EXTREMEGROUP

POL-0021
Política de Segurança da Informação

1. Objetivo

A Política de Segurança da Informação estabelece normas e diretrizes com a finalidade de garantir a disponibilidade, integridade e confidencialidade dos dados e a segurança da informação aplicadas às necessidades do Extreme Group.

Os colaboradores e terceiros devem assegurar o cumprimento todas as políticas, regras e orientações de segurança da informação adotadas pelo Sistema de Gestão da Segurança da Informação(SGSI), com o objetivo de assegurar a disponibilidade, integridade e confidencialidade dos dados.

É de responsabilidade de todos garantir que as diretrizes da Política da Segurança da Informação estabelecidas pelo Sistema de Gestão da Segurança da Informação sejam seguidas.

2. Abrangência

As normas e diretrizes definidas neste documento aplicam-se à toda Organização, terceiros e parceiros do Extreme Group.

3. Conteúdo Geral

3.1. Referências

- POL-0001_PlanoEstrategico2018-2023
- REG-0001_MetodologiaGestaoPadroesInterno
- POL-0024_ManualSGI
- POP-0019_GestaoVulnerabilidade
- REG-0008_AmbientePadraoTrabalho
- REG-0009_RegulamentoBackupRestore
- REG-0013_OrientacoesFormacaoEquipe
- REG-0031_ControleAcesso
- REG-0033_UsoAtivo
- POP-0013_Auditoria
- POP-0022_ClassificacaoInformacao
- REG-0005_GestaoMedicaoIndicadores
- MAN-0012_CISControls
- MAN-0005_Controle de Ativos

3.2. Definições

Nome	Descrição
Extreme Group	Extreme Digital Solutions, suas filiais, Extreme Digital Services, Beyond Co, EDX e O3S.
Informação	É um ativo da empresa e, como todo ativo, deve ser protegido. A informação pode ser escrita ou impressa em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas.

Segurança da Informação e Cibernética (SIC)	A Segurança da Informação é composta pela manutenção da confidencialidade, integridade e disponibilidade da informação. Como extensão da segurança da informação existe a segurança de informação para ataques externos, chamada de cibernética, que se preocupa em defender dados sensíveis que possam ser acessados por hackers.
Confidencialidade	É a garantia de que a informação é acessível somente a pessoas autorizadas.
Integridade	Integridade se refere à preservação dos dados e informações, de forma a salvaguarda a exatidão e completeza da informação e dos métodos de processamento, impedindo que sejam corrompidos, danificados e comprometidos.
Disponibilidade	A disponibilidade está relacionada com a acessibilidade dos dados e das informações sempre que necessário.
Vírus e software malicioso	Entende-se por vírus qualquer programa que tem a capacidade de se reproduzir automaticamente, sem o conhecimento ou autorização do usuário. Entende-se por software malicioso qualquer software que realiza ações nocivas aos sistemas, como vírus, cavalo de Tróia, verme (worm) e afins.
Extremers	Colaboradores do Extreme Group.
RFC	Solicitação de comentário.

DMZ	Zona desmilitarizada.
VPN	Rede Privada Virtual.
OSI	Objetivo de Segurança da Informação.
OE	Objetivo Estratégico.

4. Conteúdo Específico

4.1. Diretrizes Gerais

Diversas informações do Extreme Group, de seus colaboradores, clientes e parceiros estão sob responsabilidade de pessoas físicas e jurídicas que agem em nosso nome ou benefício. Por isso, o Extreme Group espera que todos que possuam acesso a informações de negócio e dados pessoais sejam cautelosos com exposição indevida na vida social e digital (transporte público, festas, bares, e-mails, comentários e publicações em redes sociais etc.).

Em caso de violação das diretrizes definidas nesta política e em outros procedimentos operacionais, as medidas cabíveis previstas no acordo contrato estabelecido serão tomadas.

O Sistema de Gestão da Segurança da Informação (SGSI) tem compromisso com a melhoria contínua dos processos. Desta forma, eventuais dúvidas e relato de incidentes de segurança da informação e privacidade de dados podem ser realizados por meio da abertura de chamados ou pelo e-mail sgsi@extreme.digital.

