

NORMAS DE CONDUTA E POLÍTICA DE COMPLIANCE

VERISURE BRASIL



Índice

1. CÓDIGO DE CONDUTA

1.1. MENSAGEM DO NOSSO PRESIDENTE.....	6
1.2. PRINCÍPIOS DE CONDUTA DA VERISURE BRASIL	10
1.2.1. CUMPRIMENTO DA LEI.....	11
1.2.2. RESPEITO A NOSSOS CLIENTES	12
1.2.3. RELAÇÕES COM NOSSOS COMPANHEIROS	12
1.2.4. CONDUTA INDIVIDUAL.....	13
1.2.5. PROTEÇÃO DA INFORMAÇÃO	15
1.2.6. SEGURANÇA E SAÚDE.....	15
1.3. OBRIGAÇÃO DE INFORMAR E COLABORAR:	
CANAL DE DENÚNCIAS	16
1.4. REGIME SANCIONADOR.....	18
1.4.1. COMISSÃO DE COMPLIANCE	19
1.4.2. MEDIDAS SANCIONADORAS.....	19

2. POLÍTICA DE CLASSIFICAÇÃO E PROTEÇÃO DA INFORMAÇÃO

2.1. OBJETO	21
2.2. ÂMBITO DA APLICAÇÃO	21
2.3. GRAUS DE CLASSIFICAÇÃO.....	22
2.4. RELAÇÕES COM TERCEIROS	23
2.4.1. FORNECEDORES COM ACESSO À INFORMAÇÃO	
CLASSIFICADA DA VERISURE BRASIL.....	23
2.4.2. INFORMAÇÃO DEPOSITADA DE PROPRIEDADE	
DE TERCEIROS	24
2.5. INCIDÊNCIAS	24
2.6. HISTÓRICO DO DOCUMENTO	24

3. POLÍTICA DE DEFESA DA CONCORRÊNCIA

3.1. Introdução.....	26
3.2. Destinatários	26
3.3. Conceitos básicos sobre as normas de direito	
da concorrência.....	27
3.4. Carteis, abuso de posição dominante no mercado	
e controle de atos de concentração	27
3.5. Descumprimento da Política:	
investigações e regime sancionador.....	31

4. POLÍTICA SOBRE DELEGAÇÃO DE FACULDADES, LIMITES E CONTROLES

4.1. Introdução.....	33
4.2. Destinatários	34
4.3. Controles e limites gerais.....	34
4.4. Controles especiais	35
4.5. Controles e limites contábeis e financeiros: Auditoria.....	35
4.6. Controles e limites para o investimento	36
4.7. Despesas.....	39
4.8. Compras.....	41
4.9. Estado Real	41
4.10. Reclamações e M&A	42



Índice

5. POLÍTICA SOBRE DENUNCIA INTERNA

DE IRREGULARIDADES (WHISTLE BLOWER POLICY)

5.1. Introdução.....	44
5.2. Em que consiste a denúncia de irregularidades?	44
5.3. O que eu posso denunciar?.....	45
5.4. Canal de denúncias.....	46
5.5. Como denuncio?.....	46
5.6. Garantias do processo de denúncia	46

6. POLÍTICA CONTRA SUBORNO E CORRUPÇÃO

6.1. Objeto.....	48
6.2. De inições	48
6.3. Obrigações e proibições.....	50
6.4. Requisitos adicionais e diretrizes	51
6.5. Requisitos e padrões sobre a documentação inanceira	54
6.6. Não cumprimento da Política	54

7. POLÍTICA DE USO ACEITÁVEL DOS SISTEMAS

DE INFORMAÇÃO

7.1 Objeto e Finalidade	58
7.2 Campo de aplicação	59
7.2.1 Escopo	59
7.2.2 Destinatários	59
7.3 Política.....	60
7.3.1 Propriedade e uso geral.....	60
7.3.2 Segurança e tratamento da informação.....	61
7.3.3 Segurança das credenciais e equipamentos.....	61
7.3.4 Segurança de email.....	61
7.3.5 Uso de email pessoal em meios corporativos.....	62
7.3.6 Acesso à Internet	62
7.3.7 Acesso remoto	63
7.3.8 Uso de meios próprios	63
7.3.9 Acessos do administrador de sistemas	63
7.3.10 Uso não aceitável	64
7.3.10.1 Uso não aceitável de sistemas e redes	64
7.3.10.2 Uso não aceitável de email e comunicações	65
7.3.10.3 Uso não aceitável do acesso à Internet	65
7.3.11 Blogs e redes sociais.....	65
7.3.12 Proteção de informações de caráter pessoal	66
7.3.12.1 Obrigações	66
7.3.12.2 Funções.....	67
7.4 Regime disciplinar.....	68
7.5 De inições	69



CÓDIGO DE CONDUTA
VERISURE BRASIL



1.1 Mensagem do nosso presidente



"Quero compartilhar com todos o novo Código de Conduta da VERISURE BRASIL.

Este Código de Conduta reúne os princípios que definem nossa cultura corporativa e define o comportamento ético e a integridade pessoal e profissional como forma de entender e desenvolver nossa atividade. A partir de hoje, todos que integramos esta Companhia contamos com um guia seguro de comportamento que devemos considerar em nossas relações com clientes, terceiros e parceiros. Com seu estrito cumprimento, garantimos a base para objetivos estratégicos cada vez mais ambiciosos e criamos um valor sustentável a médio e longo prazo. Definitivamente, com a aplicação deste Código de Conduta conseguiremos ser melhores, nos fortalecendo, seja interna ou externamente.

Convido todos a ler com atenção, e estou certo de que todos e cada um de nós contribuiremos com sua aplicação em nosso dia a dia".

Este Código de Conduta é direcionado a toda a organização da VERISURE BRASIL, compreendendo os administradores, diretores e empregados. Será igualmente aplicável a fornecedores, empreiteiros e colaboradores.

Antonio Anguita Ruiz
Iberia & Latam Executive President

1.2 Princípios de conduta



PROGRAMA DE COMPLIANCE VERISURE BRASIL MONITORAMENTO DE ALARMES S.A.

Estimados Colaboradores.

Seguindo as diretrizes do Grupo Securitas Direct – Verisure, informo que implementaremos o Programa de Compliance. Visamos assegurar nosso negócio e reduzir eventuais riscos à nossa empresa, seus administradores e diretores.

Esse programa é formado por estrutura de diretrizes, que servirão de base para o nosso comportamento, seguindo nossos princípios e valores.

Como parte do Programa de Compliance, adotamos um Código de Conduta, bem como uma série de políticas corporativas que ajudarão nosso crescimento acrescidos dos mais elevados níveis de qualidade. Por isso, os incentivo a ler essas políticas, zelar pelo seu cumprimento e aplicá-las diariamente no desenvolvimento de nossas atividades.

As políticas são as seguintes:

- Código de Conduta
- Política de Classificação da Informação
- Política de Canal de Denúncias
- Política Anticorrupção e Suborno
- Política de Limites e Controles
- Política de Segurança da Informação

Todas as políticas serão publicadas na Intranet corporativa e estarão disponíveis para consulta.

Vamos trabalhar juntos, buscando alcançar os mais altos padrões éticos, de qualidade, mantendo a boa reputação da nossa empresa. Com isso, nos consolidaremos como o principal fornecedor de sistemas de alarme em residências e empresas.

Gustavo Velasco
Managing Director
Verisure Brasil

Declaro que recebi as Políticas Corporativas e o Código de Conduta, integrantes do Programa de Compliance Verisure Brasil.

Data:
Funcionário:

Assinatura:

PROGRAMA DE COMPLIANCE VERISURE BRASIL MONITORAMENTO DE ALARMES S.A.

Estimados Colaboradores.

Seguindo as diretrizes do Grupo Securitas Direct – Verisure, informo que implementaremos o Programa de Compliance. Visamos assegurar nosso negócio e reduzir eventuais riscos à nossa empresa, seus administradores e diretores.

Esse programa é formado por estrutura de diretrizes, que servirão de base para o nosso comportamento, seguindo nossos princípios e valores.

Como parte do Programa de Compliance, adotamos um Código de Conduta, bem como uma série de políticas corporativas que ajudarão nosso crescimento acrescidos dos mais elevados níveis de qualidade. Por isso, os incentivo a ler essas políticas, zelar pelo seu cumprimento e aplicá-las diariamente no desenvolvimento de nossas atividades.

As políticas são as seguintes:

- Código de Conduta
- Política de Classificação da Informação
- Política de Canal de Denúncias
- Política Anticorrupção e Suborno
- Política de Limites e Controles
- Política de Segurança da Informação

Todas as políticas serão publicadas na Intranet corporativa e estarão disponíveis para consulta.

Vamos trabalhar juntos, buscando alcançar os mais altos padrões éticos, de qualidade, mantendo a boa reputação da nossa empresa. Com isso, nos consolidaremos como o principal fornecedor de sistemas de alarme em residências e empresas.

Gustavo Velasco
Managing Director
Verisure Brasil



1. Cumprimento da lei

Como companhia de segurança, nossa razão de ser não é outra a não ser cuidar de nossos clientes, suas famílias e seus negócios, e não entendemos outra forma de fazer isso que não seja cumprindo estritamente com a lei, assim como com nossas políticas internas. Não serão aceitas condutas fraudulentas dentro da Companhia.



2. Respeito com nossos clientes

Nossos clientes confiam em nós, nos disponibilizando suas informações pessoais e informação privada sobre sua residência e/ou negócio. Por isso, concedemos um grande valor à confiança depositada em nós e protegemos a informação proporcionada a nós.



3. Relações com nossos companheiros

Comprometemos-nos a criar um ambiente de trabalho integrador, onde todos os empregados tenham as mesmas oportunidades por meio de políticas de emprego e práticas claramente definidas que serão aplicáveis à contratação, seleção, promoção, disciplina, desenvolvimento, compensação e dispensa. Fica proibido o assédio e a intimidação. Não é permitido o consumo de substâncias ilegais ou ingestão de álcool.



4. Conduta individual

Atuamos com honestidade, integridade e imparcialidade em nossas relações, seja interna ou externamente. Não toleramos nenhuma forma de suborno, nem oferta de pagamentos desonestos ou presentes para empregados. Evitaremos qualquer situação que possa levar a um conflito de interesses.



5. Proteção da informação

Na VERISURE BRASIL consideramos que a informação e o conhecimento são alguns dos nossos principais ativos para o desenvolvimento do negócio, por isso eles devem ser objeto de proteção especial.



6. Segurança e saúde

É responsabilidade de todos tomar as medidas necessárias para proteger nossa segurança, saúde e bem estar e a dos demais. Por isso, a Verisure Brasil se compromete a garantir um ambiente seguro e estimulante, e apoiar a saúde, o bem estar e o equilíbrio entre a vida profissional e pessoal de todos os empregados.

1.2.1 Cumprimento da lei

Como uma Companhia de segurança, nosso motivo de ser não é outro a não ser cuidar de nossos clientes, de suas famílias, suas casas e seus negócios e não sabemos outra forma de fazer isso que não seja cumprindo estritamente com a lei, assim como com nossas políticas internas.

Leis de defesa da concorrência

A maioria dos países tem leis destinadas a proteger uma concorrência livre e justa. Estas leis proíbem acordos que restrinjam o comércio como acordar valores, dividir os clientes ou abusar de uma posição dominante.

No Brasil, existem leis destinadas a proteger uma concorrência livre e justa. Sua aplicação em determinadas situações pode ser bastante complexa. Por isso, cada um de nós deveria ter um conhecimento básico sobre a forma como nosso trabalho é aplicado.

Leis anticorrupção

Não devemos aceitar nem oferecer qualquer forma de suborno. A lei proíbe qualquer tipo de suborno, em qualquer situação comercial.

Em nenhuma hipótese devemos aceitar ou oferecer qualquer forma de suborno (pagamento a funcionários do Governo para acelerar um trâmite), comissões ilegais ou qualquer outra forma de pagamento desonesta.

Qualquer presente, atendimento ou convite que seja dado ou recebido, no âmbito de nossa atividade, superior a € 100 exigirá o consentimento prévio e por escrito do seu responsável e do departamento de Recursos Humanos.

Caso seja evidenciado que um empregado da VERISURE BRASIL deu ou recebeu qualquer forma de suborno, ficará sujeito a uma ação disciplinar e pode ser demitido.

Contratos

Todos os acordos comerciais deverão ser realizados por escrito. Todos os contratos devem estar autorizados seguindo os procedimentos internos estabelecidos, sempre com a supervisão da Assessoria Jurídica e do Departamento de Compras. Em caso de dúvidas, consulte o seu responsável e/ou o departamento de Assessoria Jurídica.

