POLÍTICA DE SEGURANÇA DA INFORMAÇÃO e SISTEMA NACIONAL DE SEGURANÇA

A Direção da Eurona, consciente da necessidade de promover, manter e melhorar o foco no cliente em todas as suas atividades, implementou um Sistema de Gestão Integrado (SGI) de acordo com o padrão, cujo objetivo final é assegurar que entendemos e compartilhamos as necessidades e metas dos nossos clientes, buscando oferecer serviços que atendam às suas expectativas, trabalhando na melhoria contínua. Declara expressamente o seu compromisso em fortalecer a Segurança e Cibersegurança da Informação do serviço prestado e compromete-se a atender às necessidades e expectativas das partes interessadas, mantendo alta a nossa competitividade nos serviços de Manutenção, Suporte, Operação e administração de infraestrutura de rede e no **Serviço de design, arquitetura e desenvolvimento de soluções de software.**

MISIÓN y OBJETIVOS*:*

- Fomentar a melhoria contínua dos serviços e suporte ao cliente
- Manter o posicionamento da Eurona como referência no setor
- Proporcionar uma proteção adequada das informações da Eurona, a operadora de telecomunicações especialista em serviços e soluções de conectividade por meio de tecnologias como internet via satélite e Wi-Fi
- Prestar o serviço com base no nosso compromisso com a melhoria contínua dos sistemas, com a segurança e cibersegurança da informação como pilar central e padrão

Nossa missão e objetivos serão alcançados através de:

- Um sistema de **objetivos,** métricas e indicadores de melhoria contínua, com acompanhamento e medição de nossos processos internos, bem como da satisfação de nossos clientes. Estabelecendo e supervisionando o cumprimento dos requisitos contratuais para garantir um serviço eficaz e seguro
- Formação e conscientização contínua da nossa equipe para atingir o mais alto grau de profissionalismo e especialização possível, mantendo nossas infraestruturas em condições adequadas e em conformidade com os requisitos de nossos clientes.
- Um procedimento seguro de gestão de aquisição de produtos.
- Cumprindo as exigências da legislação vigente, especialmente com o **GDPR** e o cumprimento da nossa D**ocumentação de Segurança.**
- Introdução de processos de melhoria contínua que permitam um avanço permanente na nossa gestão de Segurança da Informação.
- Gestão e elaboração de planos para a gestão e tratamento de riscos, com uma metodologia de análise e gestão de riscos baseada em normas.
- Gestão das comunicações internas e externas, bem como das informações armazenadas e em trânsito.
- Gestão e monitoramento das atividades por meio da gestão de logs
- Atenção especial à gestão de incidentes de segurança
- Garantindo a continuidade e disponibilidade do negócio e dos serviços.
- Assegurando que nossos Ativos e Serviços cumpram com as medidas do E**NS de Nível MÉDIO** para as dimensões de **Confidencialidade, Integridade, Disponibilidade, Autenticidade e Rastreabilidade.**

Da mesma forma, esses princípios devem ser contemplados nas seguintes áreas de segurança:

- **Física:** Compreendendo a segurança das dependências, instalações, sistemas de hardware, suportes e qualquer ativo de natureza física que trate ou possa tratar informações, bem como os acessos físicos.
- **Lógica: I**ncluindo os aspectos de proteção de aplicações, redes, comunicação eletrônica, sistemas computacionais e acessos lógicos.
- **Político-corporativa:** Formada pelos aspectos de segurança relativos à própria organização, às normas internas, regulamentações e legislação.

O objetivo final da segurança da informação é garantir que uma organização possa cumprir seus objetivos utilizando sistemas de informação.
Nas decisões relacionadas à segurança, os seguintes princípios básicos devem ser considerados:

a) Segurança integral.
b) Gestão de riscos.
c) Prevenção, reação e recuperação.
d) Linhas de defesa.
e) Reavaliação periódica.
f) Função diferenciada.

Funções ou papéis de segurança:
Responsável pela Informação: Determinar os requisitos (de segurança) da informação tratada, de acordo com os parâmetros do Anexo I do ENS.

