wavecom

Connecting every...things

Soluções criativas e inovadoras na área de engenharia de comunicações.

Política de Segurança da Informação

junho de 2024

Âmbito e Objetivo

Âmbito do SGSI: *Projeto, Execução, Auditoria, Consultoria e Manutenção de Redes de Telecomunicações.*

A utilização eficiente da informação deve ser parte indissociável da doutrina e prática quotidiana de uma organização, sendo considerada como componente vital ao êxito do trabalho no seu interior. As políticas corporativas de segurança da informação, como estrutura crítica e fundamental de uma organização, abrangem bases de dados, qualquer ambiente informático, documentos, arquivos e restantes ferramentas tecnológicas e/ou aplicacionais que envolvam a estrutura de negócio ou corporativa do seu meio envolvente.

As informações restritas e de interesse exclusivo dos colaboradores, devem ser tratadas internamente com sigilo absoluto, onde devem receber total proteção por parte da camada de gestão da organização.

A Segurança da Informação ainda é frequentemente vista, em muitos organismos, como uma relação "segurança versus tecnologia", mas na verdade, não só a tecnologia vista de um modo singular assegura a informação.

Assim, é adotado um plano de segurança estratégico global, internamente na **WAVECOM**.

Na maioria das organizações, a segurança da informação é encarada exclusivamente através da aquisição de tecnologia, quando a perspetiva correta deverá passar por uma abordagem inicial ao próprio negócio, caracterizando as vulnerabilidades e avaliando as potenciais ameaças (que variam de organização para organização). Em função destes dois fatores obtém-se uma avaliação do risco ao qual a entidade está exposta. Da mesma forma, e em função do risco caracterizado, deverão ser dimensionados os investimentos a realizar, com o objetivo de o reduzir, através da definição de:

- Políticas de Gestão de Segurança da Informação: alinhada com o negócio e os processos que a sustentam;
- Tecnologia: meios e modelos técnicos auxiliares de suporte dos procedimentos de segurança.

Uma vez identificados os requisitos de segurança, convém que sejam selecionados e implementados controlos para garantir que os riscos sejam mitigados a um nível considerado aceitável para o negócio da **WAVECOM**. Os controlos podem ser selecionados a partir de normas existentes, ou de outro conjunto de controlos que sejam desenvolvidos para atender a necessidades específicas em análise. É conveniente que os controlos sejam selecionados com base no custo da sua implementação, face ao grau de risco identificado e ao impacto na ocorrência de perda de informação. Nesse sentido, é da responsabilidade da gestão de topo da **WAVECOM** definir objetivos claros na implementação de uma doutrina de segurança, e demonstrar não só apoio, mas total empenho e dedicação na implementação e manutenção de uma política de segurança da informação em toda a organização com o fim de assegurar a confidencialidade, integridade e disponibilidade da informação da Wavecom, garantindo o cumprimento dos requisitos das partes interessadas e outros aplicáveis, assim como garantir a capacidade de prevenção de incidentes e a disponibilidade e continuidade da atividade da Wavecom.

A Política de Segurança da Informação destina-se a todos as partes interessadas da **WAVECOM**, independentemente do seu vínculo (colaboradores, fornecedores, consultores, temporários, voluntários, etc.).

É responsabilidade de todos assegurar um elevado nível de segurança, no sentido de apoiar e proteger os interesses da **WAVECOM** e permitir o funcionamento adequado de todos os sectores de atividade, assegurando assim a realização de serviços e negócios de maneira segura e eficaz. Os intervenientes que deliberadamente violem esta ou outras políticas podem ser sujeitos a sanções disciplinares ou outras previstas na lei.