Em nenhum caso devemos contratar terceiros que não cumpram com a lei.

Na VERISURE BRASIL nos preocupamos especialmente pela qualidade no processo de contratação com clientes e não medimos esforços para conseguir o pleno cumprimento dos protocolos definidos pela Companhia.

NÃO FAÇA ISSO:



- Intercambiar informação confidencial do ponto de vista da concorrência (por exemplo, valores, custos e volumes de vendas) com concorrentes.
- Acordar valores com a concorrência.
- Dividir clientes com a concorrência.
- Enviar à concorrência informações falsas

NÃO FAÇA ISSO:



- Liberações e/ou condutas fraudulentas com a finalidade de atingir objetivos comerciais do próprio empregado.
- Usar dados falsos na contratação ou dados de terceiros alheios ao contrato ou falsificar qualquer tipo de documento.
- Formalizar contratos abusando da confiança do cliente.
- Omitir ao cliente informação contratual de seu interesse.

1.2.2 Respeito aos nossos clientes

Todos os profissionais formados pela Verisure Brasil estão comprometidos em proporcionar produtos, serviços e soluções seguras e de qualidade.

Nossos clientes confiam em nós, fornecendo seus dados pessoais e informação privada sobre sua casa e/ou negócio. Por isso outorgamos um grande valor à confiança depositada em nós e protegemos a informação que nos é proporcionada.

Assim, o nosso objetivo é criar uma cultura de privacidade ao longo de nosso negócio e guardar de forma responsável e confiável a intimidade dos nossos clientes.

1.2.3 Relações com nossos companheiros

Estamos comprometidos em criar um ambiente de trabalho integrador onde todos os empregados tenham as mesmas oportunidades por meio de políticas de emprego e práticas claramente definidas que serão aplicáveis na contratação, seleção, promoção, disciplina, desenvolvimento, compensação e demissão.

Sem discriminação:

Embasamos as relações com e entre os companheiros no respeito às pessoas e aos Direitos Humanos. Não aceitamos qualquer forma de discriminação, assédio ou intimidação. Caso as ações ou conduta de um companheiro te preocupem, solicite a sua interrupção ou comunique o seu responsável.

Assédio e intimidação:

O assédio e a intimidação estão completamente proibidos. Entende-se por assédio e intimidação os comportamentos indesejados por uma pessoa quando se considere que são intimidatórios, maliciosos, ofensivos, insultantes, humilhantes ou degradantes. Eles podem ser cometidos verbalmente, fisicamente e nem sempre acontecem frente a frente (imagens, email, telefone, redes sociais, etc.).

Na VERISURE BRASIL, não existe espaço para este tipo de comportamento. Por isso, denuncie, por meio dos mecanismos existentes ou através do canal de denúncias, qualquer comportamento suscetível de ser considerado como assédio ou intimidação ao qual esteja envolvido ou tenha conhecimento.

Álcool e drogas:

Não vamos tolerar na Verisure Brasil o consumo de substâncias ilegais. Qualquer uso, venda ou distribuição de substâncias ilegais serão tratadas com a máxima seriedade e serão sancionados com a demissão e/ou a tomada de ações legais.

Igualmente, fica proibido o consumo de álcool durante qualquer atividade trabalhista, a menos que seja consumido com moderação em um evento de trabalho, normalmente fora do horário de trabalho.

FAÇA ISSO:



- Respeite a privacidade dos nossos clientes a todo o momento.
- Recorde-se que a privacidade implica algo mais que guardar informação.

NÃO FAÇA ISSO:



- Acessar ou fornecer informação dos clientes a alguém sem a devida autorização por escrito do diretor da sua área, pois isso representa infração a este código e pode levar ao cometimento de um delito.

NÃO FAÇA ISSO:



- Insultar um companheiro ou um terceiro no âmbito de sua atividade profissional
- Zombar ou menosprezar alguém.
- Excluir ou isolar alguém do trabalho ou de atividades sociais.
- Proceder com represálias a alguém por ter denunciado previamente um caso de assédio.
- Flertar, praticar insinuações ou agressão sexual.
- Tocar ou se aproximar demais a alguém sem o seu consentimento.
- Mostrar ou circular material ofensivo (por exemplo, imagens ou desenhos animados grosseiros, racistas ou de conotação sexual).
- Tomar decisões dependendo da aceitação ou recusa de favores sexuais.
- Realizar comentários negativos sobre seus companheiros perante clientes ou terceiros.

1.2.4 Conduta individual

Atuamos com honestidade, integridade e imparcialidade em nossas relações tanto internas como externas. Não toleramos qualquer forma de suborno nem ofertas de pagamento desonestos, presentes para empregados e evitaremos qualquer contrato que possa gerar um conflito de interesses.

Não realizamos comentários ou ações que possam prejudicar a reputação e os interesses econômicos da VERISURE BRASIL.

Conflito de interesses:

As decisões comerciais devem ser embasadas nos melhores interesses da VERISURE BRASIL e não em considerações ou relações pessoais. Um conflito de interesses surge quando existe o risco de que uma pessoa (ou seus familiares, amigos, etc.) obtenha um benefício à custa da VERISURE BRASIL. Os empregados devem proporcionar informação completa e imediata sobre qualquer interesse que possam ter, no momento da contratação ou durante o desempenho de sua atividade trabalhista, que crie ou possa criar um potencial risco de conflito de interesses. Qualquer conflito de interesses deve ser comunicado ao seu responsável e autorizado pelo departamento de Recursos Humanos.

Recorde:

- *Informe o seu responsável sobre qualquer possível conflito de interesses.*
- *Mantenha as relações profissionais e imparciais junto a empreiteiras e fornecedores.*
- *Não permita que suas relações pessoais com empreiteiras e fornecedores influam nas decisões de negócio que faça em nome da VERISURE BRASIL.*

Busque o consentimento de Recursos Humanos em situações de conflitos de interesses.

FAÇA ISSO:



- *Se mantiver relações comerciais com parentes, cônjuges ou outras pessoas ou amigos próximos puder dar lugar a um conflito de interesses, deve-se comentar com o seu responsável e coletar a autorização do departamento de Recursos Humanos.*
- *Igualmente, as relações íntimas entre companheiros de trabalho podem, dependendo das funções e dos respectivos cargos, criar um conflito de interesses. Caso você se defronte com a possibilidade de se ver envolto em tal conjectura ou relação pessoal, você deve entrar em contato com o seu responsável e colocar ao conhecimento do departamento de Recursos Humanos para que sejam tomadas as medidas apropriadas para eliminar o conflito.*

NÃO FAÇA ISSO:



- *Trabalhar para empresas concorrentes da VERISURE BRASIL enquanto dure a sua relação de trabalho com a Companhia.*
- *Trabalhar para empresas não concorrentes da VERISURE BRASIL fora do seu horário de trabalho, caso este trabalho sugira uma diminuição do seu rendimento na Companhia.*
- *Realizar tarefas não relacionadas com a VERISURE BRASIL durante o horário de trabalho.*
- *Aceitar dinheiro ou benefícios por qualquer tipo de conselho ou serviço que os empregados possam disponibilizar a um fornecedor em relação ao seu negócio com a VERISURE BRASIL.*
- *Influir na contratação de um familiar dentro da sua área de responsabilidade.*
- *Investimentos pessoais em um fornecedor, colaborador comercial ou na concorrência.*
- *Ter dependência hierárquica com um familiar ou alguém com quem mantenha relações íntimas.*

Tratamento dos recursos da empresa, da informação e do conhecimento:

Os bens da Verisure Brasil são destinados a atingir os objetivos de negócio da Companhia. Os empregados estão obrigados a proteger e a não utilizar indevidamente os bens e os recursos da Companhia.

Os recursos de informação e tecnologia da VERISURE BRASIL (inclusive telefones, computadores, recursos de Internet e email, etc.) são disponibilizados aos empregados para o seu uso profissional.

Os equipamentos informáticos devem ser utilizados em conformidade com a Declaração de Segurança de TI da VERISURE BRASIL.

Todos os empregados que introduzam qualquer tipo de informação nos sistemas informáticos da Companhia devem zelar para que ela seja rigorosa e confiável.

Em todo caso, não será permitida a introdução de informação nos sistemas informáticos que não esteja diretamente vinculada com as atividades realizadas pelo empregado e nunca vulnerando os direitos de propriedade intelectual ou similar aos quais a informação possa estar sujeita.

Os empregados devem respeitar os princípios deste Código de Conduta e, portanto, não devem publicar qualquer comentário depreciativo, ofensivo ou inadequado sobre a VERISURE BRASIL e/ou seus empregados, clientes, fornecedores, outros parceiros comerciais e concorrentes da Companhia.

Igualmente, os empregados não devem escrever, enviar fotos ou vídeos e nem fazer referência a outros empregados, clientes, fornecedores nem sócios do negócio sem o consentimento da pessoa em questão. Além disso, os empregados tampouco devem reclamar, nem insinuar ter autorização para falar como representante da Companhia, nem utilizar logotipos, marcas comerciais, copyrights ou outros direitos de propriedade intelectual da Companhia de qualquer forma.

NÃO FAÇA ISSO:



- *Imprimir, enviar ou copiar em qualquer meio informações confidenciais de nossos clientes.*
- *Partilhar com um terceiro informação da companhia sem autorização do diretor da área*
- *Esquecer que é um representante da Verisure Brasil quando estiver utilizando uniformes ou veículos da empresa, portanto, use-os da forma devida.*

1.2.5 Proteção da informação.

Na VERISURE BRASIL consideramos que a informação é um dos nossos ativos para o desenvolvimento do negócio, então deve ser objeto de uma proteção especial.

Por isso todos que integramos a Companhia devemos transmitir a informação de forma veraz, completa e segura.

Todos os empregados da VERISURE BRASIL têm, no nosso dia a dia acesso à informação confidencial (por exemplo, informação de clientes, dados financeiros, informação de negócios, etc.) que a concorrência desconhece, e tem um valor comercial que todos os empregados da Companhia têm que proteger. Inclusive quando deixamos de trabalhar nela, continuaremos estando obrigados a proteger a confidencialidade desta informação

Relações pessoais:

Se você tiver família e outras relações pessoais com pessoas empregadas pela concorrência, clientes, fornecedores ou colaboradores, você não só deve proteger a informação confidencial da VERISURE BRASIL, mas tampouco deve solicitar informação confidencial deles.

Informação não solicitada:

Se você receber informação não solicitada de um terceiro com informação comercial reservada, devolva ou elimine esta informação e, conforme o caso, responda educadamente ao remetente, pedindo que não envie maiores informações.

Nem sempre fica clara se a informação é confidencial ou não, então, em caso de dúvidas, peça assessoria ao departamento de Assessoria Jurídica.

1.2.6 Segurança e saúde.

Protegemos a saúde, segurança e bem estar dos nossos clientes, empregados e colaboradores.

É responsabilidade de todos tomarem as medidas necessárias para proteger nossa segurança, saúde e bem estar e a dos demais. Por isso, a VERISURE BRASIL se compromete a garantir um ambiente seguro e estimulante, e a apoiar a saúde, o bem estar e o equilíbrio entre a vida profissional e pessoal de todos os empregados..

NÃO FAÇA ISSO:



- Deixar a tela do seu computador aberta com dados de clientes. Você deve bloquear o seu computador ao deixar o seu posto de trabalho.
- Deixar documentos da Companhia em cima de sua mesa ou a de um colega na fotocopiadora ou em salas de reuniões.
- Fazer comentários em nome da VERISURE BRASIL aos meios de comunicação sem ter antes consultado o departamento de Marketing.
- Fazer qualquer declaração em qualquer âmbito que possa ter um impacto negativo na reputação da VERISURE BRASIL ou de sua marca.
- Fazer referência ao seu emprego ou relação com a VERISURE BRASIL em qualquer comunicação pessoal de forma que possa ser interpretada, inclusive por erro, como um comentário ou aprovação por parte da VERISURE BRASIL.
- Divulgar qualquer informação sobre nossos produtos ou serviços sem a correspondente aprovação.
- Ao participar em redes sociais ou páginas similares a título pessoal, não utilize o nome da VERISURE BRASIL, e nunca faça menção a qualquer atividade trabalhista sem consentimento prévio e conhecimento do departamento de Comunicação.

FAÇA ISSO:



- Cumpra com as normas de riscos trabalhistas da VERISURE BRASIL.
- Certifique-se de que nossos fornecedores e colaboradores identifiquem, avaliem e gerenciem os riscos de todas as atividades e serviços empreendidos e dos produtos oferecidos em nome da VERISURE BRASIL e que possam cumprir todas as leis aplicáveis em matéria de saúde e segurança.
- Informe sobre qualquer acidente, prática ou situação insegura imediatamente.