- Implantar e manter o Sistema de Gestão Integrado (SGI), melhorando continuamente sua eficácia.
- Implantar e manter o ENS, melhorando continuamente sua eficácia.
- Supervisionar os procedimentos e as instruções técnicas.
- Aplicar as medidas e os acompanhamentos indicados pelo DPO.
- Realizar o acompanhamento e verificar a implantação e eficácia de todas as ações corretivas e preventivas estabelecidas.
- Assegurar que o sistema implantado cumpre com a norma estabelecida.
- Analisar os dados obtidos no Sistema de Gestão Integrado (SGI) e ENS e propor melhorias.
- Elaborar o plano anual de auditorias internas.
- Gestão de Não Conformidades de segurança.
- Participar em Auditorias Externas.
- Responsável pelos dados privados da empresa em relação à sua perda, roubo e desatualização.
- Cumprir com a Normativa de Segurança.
- Manter atualizados os meios de contato com as autoridades.
- Manter o inventário de suportes que contêm dados de caráter pessoal.
- Analisar os relatórios de auditoria e elevar as conclusões ao responsável pelos dados.
- Gerir as não conformidades, ações corretivas e ações preventivas de SI.
- Manter os documentos do SGI.
- Manter e divulgar a política de segurança da Eurona, assim como o restante das políticas para o pessoal envolvido em cada uma delas.
- Elaborar os documentos de segurança da Eurona.
- Atender a incidentes relacionados à proteção de dados.
- Encaminhar o contato com as autoridades, se necessário.
- Aplicação e supervisão do cumprimento das políticas do SGI.
- Manutenção e aplicação do Documento de Aplicabilidade do SGI

Responsável de Sistemas: Determina os requisitos dos serviços prestados.

- Desenvolver, operar e manter o Sistema durante todo o seu ciclo de vida, incluindo suas especificações, instalação e verificação de seu correto funcionamento.
- Definir a topologia e a política de gestão do Sistema, estabelecendo os critérios de uso e os serviços disponíveis.
- Aprovar as mudanças que afetem a segurança do modo de operação do Sistema.
- Implantar e controlar as medidas específicas de segurança do Sistema, assegurando que estas se integrem adequadamente dentro do marco geral de segurança.
- Determinar a configuração autorizada de hardware e software a ser utilizada no Sistema.
- Aprovar toda modificação substancial da configuração de qualquer elemento do Sistema.
- Realizar o processo necessário de análise e gestão de riscos no Sistema.
- Determinar a categoria do sistema segundo o procedimento descrito no Anexo I do ENS e determinar as medidas de segurança que devem ser aplicadas, conforme descrito no Anexo II do ENS.
- Elaborar e aprovar a documentação de segurança do Sistema.
- Delimitar as responsabilidades de cada entidade envolvida na manutenção, exploração, implantação e supervisão do Sistema.
- Garantir o cumprimento das obrigações do RSI.
- Investigar os incidentes de segurança que afetem o Sistema e, se necessário, comunicar ao Responsável de Segurança ou a quem ele determinar.
- Estabelecer planos de contingência e emergência, realizando exercícios frequentes para que o pessoal se familiarize com eles.
- Além disso, o responsável pelo sistema pode acordar a suspensão do manuseio de determinadas informações ou da prestação de um certo serviço se for informado de deficiências graves de segurança que possam afetar a satisfação dos requisitos estabelecidos. Esta decisão deve ser acordada com os responsáveis pela informação afetada, pelo serviço afetado e pelo responsável de segurança antes de ser executada.

Responsável de Segurança da Informação: Determina as decisões para satisfazer os requisitos de segurança da informação e dos serviços.

- Manter a segurança da informação gerida e dos serviços prestados pelos sistemas de informação em sua área de responsabilidade, de acordo com o estabelecido na Política de Segurança da Informação da organização.
- Promover a formação e conscientização em matéria de segurança da informação dentro de sua área de responsabilidade.
- Os relatórios de autoavaliação e/ou os relatórios de auditoria serão analisados pelo Responsável de Segurança competente, que elevará as conclusões ao Responsável do Sistema para que adote as medidas corretivas adequadas.
- Supervisionar os procedimentos e as instruções técnicas.
- Responsabilidade geral por administrar a implementação das práticas de segurança.
- Assegurar que o sistema implantado cumpre com a norma estabelecida.

- Analisar os dados obtidos no Sistema de Gestão de Segurança da Informação e ENS e propor melhorias.
- Participar em Auditorias Externas.
- Responsável pelo risco de intrusão física dos dispositivos da empresa.
- Cumprir com a Normativa de Segurança.
- Segregação de tarefas e ambientes.
- Comunicar qualquer emergência de incêndio, inundação ou falha nos equipamentos de climatização que possa ativar o PCN.
- Revisar o Plano de Continuidade do Negócio.
- Verificar o funcionamento do Plano de Continuidade de Negócio.
- Controlar o acesso de pessoas aos locais onde estão instalados os sistemas.
- Supervisionar os incidentes de segurança ocorridos.
- Realizar e custodiar as cópias de segurança.
- Gerar os planos de tratamento de gestão de risco e supervisionar sua implantação.
- Atualizar a análise de riscos.
- Convocar as reuniões do CSI.
- Gerar as atas de reunião do CSI.
- Supervisionar a coleta de métricas.
- Realizar as revisões de segurança do SGI.
- Manter o Plano de Continuidade de Negócio.
- Incorporar no registro de incidentes as medidas corretivas.
- Aplicação e supervisão do cumprimento das políticas de SGI.

