal, garantindo a segurança e a integridade dos dados.

Além disso, realizamos revisões periódicas dos acessos para assegurar que apenas os profissionais com necessidade real de uso mantenham as permissões ativas, reforçando nosso compromisso com a proteção das informações.

Backup de Informações

Para garantir a continuidade dos serviços e a integridade das informações, a Unifique realiza rotinas regulares de backup (cópias de segurança) dos dados mais relevantes. Essas cópias são armazenadas em ambientes seguros, possibilitando a recuperação eficiente em caso de falhas, erros ou incidentes.

Criptografia de Dados

A Unifique utiliza tecnologias de criptografia para proteger as informações que trafegam em seus sistemas. Esse processo torna os dados ilegíveis para pessoas não autorizadas, assegurando mais segurança tanto no armazenamento quanto na transmissão das informações.

Gestão de Vulnerabilidades

Nosso ambiente tecnológico é constantemente monitorado com o objetivo de identificar e corrigir possíveis vulnerabilidades. A Unifique aplica atualizações e correções de forma contínua, minimizando riscos e garantindo a proteção dos sistemas e ativos contra ameaças cibernéticas.

Testes de Intrusão (Pentests)

A Unifique realiza periodicamente testes de intrusão, simulando ataques cibernéticos controlados. Essas simulações têm como objetivo identificar eventuais fragilidades nos sistemas, possibilitando a correção preventiva de vulnerabilidades e o fortalecimento da segurança.

Prevenção contra Malware e Softwares Maliciosos

Nossa estratégia de segurança é avançada e multifacetada, empregando capacidades de detecção, bloqueio e resposta a ameaças em tempo real. Utilizamos análises comportamentais, inteligência artificial e aprendizado de máquina para proteger ativamente nossos ativos e informações, com foco contínuo na integridade das identidades e na visibilidade global do ambiente para neutralizar riscos complexos.

Rastreabilidade de Ações

Todos os acessos e atividades realizadas nos sistemas da Unifique são registrados por meio de logs. Esse monitoramento assegura a rastreabilidade das ações dos usuários, contribuindo para auditorias, investigações e para a integridade do ambiente tecnológico.

Segmentação de Rede

Adotamos práticas de segmentação de rede que garantem um controle mais granular da segurança. A rede é dividida em diferentes zonas de confiança, permitindo a aplicação de controles específicos para cada segmento, o que reduz o risco de propagação de ameaças.

Gestão de Incidentes de Segurança e Privacidade

A Unifique possui processos estruturados para identificar, analisar e tratar incidentes de segurança da informação e proteção de dados pessoais. Esses procedimentos visam minimizar impactos, corrigir eventuais falhas e evitar a recorrência dos problemas.

Gestão de Riscos Cibernéticos

A avaliação e mitigação de riscos cibernéticos seguem o modelo de governança de riscos da Unifique. Esse processo contempla as etapas de identificação, triagem, análise e resposta a eventos que possam comprometer a segurança da informação ou a privacidade dos dados.

Avaliação de Fornecedores

Para garantir a conformidade e a segurança nas operações, todo fornecedor ou prestador de serviço que envolva atividades relacionadas à segurança da informação ou ao tratamento de dados pessoais passa por avaliação técnica da área responsável por Segurança da Informação e Privacidade de Dados.

Configuração Segura de Ativos (Baseline)

A Unifique define e aplica padrões de configuração segura para seus ativos de tecnologia, com base em requisitos técnicos, boas práticas e recomendações formalizadas pelo time de Segurança da Informação e Privacidade. Isso garante maior proteção contra falhas e ataques.

Papéis e Responsabilidades

A Unifique adota uma abordagem colaborativa e estruturada para garantir a segurança da informação e a proteção de dados, envolvendo diferentes áreas e níveis de responsabilidade dentro da organização.

Todos os Colaboradores

Todos os colaboradores têm o dever de cumprir as diretrizes estabelecidas nesta Política de Cibersegurança, contribuindo ativamente para um ambiente mais seguro e resiliente.

Todos os Fornecedores e Parceiros

Todos os Fornecedores e Parceiros devem cumprir as diretrizes estabelecidas nesta Política de Cibersegurança, garantindo que todos seus colaboradores, subcontratados e estejam cientes de suas obrigações.

Departamento de Segurança da Informação e Privacidade de Dados

É o setor responsável por liderar as ações de cibersegurança e proteção de dados na Unifique. Entre suas principais atribuições, destacam-se:

- Implementar controles físicos e lógicos que assegurem a integridade, a confidencialidade e a disponibilidade das informações;
- Estabelecer e manter políticas, processos e padrões técnicos relacionados à segurança cibernética;
- Conduzir a aplicação, atualização e revisão desta política de cibersegurança;
- Atuar de forma integrada com outras áreas da companhia, garantindo que os controles de segurança sejam aplicados aos ativos sob responsabilidade conjunta;
- Promover treinamentos de conscientização sobre segurança da informação e cibersegurança para todos os colaboradores.

Canal de Contato

Caso identifique qualquer incidente relacionado à segurança da informação ou cibersegurança, entre em contato com a equipe responsável da Unifique.

E-mail para comunicação de incidentes: csirt@redeunifique.com.br

A Unifique preza pela transparência e agilidade no tratamento de ocorrências que possam comprometer a segurança digital e a proteção de dados.

DISPOSIÇÕES GERAIS

1.1. Controle de versão:

Versão	Data	Elaborado por	Aprovado por	Descrição
001	20/12/2022	Diretoria de Inovação e Transformação Digital	Conselho de Administração	Elaboração original
002	20/01/2025	Diretoria de Inovação e Transformação Digital	Conselho de Administração	