1.3 Obrigação de informação e colaboração: Canal de denúncias



Para preservar o nosso negócio e a reputação da nossa Companhia, todos devemos assumir a responsabilidade de nossas ações e tomar as medidas necessárias caso isso seja contrário às orientações deste Código de Conduta.

Caso você suspeite ou seja testemunha de uma infração deste Código de Conduta, você deve informar sobre isso em primeiro lugar ao seu superior imediato e denunciar igualmente através do canal de denúncias interno, que permite a todos os empregados comunicar as condutas irregulares relacionadas com este Código de Conduta e demais normas aplicáveis.

Este canal de denúncias interno será de muito fácil acesso por meio da intranet corporativa ou através do seguinte endereço de e-mail: **canaldedenuncias@verisure.com.br**.

Você também tem a sua disposição o canal de denúncias gerenciado pelo Grupo Verisure Brasil, **securitas.direct@claimdesk.pwc.se**

A seguir, são detalhadas uma série de situações onde sempre se deve denunciar:

- Falta de integridade.
- Não cumprimento de uma obrigação jurídica que pode criar responsabilidades penais e/ou danos de reputação.
- Não cumprimento ou violação da privacidade dos dados ou da divulgação ilegal da informação delicada e confidencial.
- Violação do direito de concorrência.
- Situações que coloquem em risco a saúde e a segurança dos empregados ou dos clientes e colaboradores.
- Qualquer outra atividade criminal.
- Situações de conflito de interesses.
- Qualquer tentativa de ocultação dos casos anteriores.
- Lavagem de dinheiro, corrupção ou fraude.

A VERISURE BRASIL manterá total confidencialidade no tratamento de denúncias que sejam tramitadas e as investigará imediatamente. As denúncias falsas ou sem fundamento real, com a finalidade de prejudicar o denunciado, serão igualmente investigadas e, conforme o caso, o seu autor será acionado.

FAÇA ISSO:



- Se você se encontrar em uma situação em que, por exemplo, o projeto de um novo produto pode ser inseguro, informe ao seu superior. Caso não queira dizer nada porque considera o risco pequeno, informe a questão à Comissão de Compliance. Não oculte nada que, em sua opinião, coloque em risco a qualidade, o serviço, a reputação ou os interesses da VERISURE BRASIL.

1.4 Regime Sancionador



1.4.1 Comissão de Compliance.

A Comissão de Compliance é o órgão corporativo da VERISURE BRASIL responsável por zelar pelo cumprimento deste Código de Conduta.

Composição:

- Representante da Assessoria Jurídica.
- Responsável por Recursos Humanos.
- Representante de Segurança Corporativa.

Normas de atuação:

A Comissão de Compliance atuará para elucidar, caso possível, se ocorreu o não cumprimento do Código de Conduta e demais normas aplicáveis, assim como o alcance e a sua consequência.

A Comissão de Compliance se compromete a manter a máxima confidencialidade no tratamento de denúncias que sejam tramitadas, assim como respeitar os direitos das pessoas supostamente implicadas em um possível não cumprimento.

As decisões adotadas pela Comissão de Compliance estarão fundamentadas e motivadas, e nunca poderão excluir as possíveis responsabilidades penais, trabalhistas ou civis que possam ser derivadas dos possíveis não cumprimentos.

1.4.2 Medidas sancionadoras.

Para preservar a reputação da Verisure Brasil, todos devemos assumir a responsabilidade sobre nossas ações e tomar as medidas necessárias se algo não acontecer de acordo com o estabelecido pela Verisure Brasil.

Por isso, caso um de nós não cumpra com o estabelecido neste Código de Conduta, serão tomadas medidas sancionadoras para o empregado, que poderão ir desde uma advertência até uma demissão.

POLÍTICA DE CLASSIFICAÇÃO E PROTEÇÃO DA INFORMAÇÃO
Segurança Corporativa
VERISURE BRASIL



Conteúdo

2.1. Objeto

2.2. Âmbito da aplicação

2.3. Graus de classificação

2.4. Relações com terceiros

2.4.1. Fornecedores com acesso à informação classificada da Verisure Brasil

2.4.2. Informação depositada de propriedade de terceiros

2.5. Incidências

2.6. Histórico do documento

Histórico de Revisão

Versão	Autor	Revisão	Motivo da revisão	Data
0.1	Gabriel Blanco	Miguel Munoz	Criação do rascunho do documento	01/12/2014
0.6	Gabriel Blanco	Miguel Munoz	Mudanças na estrutura e conteúdo do documento original.	05/03/2015
1.0	Miguel Munoz	Miguel Munoz	Revisão com mudanças para aprovação final	20/03/2015

Distribuição do Documento

Nível de Confidencialidade	Área
C2 Difusão Limitada	Segurança Corporativa Assessoria Jurídica

2.1. Objeto

Definir e formalizar os graus de confidencialidade e os procedimentos de utilização da informação tratada pela Verisure Brasil Monitoramento de Alarmes (“Verisure Brasil”) , de acordo com sua natureza.

2.2. Âmbito da aplicação

Esta política abrange a Verisure Brasil, e conforme o caso as organizações externas, entidades colaboradoras ou com qualquer tipo de vínculo com a Verisure Brasil, que utilize ou tenha acesso à informação classificada.

Os níveis de cumprimento serão monitorados regularmente e os resultados serão revisados pelos órgãos corporativos apropriados. Qualquer não cumprimento desta normativa será tratado

como uma falta disciplinar grave e poderá estar sujeita a ações disciplinares de acordo com as provisões aplicadas pela política de Recursos Humanos.

2.3. Graus de classificação

A Verisure Brasil estabeleceu para a informação gerada, processada ou distribuída, quatro níveis de segurança, atendendo ao seu grau de confidencialidade, de forma que o Responsável pela informação deverá ser classificado, e aplicadas as medidas de segurança necessárias. As medidas estabelecidas são acumulativas, ou seja, as medidas aplicáveis a um grau serão aplicáveis em níveis superiores.

Os Responsáveis pela informação serão os Diretores dos Departamentos onde seja realizado o tratamento da informação.

C1. INFORMAÇÃO NÃO CLASSIFICADA: toda aquela informação cujo acesso ou divulgação não gere qualquer tipo de ameaça, risco, vulnerabilidade e/ou prejuízo aos interesses da Verisure Brasil, de forma que não exige proteção especial.

C2 DIFUSÃO LIMITADA SD	C3 CONFIDENCIAL SD	C4 RESERVADO SD
Informação de negócio que possa vir a ser compartilhado internamente e com terceiros em determinados casos: Comunicados aos empregados, organogramas. Atas de reuniões não confidenciais. Procedimentos internos. Apresentações não confidenciais.	Informação que, em mãos erradas (internas ou externas) possa gerar uma ameaça ou prejuízo grave aos interesses da companhia: Informação de clientes. Prospectos, leads ou informação relacionada com a geração de novos clientes. Imagens de sistemas de segurança. Informação relacionada com candidatos e empregados. Processos judiciais. Qualquer informação que inclua dados de caráter pessoal, que requeiram medidas de nível básico ou médio.	Informação que requeira o mais elevado grau de proteção, toda vez que sua revelação não autorizada ou uso indevido afete seriamente aos interesses financeiros e imagem da companhia, como: Dados financeiros não publicados, planos de negócios, novos produtos (I+D), compras, fusões e/ou aquisições. Investigações internas ou derivadas do canal de denúncias da companhia. Qualquer informação que inclua dados de caráter pessoal que exijam medidas de segurança de nível elevado Atas e decisões do Comitê de Administração da Companhia.

Nota: Qualquer informação não contemplada nas tipologias anteriores deverá ser encaminhada ao Departamento de Segurança Corporativa, com a finalidade de identifica-la e determinar as medidas de segurança aplicáveis em função da confidencialidade necessária.

Medidas de segurança		
C2 DIFUSÃO LIMITADA SD	C3 CONFIDENCIAL SD	C4 RESERVADO SD

- Durante o traslado de suportes e/ou documentos, os usuários deverão conservá-los, evitando sua perda ou subtração. - A documentação será classificada atendendo o seu grau de confidencialidade (C2, C3 ou C4). - A correspondência por meio de mensagem que contenha este tipo de documentação, não refletirá sua classificação no exterior. Os nomes de documentos e arquivos eletrônicos não devem indicar a classificação de confidencialidade. - A documentação deverá ser armazenada nos arquivos dispostos pela companhia ao finalizar a jornada de trabalho. - A informação deverá ser destruída uma vez que não seja necessária, nos contêineres ou destruidores habilitados.	Todas as medidas do C2 mais: - Não deverá ser armazenada em arquivos individuais dos usuários (físicos nem eletrônicos) devendo aplicar as medidas necessárias para controlar o acesso aos arquivos departamentais. (armários com chave, caixas fortes...). - O envio ou tratamento de informação fora dos locais, deverá estar identificado e autorizado e realizado por meio dos canais seguros proporcionados pela companhia. - A informação deverá ser encriptada ao ser encaminhada através de redes públicas ou de fora da companhia e/ou quando armazenado em dispositivos e suportes suscetíveis de ser utilizados fora dos locais da companhia. - Ao eliminar a informação de suportes reutilizáveis, será excluída de forma que não seja recuperável. Caso o suporte não fosse reutilizável, ele deverá ser destruído em destruidoras ou por meio de um fornecedor autorizado. - Deve-se imprimir informação apenas quando for imprescindível, devendo retirar a informação depois de sua impressão, envio ou cópia.	Todas as medidas do C3 mais: - Devem ser estabelecidos mecanismos que permitam o traçado dos acessos à informação por parte do responsável pela informação. - A informação será armazenada de forma encriptada, seja qual for o suporte eletrônico no qual se encontre. - Articular um sistema de rotulagem compreensível apenas para aqueles que terão acesso ao respectivo suporte.
--	---	--

2.4. Relações com terceiros

2.4.1. Fornecedores com acesso à informação classificada da Verisure Brasil.

Os fornecedores serão convocados a assinar um Acordo de Confidencialidade, como

exigência imprescindível para a prestação de um serviço, devendo o fornecedor encaminhar as condições de confidencialidade de forma expressa ao pessoal que terá acesso à informação da Verisure Brasil. Caso o fornecedor trate de dados de caráter pessoal de responsabilidade da Verisure Brasil, deverá estabelecer um acordo de acesso aos dados com o fornecedor (aprovado pela Assessoria Jurídica), onde sejam indicadas as especificações indicadas na normativa de proteção de dados.

A Verisure Brasil informará aos fornecedores que tratem sua informação da possibilidade de realização de auditorias, da possibilidade de realização de auditorias que verifiquem o cumprimento das medidas de segurança exigidas e/ou acordadas.

2.4.2. Informação depositada de propriedade de terceiros.

A informação depositada na Verisure Brasil que seja de propriedade de um terceiro será protegida de forma similar à própria da Verisure Brasil. Em caso de exigência pelo depositante para a assinatura de um acordo de Confidencialidade ou de tratamento de dados, ele será assinado prévia revisão da área de Assessoria Jurídica.

2.5. Incidências

As incidências que possam ser geradas em relação com a informação classificada (como roubo ou perda), deverão ser notificadas imediatamente à área de Segurança Corporativa, através do seguinte endereço de email: [•]

2.6. Histórico do documento:

Versão	Data	Emitido por	Revisado por	Aprovado por	Mudanças
0.1	02-03-15	Miguel Munoz	IT	Rosa Rodriguez	

POLÍTICA DE DEFESA DA CONCORRÊNCIA
VERISURE BRASIL



POLÍTICA DE DEFESA DA CONCORRÊNCIA
VERISURE BRASIL MONITORAMENTO DE ALARMES

Conteúdo

- 3.1. Introdução
- 3.2. Destinatários
- 3.3. Conceitos básicos sobre as normas de direito da concorrência
- 3.4. Carteis, abuso de posição dominante no mercado e controle de atos de concentração
- 3.5. Descumprimento da Política: investigações e regime sancionador

3.1. Introdução

O objeto desta política é prevenir ou minimizar riscos de violação e descumprimento da Lei nº 12.529 de 30 de Novembro de 2011 que estrutura o Sistema Brasileiro de Defesa da Concorrência (“SBDC”) e demais leis que tratam do assunto.

Os níveis de cumprimento desta política serão monitorados regularmente e os resultados serão revisados pelos órgãos corporativos apropriados. Eventual descumprimento será tratado como uma falta disciplinar grave e poderá estar sujeito a outras ações disciplinares de acordo com o Regime Disciplinar adotado pelo departamento de Recursos Humanos.