4.1.1 Objetivos da Segurança da Informação

Para garantir o cumprimento do Objetivo Estratégico **OE.1 Garantir aplicações das melhores práticas referentes à segurança da informação**, foram estabelecidos os seguintes objetivos relacionados à segurança a informação:

ID	Objetivo da Segurança da Informação

OSI.1	Garantir a Disponibilidade da Informação
OSI.2	Garantir a Integridade da Informação
OSI.3	Garantir a Confidencialidade da Informação
OSI.4	Garantir que todos os colaboradores conheçam as políticas do Sistema de Gestão da Segurança da Informação

Para garantir o cumprimento dos objetivos de segurança da informação, há a definição dos indicadores estratégicos e respectivo acompanhamento no projeto "Sistema de Gestão Integrada (SGI)" de responsabilidade do EPG.

Por meio do acompanhamento dos indicadores será possível avaliar a eficiência dos processos e identificar falhas, permitindo, assim, a promoção da melhoria contínua dos processos organizacionais relacionados à Segurança da Informação

4.2. Confidencialidade

Ao estabelecer o contrato de trabalho, o colaborador deverá assinar o acordo de confidencialidade, no qual se compromete a seguir todas as normas e procedimentos estabelecidos pelo Sistema de Gestão de Segurança da Informação, firmando assim seu comprometimento à disponibilidade, integridade e confidencialidade dos dados que tiver acesso.

Os prestadores de serviço, parceiros e terceiros que venham a ter acesso aos sistemas internos do Extreme Group e/ou de seus clientes deverão firmar acordo de confidencialidade com seus administradores, empregados e subcontratados envolvidos na prestação dos serviços, exigindo a manutenção de estrito sigilo e confidencialidade das informações que vierem a receber ou tomar conhecimento em decorrência do respectivo contrato, firmando assim seu comprometimento à disponibilidade, integridade e confidencialidade dos dados que tiverem acesso.

4.3. Treinamento e conscientização da Segurança da Informação

Treinamentos relativos à segurança da informação estão disponíveis na plataforma E-learning da EDS.

Campanhas de conscientização são feitas periodicamente com intuito de orientar e reforçar a importância da Segurança da Informação para os extremers.

Parceiros, prestadores de serviços e terceiros que venham a ter acesso aos sistemas internos também são orientados a seguirem a Política de Segurança da Informação.

4.4. Propriedade Intelectual

Todo e qualquer trabalho desenvolvido e/ou armazenado com a utilização de recursos e informações da empresa, ou durante a jornada de trabalho do colaborador é de propriedade do Extreme Group, sendo facultada à Empresa a reivindicação da propriedade intelectual parcial ou total sobre o trabalho produzido.

Apenas a diretoria pode autorizar a cessão de uso ou transferência de qualquer ativo cuja propriedade intelectual seja do Extreme Group.

Nenhum software de propriedade ou licenciado para o Extreme Group está autorizado a ser retirado da empresa, seja através de mídias, cópias ou de links de comunicação, sob qualquer pretexto. Assim como instalado em quantidade de computadores superior à quantidade de licenças adquiridas. Todo software deve ser usado em conformidade com licenças, observações, contratos e acordos aplicáveis.

Todos os colaboradores devem observar o uso legal de propriedade intelectual de terceiros, incluindo livros, artigos, filmes, áudio, imagens, ou qualquer outro conteúdo sujeito à legislação de propriedade intelectual.

4.5. Legislação Aplicável

Correlacionam-se com a política, as diretrizes e as normas de Segurança da Informação as Leis abaixo relacionadas, mas não se limitando a elas:

- Lei Federal 8.159, de 08 de janeiro de 1991 (dispõe sobre a Política Nacional de Arquivos Públicos e Privados);
- Lei Federal 9.610, de 19 de fevereiro de 1998 (dispõe sobre o Direito Autoral);
- Lei Federal 9.279, de 14 de maio de 1996 (dispõe sobre marcas e patentes);
- Lei Federal 3.129, de 14 de outubro de 1982 (regula a concessão de patentes aos autores de invenção ou descoberta industrial);
- Lei Federal 10.406, de 10 de janeiro de 2002 (institui o Código Civil);
- Decreto-Lei 2.848, de 7 de dezembro de 1940 (institui o Código Penal);
- Lei Federal 13.709, de 14 de Agosto de 2018 (Lei Geral de Proteção de Dados Pessoais -LGPD).