Segurança da Informação

A Segurança da Informação define-se como a preservação de:

Confidencialidade: assegurar que a informação apenas é disponibilizada a quem tem a devida autorização;
Integridade: assegurar a consistência e veracidade da informação e respetivos métodos de processamento;
Disponibilidade: assegurar que a informação está disponível a utilizadores com a devida autorização, sempre que este acesso for necessário.
Auditabilidade: os dados e informações corporativas e/ou de negócio devem ser registrados, compilados, analisados, e revelados de modo a permitir que auditores internos ou externos possam atestar a sua veracidade; **Rastreabilidade:** assegurar a capacidade de recuperação do histórico das ações concretizadas, através de um registo
que deverá estar atualizado e disponível em qualquer momento.

A informação é um ativo tão importante, como qualquer outro ativo da organização, pelo que tem de ser protegido da forma mais apropriada. A Segurança da Informação protege a informação contra uma multiplicidade de ameaças, entre as quais: assegurar a continuidade do serviço (negócio), minimizar os efeitos negativos no negócio, maximizar a rentabilização dos investimentos e melhorar a qualidade do serviço.

Necessidade da Implementação de Políticas de Segurança

A informação e os seus processos de apoio, sistemas e redes, são bens essenciais ao negócio de uma organização. Confidencialidade, integridade e disponibilidade da

informação, são elementos essenciais para preservar a competitividade, a faturação, a rentabilidade e a imagem de uma organização no mercado. Atualmente, a segurança dos sistemas da informação das organizações, é cada vez mais colocada à prova por diversos tipos de ameaças de diversificadas origens, onde se incluem as tão frequentes fraudes electrónicas, nomeadamente a espionagem, fuga de informação, sabotagem, vandalismo, hackers e ataques DoS (denial of service), que se tornam cada vez mais sofisticados e ambiciosos. A dependência dos sistemas e serviços de informação, leva a crer que as organizações estão cada vez mais vulneráveis às ameaças de segurança. O uso simultâneo de redes públicas e privadas e a partilha de recursos de informação, são fatores que contribuem para o acréscimo da dificuldade em se controlar os acessos e a respetiva segurança dos mesmos.

Determinar os ativos de informação

Os ativos da informação são inventariados pelo Sistema de Gestão de Segurança da Informação, considerando não só o ativo, mas também:

- Responsável;
- Controlo do ativo;
- Informação existente;
- Classificação da informação;
- Controlo da informação.

A utilização e manuseamento adequado dos ativos de informação está inerente à classificação da informação existente e ao descrito nas respetivas Instruções de trabalho. A preservação dos ativos e a sua adequação/manutenção são asseguradas pelos responsáveis dos ativos.

Todos os colaboradores devolvem os ativos pertencentes à empresa, em sua posse, após o término do seu contrato de trabalho.

Definições

Integridade da Informação: Propriedade de salvaguarda da exatidão e plenitude da informação e dos seus métodos de processamento

Confidencialidade da Informação: Propriedade de que a informação apenas se encontra disponível para quem está autorizado a acedê-la (indivíduos, entidades ou processos)

Disponibilidade da Informação: Garantir que as pessoas autorizadas a aceder à informação podem fazê-lo sempre que necessário e em tempo útil.

Risco: Efeito da incerteza nos objetivos (ISO 31000).

- Nota 1: Um efeito é um desvio relativamente ao esperado. Pode ser positivo, negativo ou ambos e pode abordar, criar ou resultar em oportunidades e ameaças.
- Nota 2: Os objetivos podem ter diferentes aspectos e categorias e podem ser aplicados a diferentes níveis.
- Nota 3: O risco é frequentemente expresso em termos de fontes do risco, eventos potenciais, suas consequências e a sua verosimilhança.

Gestão do Risco: Atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco.

Risco aceitável: Risco que foi reduzido a um nível que possa ser tolerado pela organização (tabela), tendo em atenção os objetivos estratégicos da organização, a política, o contexto interno e externo da organização, os requisitos dos clientes, legais ou outros.

Fonte do Risco: Elemento que, por si só ou em combinação com outros, tem o potencial de originar o risco.