3.2. Destinatários

Esta Política abrange a Verisure Brasil Monitoramento de Alarmes (“Verisure Brasil”), assim como todos os seus empregados, que estão obrigados a conhecer detalhadamente os limites e as recomendações que a legislação aplicável estabelece para o desenvolvimento da atividade comercial no Brasil.

Os gerentes e diretores da companhia serão os responsáveis por selecionar, instruir e monitorar suas equipes com o objeto de garantir uma observância plena do conteúdo da legislação antitruste mencionada no item acima.

3.3. Conceitos básicos sobre a Lei de Defesa da Concorrência

O SBDC tem por objetivo a prevenção e a repressão às infrações contra a ordem econômica, de modo a garantir a promoção da livre concorrência e, em última análise, o bem-estar do consumidor.

No Brasil, o Conselho Administrativo de Defesa Econômica ("CADE") tem como missão zelar pela livre concorrência no mercado, sendo a entidade responsável, no âmbito do Poder Executivo, não somente por investigar e decidir, em última instância, sobre a matéria concorrencial, como também fomentar e disseminar a cultura da livre concorrência.

As normas que defendem e incentivam a livre concorrência são de cumprimento obrigatório por parte de todas as pessoas físicas ou jurídicas que desenvolvem uma atividade econômica ou comercial.

As atribuições do CADE são definidas pela Lei 12.529/11 e complementadas pelo Regimento Interno do CADE ("RICADE"). Em resumo, a autarquia exerce três funções:

- **Repressiva:** investigar, em todo o território nacional, e posteriormente julgar cartéis e outras condutas nocivas à livre concorrência.
- **Preventiva:** analisar e posteriormente decidir sobre as fusões, aquisições de controle, incorporações e outros atos de concentração econômica entre grandes empresas que possam colocar em risco a livre concorrência.
- **Educativa:** instruir o público em geral sobre as diversas condutas que possam prejudicar a livre concorrência; incentivar e estimular estudos e pesquisa; dentre outras iniciativas.

O não cumprimento da legislação antitruste leva à imposição de sanções administrativas por infrações à ordem econômica aos responsáveis, sejam eles pessoas jurídicas, pessoas físicas ou, a depender do caso, administradores. Para referência, a multa pode variar de 0,1% a 20% do valor do faturamento bruto da empresa, grupo ou conglomerado obtido, no ramo de atividade empresarial em que ocorreu a infração.

3.4. Cartéis, abuso de posição dominante no mercado e concentrações

3.4.1. Cartéis

Cartel é qualquer acordo ou prática concertada entre concorrentes que, por implicar aumento de preços e restrição de oferta sem qualquer benefício econômico compensatório, causa graves prejuízos aos consumidores.

Estes acordos podem consistir na fixação de preços, limitações à produção e à venda, divisão de mercados e licitações fraudulentas.

Detalhamos a seguir as principais atuações que estão expressamente proibidas:

- Fixação de preços ou medidas de favorecimento (descontos, juros, etc.)
- Fixação de cláusulas de negociação (garantias, condições de pagamento, condições de entrega, etc.)
- Divisão do mercado (regiões, tipo de cliente, etc.)
- Fixação de cota de mercado
- Acordos com fornecedores e provedores
- Acordos relacionados à gama de produtos
- Troca de informações sensíveis (e.g., preços, custos, capacidade, estratégias, fornecedores, clientes, descontos, informações não públicas sobre P&D)
- Licitações fraudulentas

Devemos também ter cuidado com cláusulas que restringem a liberdade de atuação do distribuidor ou do fornecedor e que, portanto, podem causar preocupações do ponto de vista concorrencial:

- Acordos de exclusividade e de não concorrência
- Acordos para limitar os valores de vendas e restrições geográficas ou de tipo de cliente

3.4.2. Abuso de posição dominante no mercado

O abuso de posição dominante no mercado está totalmente proibido. Este abuso tem como base uma posição dominante, que ocorre quando uma empresa ou grupo de empresas controla parcela substancial de mercado relevante como fornecedor, intermediário, adquirente ou financiador de um produto, serviço ou tecnologia a ele relativa de tal forma que a empresa/grupo seja capaz de, deliberada e unilateralmente, alterar as condições de mercado. Como, por exemplo, estabelecer preços abusivos destinados à eliminação de concorrentes do mercado ou mesmo impor exclusividade sem que haja uma justificativa empresarial válida.

A posição dominante no mercado pode ser ostentada por uma única companhia ou várias companhias vinculadas por interesses econômicos sem integrar uma mesma estrutura empresarial.

O principal fator para determinar a existência ou não de uma posição dominante no mercado é a participação que a empresa detém em determinado mercado relevante. Para sua determinação, deve-se analisar o mercado sob o ponto de vista do produto e também geográfico. A Lei nº 12.529/2011 estabelece haver presunção de posição dominante sempre que uma empresa ou grupo de empresas for capaz de alterar unilateral ou coordenadamente as condições de mercado ou quando controlar 20% (vinte por cento) ou mais do mercado relevante, podendo este percentual ser alterado pelo CADE para setores específicos da economia (art. 36 §2º).

É preciso ressaltar que a posição dominante não é, por si só, ilícita do ponto de vista antitruste. Quando é alcançada em decorrência de um processo natural e por ter sido um agente econômico eficiente, o poder de mercado é absolutamente respeitado, desde que não sejam observados abusos em seu exercício.

Por parte da Verisure Brasil devemos ter muito claro qual a nossa participação de mercado para não incorrer em um abuso de posição dominante no mercado.

Detalhamos a seguir as atuações típicas proibidas realizadas por uma companhia que abusa de sua posição dominante no mercado:

- Estabelecimento de condições de venda abusivas
- Tratamento discriminatório a concorrentes sem justificação objetiva
- Recusa injustificada ao fornecimento de equipamentos a um cliente, dentro das condições de pagamento normais aos usos e costumes comerciais
- Fornecimento a um cliente estabelecendo condições pelas quais se obriga a comprar outros produtos que não estão diretamente relacionados com sua atividade
- Concorrência desleal (preço de venda abaixo do custo de fábrica)
- Descontos abusivos

3.4.3. Concentrações empresariais

A concentração empresarial é um controle prévio estabelecido pela legislação antitruste para investigar, no momento da realização de um ato de concentração entre agentes econômicos, os efeitos concorrenciais que a transação acarretará.

3.4.4. Normas de conduta, informação e treinamento

Todos os empregados que integram a Verisure Brasil devem estar cientes que não podemos conversar com concorrentes sobre os seguintes temas, em especial:

- Custos das empresas envolvidas;
- Nível de capacidade e planos de expansão;
- Estratégias de *marketing*;
- Precificação de produtos (preços e descontos);
- Principais clientes e descontos assegurados;
- Salários de funcionários;
- Principais fornecedores e termos de contratos com eles celebrados;
- Informações não públicas sobre marcas e patentes e P&D;
- Planos de aquisições futuras;
- Estratégias competitivas, etc.

Igualmente, estamos obrigados a deixar a reunião que mantemos com concorrentes se durante ela forem citadas possíveis alianças, acordos em matéria concorrencial. É importante que eventual abandono da reunião seja registrado em pauta e reportado ao Departamento Jurídico/de Compliance da Verisure.

Todos os empregados da Verisure Brasil que, devido a suas funções e responsabilidades, possam se ver afetados pelas Leis de Direito de Concorrência devem estar informados e, portanto, devem estar cientes de seu conteúdo e aplicação no caso concreto.

O Departamento de Treinamento liderará o treinamento online ou presencial necessário para cumprir com o anteriormente exposto.

Todas as medidas adotadas pela Verisure Brasil para evitar a prática de infrações da ordem econômica são documentadas e comunicadas anualmente aos órgãos governamentais da Verisure Brasil para seu acompanhamento e melhoria.

É imprescindível que a Verisure Brasil tenha conhecimento da violação ou não cumprimento das normas de defesa da concorrência; assim proceda imediatamente à comunicação aos órgãos de administração da Verisure Brasil, especificamente ao Secretário Geral e ao Diretor Geral Financeiro da Verisure Brasil.

3.5. Descumprimento da Política: investigações e regime sancionador

No caso em que a Verisure Brasil estiver envolvida em uma investigação relacionada a um descumprimento presumido ou violação da legislação de defesa da concorrência, é imprescindível adotar as seguintes indicações:

- O Diretor de Assessoria Jurídica será nomeado como único representante da companhia para tratar com as autoridades de defesa da concorrência
- Este representante coordenará a obtenção e comunicação de toda a informação exigida durante a investigação
- A todo o momento o Departamento Financeiro deverá estar informado dos avanços, exigências e esclarecimentos suscitados durante a investigação em curso
- Uma vez identificados em nossos escritórios os funcionários do órgão inspetor, o representante da companhia deverá solicitar seu reconhecimento e proceder com a obtenção de cópia de seus documentos de identificação.
- Garantir que os funcionários do órgão inspetor deverão, a todo o momento, ser acompanhados pelo representante da companhia, o qual deverá tomar nota e documentar todas as fases da investigação
- Não destruir qualquer documentação durante a inspeção, enquanto essa atuação estiver proibida e, portanto, sujeita a multas pecuniárias muito elevadas

**POLÍTICA SOBRE DELEGAÇÃO DE FACULDADES,
LIMITES E CONTROLES**
VERISURE BRASIL



POLÍTICA SOBRE DELEGAÇÃO DE FACULDADES, LIMITES E CONTROLES

VERISURE BRASIL MONITORAMENTO DE ALARMES

Conteúdo

- 4.1. Introdução
- 4.2. Destinatários
- 4.3. Controles e limites gerais
- 4.4. Controles especiais
- 4.5. Controles e limites contábeis e financeiros: Auditoria
- 4.6. Controles e limites para o investimento
- 4.7. Despesas
- 4.8. Compras
- 4.9. Estado Real
- 4.10. Reclamações e M&A

4.1. Introdução

O objeto desta política é definir e estabelecer os limites e controles corporativos dos Diretores e Gerentes da Verisure Brasil Monitoramento de Alarmes ("Verisure Brasil") no momento da tomada de decisões.

Para tal efeito, foram estabelecidos limites quantitativos, bem como limitações para o seu exercício, juntando diversas faculdades com cargos executivos da Verisure Brasil.

O Conselho de Administração do Verisure Brasil tem faculdades ilimitadas e por isso pode delegá-las funcional e internamente, com certos limites, a Diretores e Gerentes de suas distintas filiais, como é o caso da Verisure Brasil.

Os níveis de cumprimento desta política serão monitorados regularmente e os resultados serão revisados pelos órgãos corporativos apropriados. Qualquer descumprimento será tratado como uma falta disciplinar grave e poderão estar sujeitas outras ações disciplinares de acordo com o Regime Disciplinar adotado pelo departamento de Recursos Humanos.

4.2. Destinatários

Esta Política abrange a Verisure Brasil, bem como todos os seus empregados que ocupem um cargo de direção ou de Gerência, bem como os empregados aos quais foram delegadas diferentes faculdades de representação, disposição, etc.

4.3. Controles e limites gerais

Neste tópico estão estabelecidos controles e limites gerais que devem ser cumpridos sempre e quando estivermos em uma das seguintes situações:

4.3.1. Operações combinadas

Não se pode executar um ato ou operação direcionada a um único destinatário, por duas ou mais pessoas, com o objeto de evadir o limite de autoridade, constituindo uma infração muito grave desta política.

4.3.2. Substituição de faculdades ou de mandato

Nenhum ato ou operação poderá ser executado por um empregado da companhia que não tenha o nível de autoridade exigido para a realização do respectivo ato ou operação, salvo que este empregado ostente capacitação ou faculdade delegada de forma expressa e notarial para tal.

4.3.3. Sistema de documentação de cumprimento

Os empregados que executam contratos ou aprovam operações devem se certificar a todo o momento que:

- dispõem de autoridade e faculdade necessária exigida por esta política
- dispõem da devida autorização interna para a realização ou executar o contrato ou operação
- dispõem do devido instrumento de procuração, nos termos da lei.

4.3.4. Modificação e renovação desta política

Qualquer modificação ou renovação realizada sobre esta política deverá ser realizada e comunicada pelo Conselho de Administração da Verisure Brasil.

4.4. Controles especiais

4.4.1. Aquisições e Desinvestimentos de negócio

Para realizar qualquer tipo de operação de aquisição ou venda de ativos, deve-se contar com autorização formal, expressa e prévia do Conselho de Administração da Verisure Brasil.

4.4.2. Nomes e Marcas Comerciais

Qualquer atividade que implique ou afete nomes e marcas comerciais exige expressamente a aprovação formal e previa do Conselheiro Delegado e do Diretor Financeiro da Verisure Brasil.