4.6. Papéis e Responsabilidades

É de responsabilidade de todos os extremers o comprometimento com os requisitos da segurança da informação e divulgação da Política de Segurança da Informação.
Os papéis definidos no contexto da Política de Segurança da Informação podem ser encontrados em REG-0013_OrientacõesFormacaoEquipe.

4.7. Ferramentas

As ferramentas utilizadas no contexto da segurança da informação estão descritas em REG-0008_AmbientePadraoTrabalho.

4.8. Arquitetura de Rede

A infraestrutura de rede local do Extreme Group possui uma arquitetura de rede privada baseada em IP, estruturada dentro dos requisitos da RFC 1918 e, para complementar essa arquitetura, utilizamos os principais serviços de rede como exemplo: Serviço de Diretório, Resolução de Nome, Serviço de Arquivo, Aplicações, Serviço de Backup, Monitoria de Eventos de Servidores, Serviço endpoint (antivírus e Anti-malware)[RAdA4], Switches, Roteadores e Firewall.

A infraestrutura de segurança de acesso do Extreme Group possui capacidade de atendimento aos principais serviços de conectividade disponíveis no mercado, como por exemplo: Links privados, DMZ, Rede Wireless e VPN.

A infraestrutura dos principais serviços que estão em nuvem possuem redundância de hardware, garantindo, assim, o maior nível de serviço para a empresa e nossos clientes, sendo esses recursos monitorados e gerenciados em uma plataforma web que permite total controle dos requisitos de segurança de rede adotados pela empresa.

Toda a rede é documentada através da topologia da rede no documento MAN-0005_Controle de Ativos e a segurança de borda está descrita no documento MAN-0012 CIS Controls.

4.9. Backup

Os procedimentos de realização de backups estão definidos em REG-0009_RegulamentoBackupRestore.

4.10. Antivírus

- Todos os computadores do Extreme Group são protegidos com antivírus, que são mantidos atualizados de forma automática. A rede corporativa também é protegida por antivírus, anti Spyware e Firewall.

- É terminantemente proibido ao colaborador introduzir de forma consciente vírus de computador nas estações de trabalho do Extreme Group. A qualquer suspeita de contaminação por vírus o colaborador deve imediatamente desligar a máquina no botão de Power off e, em seguida, acionar a infraestrutura.
- Será considerado ato intencional de quebra de segurança o ato de desligamento do antivírus homologado pelo Extreme Group e será tratado como um incidente de segurança.
- A instalação do antivírus nas estações de trabalho da organização é realizada de forma manual para garantir o êxito da instalação, por intermédio da infraestrutura. A atualização das vacinas é feita automaticamente após o término da instalação.
- A atualização de vacinas é feita a partir de uma console central, que tem como objetivo principal gerenciar, monitorar, baixar novas versões de vacinas e distribuí-las de forma automática para todos os servidores e estações de trabalho, bastando apenas que o equipamento esteja conectado à internet ou à rede do Extreme Group. Através da console central, é possível verificar quais estações e servidores estão com a vacina de antivírus atualizada ou desatualizada. Mensalmente são verificadas quais máquinas estão com o antivírus em mau funcionamento, desatualizado ou com algum alerta. Sendo assim, a infraestrutura pode atuar de forma preventiva, corretiva presencial e remotamente.

4.11. Monitoramento

A organização possui softwares e sistemas que podem monitorar, gravar e arquivar todo acesso aos recursos da rede e das estações de trabalho. Por motivo de segurança, o Extreme Group se reserva no direito de inspecionar qualquer utilização de seus recursos, incluindo, mas não se limitando ao acesso à internet, mas também aos arquivos armazenados no disco local da estação de trabalho, nos servidores de rede ou em e-mails.

Todas as mensagens criadas, enviadas ou recebidas usando a rede corporativa ou com a utilização do e-mail corporativo são de propriedade do Extreme Group, que se reserva ao direito de acessar todo o conteúdo, caso necessário.

Todos os sistemas operacionais estão com os logs habilitados e redirecionados para a ferramenta de monitoração, que está descrita em REG-0008_AmbientePadraoTrabalho.