Responsável do Serviço: Determina os níveis de segurança dos serviços.

- Garantir o cumprimento dos objetivos e métricas estabelecidos para o serviço (SLAs).
- Organização diária dos recursos.
- Responsável pela perda e roubo de informação dos serviços e soluções informáticas para clientes e usuários em geral.
- Cumprir com a Normativa de Segurança.
- Incluir as especificações de segurança no ciclo de vida dos serviços e sistemas, acompanhadas dos correspondentes procedimentos de controle.
- Programar, dirigir, coordenar, supervisionar e controlar todas as atividades do serviço.
- Revisão e cumprimento dos relatórios dos serviços.
- Avaliar as consequências de um impacto negativo sobre a segurança dos serviços, considerando sua repercussão na capacidade da organização para alcançar seus objetivos, na proteção de seus ativos, no cumprimento de suas obrigações de serviço, no respeito à legalidade e aos direitos dos cidadãos.

O Comitê de Segurança da Informação (CSI) da Eurona abrange toda a empresa, sendo o mecanismo de coordenação e resolução de conflitos, entre outras funções:

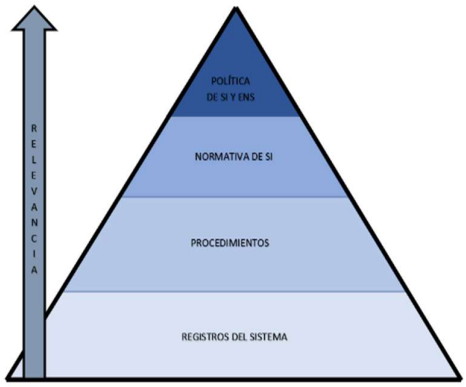
- Atender as inquietações da Direção e dos diferentes departamentos.
- Informar regularmente sobre o estado da segurança da informação à Direção.
- Promover a melhoria contínua do sistema de gestão da segurança da informação.
- Elaborar a estratégia de evolução da organização no que se refere à segurança da informação.
- Coordenar os esforços das diferentes áreas em matéria de segurança da informação, para garantir que os esforços são consistentes, estão alinhados com a estratégia decidida e evitam duplicidades.
- Elaborar (e revisar regularmente) a Política de Segurança da Informação para sua aprovação pela Direção.
- Elaborar e aprovar os requisitos de formação e qualificação de administradores, operadores e usuários, do ponto de vista da segurança da informação.
- Monitorar os principais riscos residuais assumidos pela organização e recomendar possíveis ações.
- Monitorar o desempenho dos processos de gestão de incidentes de segurança e recomendar possíveis ações em relação a eles. Em particular, velar pela coordenação das diferentes áreas de segurança na gestão desses incidentes.
- Promover a realização de auditorias periódicas que permitam verificar o cumprimento das obrigações do organismo em matéria de segurança.
- Aprovar planos de melhoria da segurança da informação da organização, com especial atenção à coordenação de diferentes planos que possam ser realizados em várias áreas.
- Priorizar as ações em matéria de segurança quando os recursos forem limitados.
- Assegurar que a segurança da informação seja considerada em todos os projetos de TIC desde sua especificação inicial até sua implementação. Em particular, deve velar pela criação e utilização de serviços horizontais que reduzam duplicidades e apoiem um funcionamento homogêneo de todos os sistemas de TIC.
- Resolver os conflitos de responsabilidade que possam surgir entre os diferentes responsáveis e/ou entre diferentes áreas da organização, elevando aqueles casos em que não tenha autoridade suficiente para decidir.

Compõem o CSI:

- Responsável da Informação
  Responsável do Serviço
  Responsável de Segurança da Informação

- Responsável do Sistema (Hotspots)
- Responsável do Sistema (Operações)
- Responsável do Sistema (TI)
- Responsável do sistema delegado (Portais e Dashboard)
- Responsável de contratação e aquisição
  Administrador de rede

Estruturação da documentação de segurança do sistema: A documentação do sistema segue a seguinte estrutura:



A classificação da informação do sistema é dividida nas seguintes categorias, conforme estabelecido no documento de Normativa de Segurança:

- Uso Público
- Uso Interno
- Uso Confidencial

Legislação aplicável em matéria de tratamento de dados de caráter pessoal
Em matéria de tratamento de dados de caráter pessoal, terá-se em conta, principalmente, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que revoga a Diretiva 95/46/CE e a legislação nacional correspondente.

O marco legal e regulatório aplicável está registrado no documento Registro de Identificação e Avaliação de Requisitos Legais da Eurona.
Considerando essas diretrizes, esta direção reitera seu firme compromisso em unir esforços para alcançar esses objetivos, de modo que esta política seja entendida, implantada e mantida atualizada em todos os níveis da organização.

Fdo.

Jordi Puig Cruz
Representante da Direção