4.4.3. Relações com investidores / Relações com os meios de comunicação

Estão autorizados única e exclusivamente para contatar, revelar ou compartilhar informação sobre a Verisure Brasil aos investidores e aos meios de comunicação as seguintes pessoas:

- Membros do Conselho de Administração da Verisure Brasil
- Conselheiro Delegado da Verisure Brasil
- Diretor Financeiro da Verisure Brasil
- Diretor de relações com os investidores da Verisure Brasil

4.5. Controles e limites contábeis e financeiros: Auditoria

4.5.1. Políticas contábeis e financeiras

Qualquer decisão, instrução ou protocolo interno relativo a controles e limites contábeis e financeiros deverá ser aprovado pelo Conselho de Administração da Verisure Brasil, assistido pelo Diretor Geral Financeiro da Verisure Brasil, bem como pelo Diretor Financeiro da Verisure Brasil.

4.5.2. Business plan, orçamento e planejamento

Requer a aprovação previa do Conselho de Administração da Verisure Brasil para a fixação do planejamento, do business plan e do orçamento anual da Verisure Brasil.

4.5.3. Livro diário de assentos contábeis

Qualquer apontamento de assento contábil diário que exceda 0,02 % das receitas da Verisure Brasil, deve ser aprovado previamente pelo Diretor Financeiro da Verisure Brasil.

4.5.4. Fixação de preços

A fixação dos preços deverá estar incluída no orçamento anual da Verisure Brasil e, aprovado pelo Conselho de Administração da Verisure Brasil. Esta fixação de preços deverá estar fundamentada pelo Diretor de Vendas da Verisure Brasil.

Em relação aos créditos documentados, eles devem ser aprovados em conformidade com as Políticas fiscais e de crédito da Verisure Brasil.

4.5.5. Registro Anual

O registro anual da Verisure Brasil deve ser aprovado pelo seu Conselho de Administração. Em relação ao registro anual da Verisure Brasil, ela deve unicamente formular e aprovar se é legalmente exigível pela Lei das Sociedades Anônimas, cumprindo com o controle prévio interno, consistente na sua aprovação por parte do Diretor Geral Financeiro da Verisure Brasil, bem como do Diretor Financeiro da Verisure Brasil.

4.5.6. Auditores de contas

A definição ou fechamento dos auditores de contas no âmbito da Verisure Brasil, exigirá a aprovação do Conselho de Administração da Verisure Brasil.

4.6. Controles e limites para o investimento

Todas as funções e responsabilidades relacionadas à tesouraria da Verisure Brasil devem seguir a todo o momento as linhas e os limites marcados na Política de Tesouraria da Verisure Brasil.

O financiamento intragrupo da Verisure Brasil deverá ser ajustado a todo o momento ao marco legal e às obrigações estabelecidas nos diferentes contratos de financiamento externo da Verisure Brasil.

Cabe ao Tesoureiro da Verisure Brasil o trabalho de velar pelo cumprimento das obrigações estabelecidas nos diferentes contratos de financiamento externo da Verisure Brasil.

4.6.1. Empréstimos, e provisões relacionadas com as instalações

Os empréstimos que constituem o financiamento externo da Verisure Brasil devem ser aprovados anualmente pelo Conselho de Administração da Verisure Brasil.

Será delegada ao Tesoureiro da Verisure Brasil a gestão dos empréstimos citados.

As provisões que forem acordadas na Verisure Brasil deverão contar com a aprovação expressa e prévia do Tesoureiro da Verisure Brasil, e a sua execução acontecerá de acordo com a política corporativa da Tesouraria.

4.6.2. Pedido de financiamento (empréstimos, cartas de crédito, etc.)

Para solicitar financiamento externo para a Verisure Brasil, será necessário contar com a aprovação expressa e prévia do Conselho de Administração da Verisure Brasil.

4.6.3. Garantias

Para outorgar garantias em nome da Verisure Brasil, pedir uma hipoteca ou outorgar garantias sobre os bens da Companhia, se requer autorização prévia e por escrito do Conselho de Administração da Verisure Brasil.

4.6.4. Acordos de financiamento intragrupo

O financiamento intragrupo que afete a Verisure Brasil, assim como as demais filiais da é competência do Tesoureiro da, por meio da supervisão e aprovação do Diretor Geral Financeiro da Verisure Brasil.

4.6.5. Abertura e cancelamento de contas bancárias

Para abrir ou fechar contas bancárias em nome da Verisure Brasil, se requer autorização prévia do Tesoureiro da Verisure Brasil.

4.6.6. Investimentos

Todo o excesso de caixa da Verisure Brasil deve ser investido de acordo com o contemplado na Política Corporativa de Tesouraria, sendo ela aprovada pelo Tesoureiro da Verisure Brasil.

4.6.7. Cartas de crédito, garantias bancárias e assistência financeira

A emissão de fundos em favor da Verisure Brasil deve ser aprovada anualmente pelo Conselho de Administração da Verisure Brasil.

O Diretor Financeiro da Verisure Brasil pode solicitar cartas de crédito, garantias bancárias e demais assistência financeira, sempre e quando conta com a prévia autorização do Diretor Geral Financeiro da Verisure Brasil.

4.6.8. Instrumentos financeiros derivados

O programa de instrumentos financeiros derivados deve ser aprovado anualmente pelo Conselho de Administração da Verisure Brasil. Todas as atividades relacionadas com instrumentos financeiros derivados estão submetidas ao controle do Tesoureiro da Verisure Brasil.

4.6.9 Autorizações e limites

A tabela a seguir abrange as autorizações e limites estabelecidos para as atividades relacionadas nos pontos anteriores (4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7 e 4.6.8)

Nível de Autoridade Atividade	Conselheiro Delegado da Verisure Brasil	Diretor Financeiro da Verisure Brasil	Gerente Regional	Diretor financeiro do país	Chefe de departamento	Centro de custo responsável
	Limite	Limite	Limite	Limite	Limite	Limite
Empréstimos e provisões (instalações)	Quantidade aprovada pelo Conselho de Administração	Quantidade aprovada pelo Conselho de Administração	Quantidade aprovada pelo Conselho de Administração	Quantidade aprovada pelo Conselho de Administração	Não	Não
Pedido de financiamento	Não	Não	Não	Não	Não	Não
Garantias	Não	Não	Não	Não	Não	Não
Financiamento intragrupo	€5M	€5M	€1M	Não	Não	Não
Contas bancárias	Sim	Sim	Não	Sim (Somente Tesoureiro da Verisure Brasil)	Não	Não
Investimentos	De acordo com a Política de Tesouraria Corporativa	De acordo com a Política de Tesouraria Corporativa	De acordo com a Política de Tesouraria Corporativa	De acordo com a Política de Tesouraria Corporativa	Não	Não
Cartas de crédito/garantias	€1M	€1M	Não	Não	Não	Não
Instrumentos financeiros derivados	Quantidade aprovada pelo Conselho de Administração (€30M)	Quantidade aprovada pelo Conselho de Administração	Quantidade aprovada pelo Conselho de Administração	Quantidade aprovada pelo Conselho de Administração	Não	Não

4.7. Despesas

4.7.1 Despesas gerais

Todas as despesas devem ser contempladas no orçamento anual. As faturas movimentadas e contabilizadas pela Verisure Brasil devem ser aprovadas por pessoa autorizada para tal de acordo com os limites estabelecidos no quadro citado no ponto 7.8 deste capítulo.

4.7.2 Investimento de capital - Compra de carteira

Todas as operações financeiras de compra de carteira devem ser contempladas no orçamento anual, que deve ser aprovado pelo Conselho de Administração da Verisure Brasil.

4.7.3 Investimento de capital - Outros

Todas as demais operações financeiras de investimento devem ser aprovadas de acordo com o estabelecido na tabela constante no ponto 7.8 deste capítulo.

4.7.4 Venda de bens

Qualquer operação de venda de ativos da Verisure Brasil (incluindo todas as vendas de equipamentos) à margem do curso ordinário, deverá se notificar e obter autorização do Diretor Geral Financeiro da Verisure Brasil.

Toda operação de venda de ativos da Verisure Brasil, cujo valor total supere € 100.000 , deverá notificar e obter autorização do Diretor Geral Financeiro da Verisure Brasil.

4.7.5 Despesas operacionais

Todas as despesas operacionais devem ser aprovadas de acordo com o estabelecido na tabela constante no ponto 7.8 deste capítulo.

4.7.6 Relatórios de despesas

Todos os relatórios de despesas devem ser aprovados pelo gerente correspondente. Para efeitos práticos, os relatórios de despesas do Diretor Geral do País podem ser aprovados pelo Diretor Financeiro do País antes do pagamento, e pelo Presidente da região com efeitos retroativos de acordo com o ponto 7.7

4.7.7 Gestão de despesas

Todas as despesas pessoais devem ser aprovadas pelo superior direto, conforme o estabelecido na tabela constante no ponto 7.8. Caso não seja possível a aprovação do pagamento antes de sua realização, ele será aproado com caráter anual com efeito retroativo.

Será elaborado um relatório anual das despesas incorridas pelo Presidente e pelo Diretor Financeiro da Verisure Brasil, os quais serão aprovados pelas seguintes pessoas:

- As despesas do Presidente da Verisure Brasil devem ser aprovadas pelo Conselho de Administração da Verisure Brasil.
- As despesas do Diretor Financeiro da Verisure Brasil devem ser aprovadas pelo Presidente da Verisure Brasil.

4.7.8 Autorizações e limites

Nível de Autoridade Atividade	Conselheiro Delegado	Diretor Financeiro	Gerente Regional	Diretor financeiro do país	Chefe de departamento	Centro de custo responsável
	Limite	Limite	Limite	Limite	Limite	Limite
Investimento de capital-Compra de carteira	De acordo com o orçamento	De acordo com o orçamento	De acordo com o orçamento	De acordo com o orçamento	De acordo com o orçamento	De acordo com o orçamento
Investimento de capital	€100.000	€100.000	€50.000	€10.000	€2.500	€1.000
Despesas operacionais (dentro curso ordinário)	De acordo com o orçamento	De acordo com o orçamento	De acordo com o orçamento	De acordo com o orçamento	De acordo com o orçamento	De acordo com o orçamento
Despesas operacionais (fora curso ordinário)	€100.000	€100.000	€50.000	€10.000	€2.500	€1.000

Venda bens (dentro curso ordinário)	€1.000.000	€1.000.000	€10.000	€10.000	€10.000	€10.000
Venda bens (fora curso ordinário)	€1.000.000	€1.000.000	€10.000	€1.000	€1.000	€1.000
Relatório de despesas	€10.000	€10.000	€10.000	€5.000	€5.000	€5.000

4.8. Compras

4.8.1 Termos e condições gerais

Todos os contratos de compra e venda de equipamentos e mercadorias cujo valor anual supere o valor de €1.000.000 devem ser aprovados previamente pelo Presidente da Verisure Brasil, pelo Diretor Geral Financeiro da Verisure Brasil, assim como pelo Secretário Geral da Verisure Brasil.

Este limite quantitativo pode ser aumentado para a Verisure Brasil de acordo com o volume médio de suas operações.

4.8.2 Contratos do cliente

Todas as condições gerais dos contratos de cliente da Verisure Brasil que são modificadas, deverão ser previamente aprovadas pelo Presidente da Verisure Brasil, assim como pelo Secretário Geral e pelo Diretor Geral Financeiro da Verisure Brasil.

4.9. Estado Real

4.9.1 Operações imobiliárias de compra e venda de bens imóveis

Toda operação de aquisição ou venda de bens imóveis deve ser aprovada previamente pelo Conselho de Administração da Verisure Brasil, após receber por parte do Presidente da Verisure Brasil e do Secretário Geral da Verisure Brasil, a documentação necessária para a operação. Igualmente, o Diretor Geral Financeiro da Verisure Brasil deve validar a operação de compra/venda.

4.9.2 Arrendamentos (de imóveis e equipamentos)

Toda operação de arrendamento de bens imóveis deve ser aprovada pelo Conselho de Administração da Verisure Brasil, assim como pelo seu Conselheiro Delegado.

Toda operação de leasing deve ser aprovada previamente pelo Diretor Financeiro da Verisure Brasil, assim como pelo Diretor Geral Financeiro e pelo Tesoureiro da Verisure Brasil.

4.10. Reclamações e M&A

4.10.1 Reclamações

Requer-se a aprovação do Conselho de Administração da Securitas, do Conselheiro Delegado da Verisure Brasil e do Diretor Geral Financeiro da Verisure Brasil para interpor qualquer demanda ou reclamação por um valor superior a €100.000.