A ferramenta de monitoração realiza a coleta de logs através de agentes pré configurados, que garantem a coleta adequada dos logs.

O servidor que hospeda a ferramenta de monitoração possui espaço em disco elástico que possibilita aumentar de acordo com a necessidade.

As configurações realizadas no processo de monitoramento estão detalhadas no documento MAN-0012_CISControls.

A Infraestrutura revisa os logs registrados pela ferramenta e havendo algum alerta ou registro inadequado, as medidas cabíveis são tomadas pela Infraestrutura com o objetivo imediato para aplicar a respectiva correção.

A análise de vulnerabilidade é feita de acordo com POP-0019_GestaoVulnerabilidade.

4.12. Incidentes de Segurança

Incidentes de Segurança são eventos que podem causar danos à confidencialidade, integridade, disponibilidade ou processamento das informações. Eles se materializam como incidentes ou atos intencionais realizados por agentes externos ou como incidentes por não seguir as diretrizes desta política.

Caso algum incidente seja constatado pelos colaboradores, este incidente de segurança deve ser registrado na ferramenta de incidente ou informado pelo e-mail sgsi@extreme.digital.

Caso algum incidente de segurança seja constatado por parceiros, clientes ou terceiros deve ser informado pelo e-mail sgsi@extreme.digital.

Em caso de incidentes graves, o Comitê de Segurança da Informação será acionado pela Infraestrutura.

4.13. Controle de Acesso Físico e Lógico

As diretrizes a serem seguidas para acessos físicos e lógicos estão definidas em REG-0031_ControleAcesso.

4.14. Uso aceitável de ativos

As diretrizes a serem seguidas estão definidas em REG-0033_UsoAtivos.

4.15. Classificação das Informações

As classificações para as informações geradas e armazenadas estão definas na POP-0022_ClassificacaoInformacao.

4.16. Mesa Limpa

A política de Mesa Limpa/Tela Limpa busca resguardar o Extreme Group, bem como o próprio extremer contra o acesso não autorizado a informações como, por exemplo, terceiros observando dados expostos em mesas ou telas.

Assim, segue algumas diretrizes que devem ser seguidas:

- Documentos com informações pessoais e de terceiros, relatórios, livros e mídia eletrônica que contenham informações confidenciais devem ser armazenados em armários trancados adequados e/ou em outras formas de mobiliário de segurança, quando não estiverem em uso, especialmente fora do horário do expediente;
- Computadores pessoais e terminais de computador e impressoras não devem ser deixados autenticados/registrados quando não houver um operador (usuário) junto e devem estar com a tela bloqueada por senha quando não estiverem em uso;
- Informações sensíveis ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;
- Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidos, sempre que possível, fora da superfície da mesa (mesa limpa);
- Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho;
- Um protetor de tela que solicite uma senha para acesso deve ser usado;
- Documentos sensíveis/confidenciais sem utilidade devem ser destruídos de forma apropriada, utilizando-se por exemplo, desfragmentadora de papel.

4.17. Mascaramento de dados

O mascaramento de dados (termo que engloba anonimização, pseudoanonimização, redefinição, limpeza ou desidentificação de dados) é um método de proteção de dados sensíveis que substitui o valor original por um valor equivalente fictício, mas realista. O mascaramento de dados também é chamado de camuflagem de dados.

O objetivo do mascaramento de dados e manter a confidencialidade dos dados. Um mascaramento correto pode proteger o conteúdo dos dados e preservar o valor para o negócio. A segurança dos dados, em especial, dados pessoais e sensíveis se faz ainda mais necessária para garantir a confidencialidade das informações de colaboradores e clientes, evitando possíveis abusos.

O método mascaramento adotado pelo Extreme Group para informações em dados anonimizados, podem ser:

- Supressão de dados - esta técnica consiste na remoção completa dos dados identificáveis.
- Encobrimento de caracteres - os caracteres referentes aos dados são substituídos por outros como “X”, os asteriscos ou tarja preta.

4.18. Auditoria

As auditorias são planejadas e executadas conforme procedimentos definidos em POP-0013_Auditoria.

5. Anexo

Não aplicável