Ameaça: Origem/causa potencial de um incidente (evento com impacto) indesejado que pode resultar num dano (evento – acontecimento)

Vulnerabilidade: Fraqueza de um ativo que pode ser explorado por ameaças. Existem vulnerabilidades (fraquezas) exploradas por ameaças e ameaças (causas de acidentes) que causam danos e perdas e organização.

Análise do risco: Processo destinado a caracterizar o risco e a determinar o nível do Risco. Análise do Risco fornece a base para a avaliação do Risco e decisões sobre o tratamento do Risco.

Avaliação do risco: Processo de comparação dos resultados da análise do risco com os critérios do risco para determinar se o risco é inexistente, aceitável ou tolerável.

Tratamento do risco: Processo para modificar o risco, podendo:

- Evitar: Deixar de realizar as atividades que podem resultar em danos. Não estar exposto ao risco.
- Assumir: Reconhecer o risco. Aceitar o risco. Não implementar qualquer atividade que modifique o risco ou o desempenho
- Eliminar a origem: Fazer desaparecer a origem dos possíveis danos
- Partilhar o risco: Repartir ou dividir as consequências do risco
- Mitigar: Implementar ações/tarefas que reduzam ou eliminem o impacto provocado pelo risco

Controlo: Medida em que o risco é modificado

Objetivos do controlo: Declaração, descrevendo o que deve ser alcançado como resultado da implementação do controlo

Evento: Ocorrência ou mudança de um determinado conjunto de circunstâncias.

Evento de Segurança da Informação: Ocorrência identificada num sistema, serviço ou rede, indicando uma possível violação da política da SI ou falha das medidas de segurança, ou uma situação desconhecida, que pode ser de segurança relevante.

Incidência/Incidente de Segurança da Informação: Um simples ou uma série de eventos de SI indesejados ou inesperados, que têm uma grande probabilidade de comprometer as operações de negócio ou ameaçar a segurança da informação

Incidente de SI: Evento ou conjunto de eventos indesejáveis ou inesperados de segurança da informação, com uma probabilidade significativa de comprometer as operações de negócio e ameaçar a segurança da informação.

SGSI – Sistema de Gestão de Segurança da Informação.

SGI – Sistema de Gestão Integrada.

QAS – Qualidade, Ambiente, Saúde (enquadramento normativo).

Dados pessoais: informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Controlos de Segurança da Informação

Após a avaliação de Risco e assim que as medidas mitigadoras tenham sido identificadas, devem ser selecionados e implementados os controlos apropriados para garantir que o Risco é reduzido para um nível aceitável. Os controlos de Segurança da Informação podem ser selecionados a partir de um standard ou de outros conjuntos de controlos, podendo ser adicionados novos controlos para responder a necessidades específicas.

A seleção dos controlos depende das decisões da WAVECOM baseadas em critérios de aceitação de Risco, tratamento de Risco e na gestão do Risco de um modo geral. Estes critérios resultam da análise de Risco efetuada e devem ter em conta a regulamentação e legislação, quer nacional quer internacional, aplicável.

Os mecanismos de Segurança da Informação implementados devem ser alvo de revisões periódicas para garantir os níveis de Segurança esperados, com particular enfoque para a salvaguarda da continuidade do Negócio e processos críticos.

Responsabilidades

- Administração
- Gestor de SGSI
- Gestor de SI
- Diretores de departamento
- Colaboradores

Documentos associados

- Ativos de informação
- Matriz do risco
- Declaração de Aplicabilidade
- Instruções de trabalho
- Manual de Gestão

Revisão da Política de Segurança

A política de segurança da organização deverá ser revista anualmente ou sempre que existam alterações significativas.

Referências

Este documento foi criado com base nas melhores práticas e standards do mercado, nomeadamente:

- Norma ISO/IEC 27001, cláusula 5.2 e 6.2;
- Norma ISO/IEC 27002, A.5.1;
- Diretiva 95/46/CE - Regulamento Geral sobre a Proteção de Dados.

wavecom 20 ANOS INOVAÇÃO

wavecom@wavecom.pt

wavecom.pt

+351 234 919 190