É exigida a aprovação do Diretor Geral Financeiro da Verisure Brasil para interpor qualquer demanda ou reclamação por um valor superior a €10.000.

Estes limites podem ser aumentados de acordo com o volume médio de demandas recebidas, assim como a quantidade média objeto de reclamação.

4.10.2 Constituição / Dissolução / Fusão de sociedades comerciais e Joint Ventures

O Secretário Geral e o Diretor Geral Financeiro da Verisure Brasil são os responsáveis por analisar e autorizar conforme o caso toda operação corporativa consistente na constituição ou dissolução de companhias, Joint Ventures, filiais, etc.

**POLÍTICA SOBRE DENUNCIA INTERNA DE IRREGULARIDADES
(WHISTLE BLOWER POLICY)**
VERISURE BRASIL



POLÍTICA SOBRE DENÚNCIA INTERNA DE IRREGULARIDADES (WHISTLE BLOWER POLICY)

Conteúdo

- 5.1. Introdução
- 5.2. Em que consiste a denúncia de irregularidades?
- 5.3. O que eu posso denunciar?
- 5.4. Canal de denúncias
- 5.5. Como denuncio?
- 5.6. Garantias do processo de denúncia

5.1. Introdução

O objeto desta política é incentivar dentro da Verisure Brasil Monitoramento de Alarmes (“Verisure Brasi”) a tolerância zero frente a condutas que possam deixar vulnerável o marco legal vigente e os princípios que formam o nosso Código de Conduta.

Para tanto, contamos com todos vocês, por isso convidamos todos a ler essa política e a utilizar o canal interno de denúncia que temos a nossa disposição para denunciar qualquer irregularidade em nosso posto de trabalho. Temos que conseguir que no nosso dia a dia não se descumpra a normativa legal aplicável nem nosso Código de Conduta.

Os níveis de cumprimento desta política serão monitorados regularmente e os resultados serão revisados pelos órgãos corporativos apropriados. Qualquer não cumprimento será considerado como uma falta disciplinar grave e poderá estar sujeito a outras ações disciplinares de acordo com o Regime Disciplinar adotado pelo Departamento de Recursos Humanos.

5.2. Em que consiste a denúncia de irregularidades?

A denúncia de irregularidades é o complemento necessário para cobrir integralmente todos os canais internos de reporte da informação, através da qual os empregados da Verisure Brasil enfocam de atenção em ações potencialmente ilegais e outros assuntos

que entram em conflito com o nosso Código de Conduta e demais usos e costumes, que põem danificar a imagem e a reputação da Companhia.

5.3. O que eu posso denunciar?

Detalhamos a seguir uma lista de ações e atuações irregulares, que sem ser ampla, abrange as mais frequentes:

- Descumprimento dos princípios que compõem o nosso Código de Conduta
- Descumprimento das seguintes normas: (i) Lei nº 12.843/2014 (“Lei Anticorrupção”); (ii) Decreto nº 8.420/2015; (iii) Lei nº 8.429/1992 (“Lei de Improbidade Administrativa”); e (iv) Lei 12.813/2013 (“Lei de Conflito de Interesses”).
- Más práticas contábeis e financeiras
- Abuso de poder na realização e atuações irregulares não autorizadas pela Companhia
- Discriminação por qualquer motivo durante a contratação ou durante a prestação de serviços a nossos clientes
- Falta de integridade
- Descumprimento de uma obrigação jurídica que possa levar responsabilidades penais e/ou danos de reputação
- Descumprimento ou violação da privacidade dos dados ou da divulgação ilegal de informação delicada e confidencial
- Violação do direito de concorrência
- Situações que coloquem em risco a saúde e a segurança dos empregados ou dos clientes e colaboradores
- Qualquer outra atividade criminal
- Situações de conflito de interesses
- Qualquer tentativa de ocultação dos casos anteriores
- Lavagem de dinheiro, corrupção ou fraude

5.4. Canal de denúncias

Este canal de denúncias interno é de fácil acesso através da internet corporativa ou através do seguinte endereço de e-mail: [•] canaldedenuncias@verisure.com.br

Você também tem a sua disposição o canal de denúncias gerenciado pelo Grupo VERISURE BRASIL: [•] securitas.direct@claimdesk.pwc.se.

5.5. Como denunciar?

A denúncia de qualquer ato ou situação irregular que deixe vulnerável o marco normativo legal e/ou nosso Código de Conduta deve ser denunciado imediatamente através do Canal estabelecido pela Verisure Brasil (ver ponto 4), cumprindo a todo o momento os seguintes requisitos:

- Denúncia por escrito
- Identificação do denunciante
- Breve descrição dos fatos
- Data, hora e lugar de ocorrência dos fatos
- Possíveis terceiros que tenham testemunhado a atuação irregular
- A existência ou não de provas documentais que suportam a denúncia

5.6. Garantias do processo de denúncia

A Verisure Brasil guardará total confidencialidade no tratamento de denúncias que sejam tramitadas e as investigará imediatamente. As denúncias falsas ou sem fundamento real, com a finalidade de prejudicar o denunciado, serão igualmente investigadas e, conforme o caso, será sancionado o seu autor.

POLÍTICA CONTRA SUBORNO E CORRUPÇÃO
VERISURE BRASIL



POLÍTICA CONTRA SUBORNO E CORRUPÇÃO

VERISURE BRASIL MONITORAMENTO DE ALARMES S.A.

Conteúdo

- 6.1. Objeto
- 6.2. Definições
- 6.3. Obrigações e proibições
- 6.4. Requisitos adicionais e diretrizes
- 6.5. Requisitos e padrões sobre a documentação financeira
- 6.6. Não cumprimento da Política

6.1. Objeto.

O objeto desta política é definir e formalizar as obrigações, proibições, medidas a adotar e procedimentos relacionados a práticas de suborno e os atos de corrupção dentro do âmbito de atuação da Verisure Brasil Monitoramento de Alarmes (“Verisure Brasil”).

Esta Política abrange a Verisure Brasil, e em seu caso as organizações externas, entidades colaboradoras ou com qualquer tipo de vínculo com a Verisure Brasil, que utilize ou detenha acesso à informação classificada.

Os níveis de cumprimento serão monitorados regularmente e os resultados serão revisados pelos órgãos corporativos apropriados. Qualquer descumprimento será tratado como uma falta disciplinar grave e poderá estar sujeita a outras ações disciplinares de acordo com o Regime Disciplinar adotado pelo departamento de Recursos Humanos.

6.2. Definições

6.2.1 O que é suborno e corrupção?

Suborno e corrupção significa dar, oferecer ou receber uma recompensa indevida com a intenção de influenciar no comportamento de alguém, sejam elas autoridades públicas ou entidades privadas, nos negócios com a finalidade de obter ou conservar uma vantagem comercial.

O Brasil possui legislação anticorrupção, com as seguintes principais normas: (i) Lei nº 12.843/2014 (“Lei Anticorrupção”); (ii) o Decreto nº 8.420/2015; (iii) Lei nº 8.429/1992 (“Lei de Improbidade Administrativa”); e (iv) Lei 12.813/2013 (“Lei de Conflito de Interesses”).

A violação da lei pode resultar em responsabilidade administrativa ou civil para a Verisure Brasil, assim como responsabilização administrativa, civil ou penal aos seus administradores e demais pessoas físicas que violem a legislação pertinente.

Dessa forma, a Verisure Brasil, bem como todos os seus empregados, deverão cumprir integralmente com as disposições dessas leis.

6.2.2 Quais formas de suborno e corrupção podem ser dadas?

O suborno e a corrupção podem ser materializadas nas seguintes formas: dinheiro em espécie, presentes, doações, entretenimento excessivo ou inapropriado, viagens não relacionadas com assuntos de trabalho ou negócios. Estes são meros exemplos de formas de suborno e corrupção, que podem ainda ser de muito mais tipos. Inclusive sem ser aceita, a oferta ou pedido de suborno ou de um ato de corrupção podem ser considerados ilegais.

6.2.3 Glossário

O termo “Verisure Brasil” se refere e inclui todas as entidades que dependem diretamente da Verisure Brasil, incluindo todas as unidades operacionais, delegações e empregados. Para os fins desta Política, “os empregados da Verisure Brasil” incluem os trabalhadores eventuais como trabalhadores temporários e outro tipo de relações trabalhistas.

O termo vantagem (“Vantagem”) compreende dinheiro em caixa, presentes, doações, refeições / bebidas e outro tipo de entretenimento, serviços, ofertas de trabalho, empréstimos, honorários, viagens, compromissos de compra, comissões, reembolsos e descontos, inclusive em valor nominal. Esta não é uma lista completa das situações que podem ser consideradas como uma vantagem.

Um ponto importante desta Política é a interação com Funcionários. Um “Funcionário” é qualquer empregado do Governo, partido político, candidato político ou qualquer pessoa atuando em nome dos respectivos cargos. Um “Funcionário” inclui qualquer pessoa que: (a) ostente um cargo público ou judicial; (b) seja diretor ou empregado de

qualquer entidade pertencente ao governo; ou (c) seja um empregado de uma organização internacional.

Conhecimento: É considerado como tendo “Conhecimento” se você (i) está consciente de uma ação ou omissão que possa ser conflitante com esta Política, (ii) esteja consciente da possibilidade de produção de uma ação ou omissão que possa conflitar com esta Política.

Negar tal Conhecimento, ignorá-lo deliberadamente, mostrar indiferença e premeditação são consideradas como “Conhecimento” para fins desta Política.

“Representantes de Empresas” : este conceito inclui agentes, *brokers*, representantes, consultores, distribuidores, grupos de pressão, prestadores de serviços e qualquer outra pessoa contratada para atuar em nome e representação da Verisure Brasil para (a) vender ou desenvolver o negócio, ou (b) tratar com autoridades ou Funcionários.

6.3. Obrigações e proibições

Não se pode pagar ou dar qualquer tipo de compensação a ninguém como contraprestação a qualquer benefício ou vantagem obtida quando esta ação seja ou possa ser considerada imprópria.

Não se pode pagar ou dar qualquer tipo de compensação a Funcionários (como propinas ou subornos) para obtenção de aceleração de atuação governamental rotineira em benefício próprio.

Não se deve receber qualquer pagamento ou qualquer tipo de compensação de alguém como contraprestação a qualquer benefício ou vantagem obtida quando esta ação seja ou possa ser considerada imprópria.

Não se pode, sob nenhuma circunstância, pagar por refeições ou outro tipo de entretenimento a qualquer autoridade.

Podem-se realizar convites unicamente para refeições de trabalho ou outro tipo de entretenimentos ocasionalmente a terceiros não vinculados à Verisure Brasil, caso este convite esteja relacionado diretamente com os fins legítimos de trabalho.

Podem-se receber convites para refeições de trabalho ou outro tipo de entretenimentos ocasionalmente por terceiros se esta representação estiver relacionada diretamente com fins legítimos de trabalho.

Não se pode dar, oferecer ou autorizar qualquer vantagem a qualquer pessoa, seja ela funcionária ou não, ou solicitar o mesmo de tais pessoas, com a finalidade de influenciar, induzir, recompensar qualquer ato, omissão ou decisão de garantir uma vantagem inapropriada, e obter ou conservar uma oportunidade de negócio.

Não se pode receber ou solicitar qualquer vantagem de terceiros ou funcionários com a finalidade de dar, induzir ou recompensar qualquer ato, omissão ou decisão de garantir uma vantagem inapropriada, obter ou conservar negócio à conta de, direta ou indiretamente, qualquer pessoa ou funcionário.

Não se pode, sob nenhuma circunstância, oferecer entretenimento ou presentes a Funcionários ou, com base no ponto 4.5, a qualquer outro terceiro incluindo Representantes de Empresas.

Pode-se, por meio de autorização expressa, pagar por refeições e outros tipos de entretenimentos ocasionais sempre que estas atuações estejam diretamente relacionadas com os fins legítimos de negócios e seja razoável em relação ao valor e conteúdo. Qualquer outro convite / entretenimento que implique um Funcionário fica completamente proibido.

Podem-se aceitar convites de refeições de trabalho ou outro tipo de entretenimentos ocasionais de terceiros sempre que estas atuações estejam diretamente relacionadas com fins legítimos de negócios e seja razoavelmente relacionado ao valor e conteúdo. Qualquer outro convite / entretenimento que implique um Funcionário fica completamente proibido.

6.4. Requisitos adicionais e diretrizes

6.4.1 Despesas

Deve-se garantir que todas as despesas são razoáveis em valor e coerentes com a prática habitual de negócio e alinhado com as regras de negócio da Verisure Brasil.

Em caso de conflito entre a prática / cultura de negócio local e as regras de negócio e políticas da Verisure Brasil, sempre prevalecerão as últimas.

Devem-se obter as autorizações necessárias do seu Gerente.

Deve-se, ao pagar refeições ou outro tipo de entretenimento, pagar diretamente as despesas e não financiar a ninguém.

Não se deve incluir ao seu par ou membros de sua família a menos que seja apropriado por meio de determinadas circunstâncias e seja a prática habitual.

Deve-se preparar um relatório de despesas indicando os nomes das pessoas ou entidades envolvidas na finalidade de negócio, e qualquer outra informação relevante, descrevendo detalhadamente a despesa e incluindo o recibo.

6.4.2 Requisitos adicionais relacionados aos Funcionários

Não se devem pagar refeições / bebidas ou outro tipo de entretenimento a nenhum antigo Funcionário caso seja realizado com a intenção ou tenha como fim recompensar pelos serviços prestados quando o Funcionário em questão ostentava tal representação.

Não se deve pagar por refeições / bebidas ou outro tipo de entretenimento a familiares e amigos próximos de um Funcionário público, caso seja realizado com a intenção ou tenha aparência de que seja realizado para influir na decisão do Funcionário.

6.4.3 Reporting

Caso tenha Conhecimento – ver acima o que significa “Conhecimento”- fica obrigado imediatamente a informar acerca desta situação e todas as suas circunstâncias ao seu gerente, diretor de área ou diretor de assessoria jurídica, ou por meio do canal de denúncias. Como está descrito detalhadamente na Política de Denúncias, pode-se denunciar atuações irregulares e suspeitas de alguém fora das instalações de trabalho. Esta oportunidade está disponível para todos os empregados da Verisure Brasil.

6.4.4 Dúvidas e questões

Em caso de qualquer dúvida sobre esta Política ou qualquer queixa relacionada a ela, coloque-se em contato com o seu Gerente ou com o Departamento Legal.

6.4.5 Relações comerciais com Representantes de Empresas.

As leis anticorrupção nem sempre diferenciam entre a conduta da empresa e a conduta de um terceiro atuando em nome e representação da empresa.

Portanto, é obrigação da Verisure Brasil “conhecer seus colaboradores comerciais” e garantir que qualquer Representante de Empresa com quem a Verisure Brasil mantenha relações comerciais, se comprometa a cumprir com esta Política.

Estas proibições são também aplicáveis às atuações de terceiros em nome e representação da Verisure Brasil. Não se pode oferecer qualquer vantagem a um terceiro, incluindo os Representantes de Empresas, com Conhecimento de que toda ou parte da vantagem será oferecida para obter ou preservar um contrato ou negócio, quando eles entrem em conflito com esta Política.

Os gerentes devem ser conscientes de que tratar com certas categorias de terceiros leva a um risco de corrupção e a Verisure Brasil seria legalmente responsável, dessa forma os gerentes terão que supervisionar o cumprimento desta Política. De forma concreta, os gerentes, no momento de firmar acordos junto a terceiros, devem ter a capacidade de classificar a outra parte em uma das seguintes categorias:

- (i) Terceiros atuando em nome da Verisure Brasil.
- (ii) Terceiros (incluindo, mas não se limitando a sócios de empresas conjuntas) sobre as quais a Verisure Brasil tem um elevado grau de controle.
- (iii) Terceiros que, no curso de negociações com a Verisure Brasil, interatuem com Funcionários, e
- (iv) Terceiros organizados e operando em mercados de alto risco.

Para garantir o cumprimento dos requisitos desta Política por colaboradores terceirizados, os gerentes estão obrigados a realizar auditorias, incluindo mas não se limitando à fase pré-contratual, execução de medidas apropriadas de anticorrupção para relações comerciais e fase pós-contratual.

Antes de assinar com qualquer Representante de Empresa, deve-se:

- (i) Realizar um processo de auditoria suficiente para identificar fatores de risco.
- (ii) Advertir aos Representantes de Empresas que a Verisure Brasil tenha uma cultura de cumprimento dos mais elevados padrões éticos e de cumprimento com as leis aplicáveis, e
- (iii) Entregar esta Política aos Representantes de Empresas e salvaguardar por escrito que o Representante de Empresa reconhece que está obrigado com o contido desta Política.

6.5. Requisitos e padrões sobre a documentação financeira

Todos os livros contábeis, registros e contas da Verisure Brasil devem refletir com precisão e clareza os aspectos essenciais e imprescindíveis das operações e cumprir com as políticas contábeis da companhia e requisitos internos de controle, independentemente da magnitude da operação.

Ficam proibidas as seguintes atuações:

Autorizar ou financiar qualquer operação que não esteja discriminada ou refletida nos livros contábeis, registros e contas para qualquer finalidade.

Aprovar, induzir ou realizar qualquer pagamento com a intenção, propósito ou entendimento de que este pagamento seja utilizado com finalidades diferentes aos documentos que refletem o pagamento.

Omitir, falsificar, camuflar ou, de qualquer forma, criar confusão ou refletir assentos contábeis incompletos nos livros contábeis, registros e contas, ou aprovar ou induzir a realização de tais atuações nos livros contábeis, registros e contas de terceiros com os quais a companhia mantém relações comerciais, e

Pagar despesas que são inapropriadas, sem autorizar o suporte da documentação apropriada.

6.6. Descumprimento da Política

Caso se adote e se incorra em uma conduta proibida por esta Política ou pela lei aplicável, esta conduta ficará sujeita a medidas disciplinares, chegando inclusive à extinção de sua relação trabalhista com a companhia. Ignorar esta Política, seu conteúdo, os padrões da Verisure Brasil e a lei não são justificativas em relação a esta Política, e desde sua publicação é de cumprimento obrigatório para todos os treinados na Verisure Brasil.

POLÍTICA DE USO ACEITÁVEL DOS SISTEMAS DE INFORMAÇÃO

VERISURE BRASIL



Conteúdo

7.1. Objeto e Finalidade

7.2. Campo de aplicação

7.2.1. Escopo

7.2.2. Destinatários7.3. Política

3.7.1. Propriedade e uso geral

7.3.2. Segurança e tratamento da informação

7.3.3. Segurança das credenciais e equipamentos

7.3.4. Segurança de email

7.3.5. Uso de email pessoal em meios corporativos

7.3.6. Acesso à Internet

7.3.7. Acesso remoto

7.3.8. Uso de meios próprios

7.3.9. Acessos do administrador de sistemas

7.3.10. Uso não aceitável

7.3.10.1. Uso não aceitável de sistemas e redes

7.3.10.2. Uso não aceitável de email e comunicações

7.3.10.3. Uso não aceitável do acesso à Internet

7.3.11. Blogs e redes sociais

7.3.12. Proteção de informações de caráter pessoal

7.3.12.1. Obrigações.

7.3.12.2. Funções

7.4. Regime disciplinar

7.5. Definições

Controle do Documento

Histórico da Revisão

Versão	Autor	Revisão	Motivo da revisão	Data
1.0	Mario Trotta	Rosa Rodriguez, Bernardino Beotas, Miguel Munoz, Gabriel Blanco	Criação da primeira versão do documento	16/07/2015

Distribuição do Documento

Nível de Confidencialidade	Área
C2 Difusão Limitada	Todas as pessoas e empresas envolvidas com acesso ao uso dos recursos tecnológicos e sistemas de informação de propriedade da Verisure Brasil

Documentos Referenciados

Nome	Descrição
Código de Conduta	Normativa interna que reúne os princípios que conformam a cultura corporativa da Verisure Brasil e que definem o comportamento ético e a integridade pessoal e profissional como forma de entender e desenvolver sua atividade.
Política de Classificação da Informação	Normativa interna que define e formaliza os graus de confidencialidade e os procedimentos de uso da informação tratada pela Verisure Brasil, de acordo com sua natureza.

7.1. Objeto e Finalidade

Este documento tem por objeto regular o uso dos meios, recursos tecnológicos e sistemas de informação de propriedade da Verisure Brasil colocados à disposição dos trabalhadores, assim como garantir a segurança, rendimento, confiabilidade e privacidade das comunicações, preservar a privacidade do pessoal e em geral garantir o cumprimento eficaz das atividades e demais tarefas administrativas que emanam do âmbito estritamente profissional.

A intenção desta política não é a de impor restrições injustificadas. Pelo contrário, o que se pretende é compatibilizar a cultura de abertura, confiança e integridade da Verisure Brasil com o compromisso de proteger as informações dos clientes, empregados, colaboradores e os da própria companhia contra ações ilegais ou prejudiciais.

A Verisure Brasil disponibiliza a seus empregados e colaboradores um conjunto de recursos e ferramentas, com o objetivo único de suportar um desempenho de sua atividade profissional o mais eficiente possível. Entre tais recursos e ferramentas estão todos os sistemas de informações de propriedade da empresa, os equipamentos informáticos (PCs, portáteis, servidores, tablets, dispositivos móveis, sistemas de armazenagem, etc.), infraestrutura de comunicações, conexão com redes internas ou externas, terminais, software, hardware, serviços telemáticos, infraestrutura de redes, acessos à Internet e todos os recursos aos quais o pessoal ou usuário tenha acesso para o cumprimento das tarefas definidas no âmbito profissional.

A segurança da informação é um trabalho em equipe que requer o envolvimento de cada um dos empregados da Verisure Brasil e de seus colaboradores. É responsabilidade de cada usuário conhecer esta política e dar cumprimento.

7.2. Campo de aplicação

7.2.1. Escopo

Por este documento, a Verisure Brasil estabelece a regulação do uso dos recursos tecnológicos e sistemas de informação através do estabelecimento de medidas de cumprimento obrigatório para todo o pessoal, os quais ficam sujeitos a esta política.

Esta política está sujeita a revisões e modificações. Qualquer mudança será comunicada utilizando os métodos oficiais da companhia. Igualmente a última versão estará disponível para sua consulta na Intranet Corporativa.

7.2.2. Destinatários

O conteúdo deste documento tem como destinatários todos os empregados da Verisure Brasil e os terceiros que tenham acesso à utilização dos recursos tecnológicos e sistemas de informação de propriedade da Verisure Brasil.

Os diferentes administradores de sistemas e pessoal da área de Segurança de TI estão legitimados para realizar revisões de controle sobre o cumprimento das especificações da normativa de segurança desenvolvida a este respeito e integra suas obrigações a realização destes controles.

Igualmente, as pessoas integrantes da área de Segurança de TI e da área de Segurança Corporativa estão legitimadas para supervisionar e auditar em toda organização o cumprimento desta política e as normas que a desenvolvem, e a execução das funções de controle.

7.3. Política

7.3.1. Propriedade e uso geral

O uso dos recursos e do material disponibilizado pela Verisure Brasil deverá ser direcionado ao cumprimento das finalidades previstas para a execução das funções encomendadas. Portanto, como norma geral não se possibilita a utilização de seus recursos pelos empregados e colaboradores com fins pessoais ou alheios aos objetivos próprios da posição de trabalho correspondente.

Ainda que de forma excepcional possa dar-se um uso privado dos sistemas, os usuários devem ser conscientes de que as informações criadas nos sistemas corporativos são de propriedade da Verisure Brasil. A necessidade de proteger os sistemas de informação faz com que não se possa garantir a privacidade da informação armazenada nos sistemas corporativos.

A empresa poderá realizar as investigações e controles que sejam necessários tanto de equipamentos como das ferramentas fornecidas ao usuário por parte da empresa, o que inclui, entre outros o e-mail corporativo, computadores, dispositivos moveis, *tablets*, sistemas de armazenagem, etc.

Igualmente e em virtude do disposto na Lei nº 6.404/76 ("Lei das Sociedades Anônimas"), os administradores têm os deveres de diligência, lealdade, sigilo, de informar, etc, para assegurar o controle da atividade empresarial e coibir a prática de ilícitos.

Os direitos e deveres expostos sugerem que a vigilância e o controle pela empresa do uso dos sistemas de informação são necessários e inalienáveis.

Como consequência de tal, o controle e acesso aos meios disponibilizados pela empresa, incluindo os documentos gerados, as comunicações que partam deles e inclusive a localização geográfica do sistema utilizado poderá ser realizado sem uma justificação específica, de forma temporária ou permanente, dada conta da natureza de tais meios como ferramentas de produção disponibilizadas pela empresa. O controle destes meios serão realizados sem danificar e sem atentar contra a dignidade ou intimidade do usuário.

As finalidades genéricas deste controle são as seguintes:

- Quando da existência de indícios razoáveis de que possam estar cometendo delitos ou faltas utilizando os sistemas de informação corporativos.
- Proteção do sistema e rede informática e dos equipamentos que o integram, a fim de proteger a integridade do Sistema e a Segurança da Informação.
- Garantir a continuidade do trabalho no caso de que o usuário se ausente por qualquer motivo.
- Prevenção da responsabilidade frente a terceiros.
- Garantir o cumprimento das obrigações profissionais do usuário.
- Comprovação da existência ou não do uso abusivo dos meios tecnológicos disponibilizados pela empresa.

7.3.2. Segurança e tratamento da informação

A informação contida nos sistemas deverá ser classificada de acordo com o seu grau de confidencialidade seguindo a Política Corporativa de Classificação da Informação definidas pela Área de Segurança Corporativa.

7.3.3. Segurança das credenciais e equipamentos

Todo usuário autorizado tem acesso aos sistemas informáticos utilizando credenciais (contrassenhas, usuários, cartões de acesso, etc.) que os identificam e que são pessoais e intransferíveis. Deve tratá-las com a máxima diligência e confidencialidade, sendo o único responsável do seu bom uso. O titular autorizado será o responsável por todo o executado nos sistemas utilizando essas credenciais.

O usuário é responsável por utilizar senhas seguras e de não compartilhar contas. Os usuários autorizados são responsáveis pela segurança de suas contrassenhas e de suas contas.

O usuário deverá bloquear o seu equipamento quando estiver ausente do posto de trabalho para evitar o acesso não autorizado ao sistema durante esse tempo.

Nos casos em que a informação seja reservada ou confidencial, deve-se encriptar essa informação de acordo com os padrões marcados pela área de Segurança de TI da Verisure Brasil.

Todos os dispositivos que se conectam à rede corporativa devem cumprir com as medidas de segurança requeridas pela Verisure Brasil para poder realizar essa conexão.

Os empregados e colaboradores se comprometem a avisar aos administradores de sistemas ou a área de Segurança de TI de qualquer incidência ou anomalia detectada nos acessos aos sistemas de informação ou na sua segurança.

Os empregados e colaboradores se comprometem em caso de roubo, furto ou danos infligidos por terceiros, a interpor a denúncia correspondente perante as autoridades competentes e a notificar a Área de Segurança Corporativa da empresa.

Qualquer empregado ou colaborador responderá pelos danos causados por negligência ou dolo no sistema ou material informático.

7.3.4 Segurança de e-mail

A Direção da Empresa disponibilizou um endereço individual de e-mail àqueles usuários que a exigiram para o desempenho das funções do seu posto de trabalho. Visto que é faculdade da empresa a organização do e-mail e o sistema que deva ser seguido, com liberdade absoluta para decidir sobre suas condições, a Verisure Brasil se reserva, em função das necessidades de que cada posto de trabalho presente a cada momento, a possibilidade de manter, modificar ou suprimir o uso de tal ferramenta.

Com a finalidade de evitar sobrecargas ao sistema informático encarregado pelo serviço de e-mail, a companhia se reserva o direito de estabelecer cotas de espaço disponível para cada conta de correio, podendo se restringir de forma automática ao envio e/ou recepção de mensagens caso o limite estabelecido seja superado.

Os empregados e colaboradores devem ser especialmente cautelosos quando da abertura de anexos ao e-mail para evitar a distribuição de software malicioso. Ou seja, software designado para danificar ou para realizar ações indesejadas no dispositivo.

Os empregados e colaboradores, uma vez extinta sua relação com a Verisure Brasil, cessarão imediatamente o uso do e-mail corporativo.

Em nenhum caso se produzirá responsabilidade da empresa nem qualquer obrigação de comunicar os

conteúdos dos correios que possam ser recebidos posteriormente ao respectivo término, salvo que seja encaminhada advertência de forma expressa e justificada, que deverá especificar os correios sobre os quais possa ser necessário atuar de forma excepcional.

No momento da extinção do contrato, o trabalhador estará obrigado a proceder com a devolução em devidas condições de todo o material informático proporcionado pela empresa com toda a informação profissional armazenada, bem como facilitar as chaves de acesso ao seu computador, programas, bancos de dados, arquivos protegidos, Intranet, Internet e e-mail.

A empresa poderá dispor do equipamento informático do empregado em questão na mesma data de sua relação de trabalho.

No momento de finalização da relação de trabalho com a Empresa, a obrigatoriedade de confidencialidade permanecerá vigente, proibindo-se expressamente que o empregado se aproprie de qualquer informação, lista ou conteúdo dos bancos de dados, arquivos, pastas ou disco rígido aos quais tenha tido acesso por motivo de seu vínculo profissional com a empresa, salvo os arquivos que incluam itens do próprio empregado e os arquivos relacionados a sua agenda e contatos pessoais.

7.3.5 Uso de e-mail pessoal em meios corporativos

O uso de contas de correio pessoais, com base no acesso web, está permitido caso seja usado com moderação. Ou seja, de forma que não interfira no seu trabalho habitual e possa ser possível sua utilização fora do horário de trabalho.

O acesso deverá ser exclusivamente àqueles e-mails que sejam de plena confiança, e em nenhuma hipótese devem ser links ou downloads de arquivos anexos no computador do usuário ou de outros usuários, ainda que sejam provenientes de pessoas conhecidas, para evitar assim a infecção por vírus ou códigos maliciosos.

Em nenhum caso o email pessoal deverá ser utilizado para armazenar ou compartilhar informação pertencente à Verisure Brasil.

O usuário deve ser consciente de que o uso de e-mail pessoal também estará sujeito às medidas de controle mencionadas no ponto 3.1 e que deve ser considerado em suas expectativas de privacidade.

7.3.6 Acesso à Internet

A Verisure Brasil admite que em determinadas circunstâncias se faça uso privado moderado do acesso à Internet para necessidades dos usuários que sejam alheias ao desempenho profissional para a empresa. Este uso privado não deve interferir com o seu trabalho habitual e, caso possível, deve ser realizado fora do horário de trabalho. Este uso nunca poderá ser para outras atividades profissionais do usuário.

De acordo com o estabelecido no ponto 3.1, a navegação por Internet poderá ser monitorada por um software adequado para filtrar os acessos às páginas que, ao ver do administrador sejam consideradas inapropriadas para a empresa. Ou seja, que sejam desnecessárias para a atividade profissional, perigosas para a integridade dos sistemas de informação ou que estejam relacionados com atividades que atentem contra a legislação vigente.

A navegação por páginas web, o envio de mensagens, registros, liberações, preenchimento de formulários e qualquer outra atividade realizada via Internet, serão de completa responsabilidade do usuário emissor e, em todo caso, deverá assumir as consequências oriundas de sua atuação.

7.3.7 Acesso remoto

As conexões dos empregados, fornecedores, clientes e demais agentes com privilégios de acesso remoto à rede corporativa tem a mesma consideração que a conexão direta dos usuários à rede.

O usuário se responsabiliza de que nenhuma outra pessoa, incluindo membros de sua família, faça uso da conexão em questão.

Para ter acesso, o usuário deve respeitar as condições impostas pela empresa, incluindo de forma não exclusiva a política de encriptação, acesso vpn, acesso wireless e a política de uso aceitável.

A conexão remota estará estritamente controlada e monitorada.

Não será permitida a conexão de equipamentos que não cumpram com os critérios mínimos estabelecidos pela empresa (versão do sistema operacional, patches de segurança aplicados, software instalado, instalação de antivírus com as assinaturas atualizadas, etc.)

7.3.8 Uso de meios próprios

A norma é não autorizar o uso de dispositivos ou sistemas de armazenagem próprias para gerenciar a informação da companhia, salvo que para um caso justificado e se tenha permitido de forma expressa. Nos casos em que este uso tenha sido autorizado, o usuário deverá aceitar esta política e se certificar do cumprimento do ora incluído. Especialmente, deve-se cumprir as seguintes regras:

- Os administradores de sistemas tem o direito de recusar a conexão de um determinado dispositivo próprio do usuário em qualquer momento.
- Antes de efetuar a conexão, o dispositivo deve ter sido aprovado pelo departamento de sistemas.
- Os usuários que queiram conectar um sistema próprio ao ambiente corporativo devem cumprir com as medidas de segurança exigidas pela Verisure Brasil.
- O usuário aceita que seus equipamentos que se conectem ao ambiente corporativo sejam inspecionados e monitorados pelos administradores de sistemas para garantir que cumprem com as diretivas de segurança requeridas.

7.3.9 Acessos do administrador de sistemas

Os privilégios de acesso conferidos aos administradores de sistemas, são necessários entre outras coisas para realizar a gestão dos sistemas de informação da companhia, assim como a resolução de incidências que possam ocorrer, embora seja necessário citar que tais privilégios deverão ser utilizados unicamente para o desenvolvimento necessário de suas funções, estando sujeitos, assim como os demais empregados, à observação e cumprimento desta política.

O administrador de sistemas se obriga a atuar com absoluta diligência, guardando total confidencialidade sobre as informações, documentos, e demais informações as quais se pode ter acesso no exercício de suas tarefas. A título de exemplo, porém não limitativo, pode-se incluir os seguintes:

- Acesso aos equipamentos e sistemas de informação para a realização de tarefas de manutenção.
- Autorizar os acessos dos usuários aos sistemas de informação que requerem para o cumprimento de suas tarefas, assim como aos equipamentos informáticos, conjuntamente com a Área de Segurança de TI.

- Acesso aos equipamentos, redes ou sistemas de informação por incidências na Segurança da Informação.

7.3.10 Uso inaceitável.

Em circunstância alguma, estará um empregado ou colaborador da Verisure Brasil autorizado a realizar atividades ilegais abrangidas dentro das leis locais ou internacionais utilizando recursos da companhia.

Os usuários se comprometem a respeitar e colaborar com os diferentes administradores e pessoal de segurança da companhia. Qualquer situação que sugira intromissão no seu trabalho será considerado como um fato não aceitável sujeito a medida disciplinar contida neste documento.

Os usuários se comprometem a respeitar a integridade dos recursos e sistemas de informação aos quais tenham acesso para o cumprimento das tarefas dentro do âmbito exclusivamente profissional. Fica explicitamente proibido proceder com qualquer terceiro a comissão de qualquer dos casos listados a seguir a título de exemplo.

3.10.1 Uso inaceitável de sistemas e redes

- Tentar acessar aos sistemas ou recursos aos quais não disponha de autorização expressa por parte do administrador de sistemas.
- Alterar de forma total ou parcial os componentes de hardware, software e as configurações dos sistemas operacionais dos equipamentos informáticos definidos ao mesmo usuário ou a outros usuários sem a devida autorização.
- Utilizar meios próprios não autorizados para acessar informação da companhia.
- Não se permite conexão simultânea a outras redes não controladas nem autorizadas pela empresa enquanto se mantenha a conexão à rede corporativa.
- Utilizar aplicações informáticas que saturem as redes, os servidores ou que entorpeçam o funcionamento dos equipamentos informáticos.
- Fazer modificações privilegiadas ou permissões sem autorização do administrador de sistemas.
- Evadir qualquer das medidas de segurança implantadas.
- Utilizar qualquer forma de monitoria das comunicações para interceptar dados não direcionados a esse usuário (a não ser que seja parte de seu trabalho habitual). Aqui se inclui de forma não excludente os escaneamentos de portas e ferramentas de auditoria de rede.
- Ocasionar danos físicos ou lógicos, pelo mau uso ou negligência aos equipamentos informáticos, aplicações, ferramentas informáticas e todo dispositivo ou meio tecnológico.
- Desenvolver ou usar de forma intencionada programas maliciosos nos sistemas de informação da companhia.
- Descuidar de forma negligente de chaves, contrassenhas, nomes de usuários ou quaisquer outros identificadores que possam ser disponibilizados ao trabalhador para utilizar qualquer das ferramentas, ou para ter acesso aos equipamentos ou sistemas da Empresa.
- As violações dos direitos protegidos por copyright, patentes, segredo comercial ou qualquer outra propriedade intelectual ou leis ou regulações similares, incluindo de forma enunciativa a instalação ou distribuição de software sem a devida licença de uso (software “pirata”)

- A utilização de ativos da companhia para realizar ofertas de produtos ou serviços fraudulentos.

7.3.10.2 Uso inaceitável de e-mail e comunicações

- A utilização de forma imprópria do e-mail, especialmente quando se trata de usar este recurso para o envio de anexos e outros elementos multimídia que além de impactar negativamente no rendimento dos recursos compartilhados de infraestrutura, possam atentar contra as ideias, crenças, princípios éticos ou morais e a legislação vigente. Serão evitados de forma escrupulosa os conteúdos de caráter violento, racista, sexista, pornográfico.
- A utilização do e-mail com fins lucrativos ou comerciais em ações que não guardem relação com a atividade profissional. Fica rigorosamente proibida a utilização do e-mail correspondente ao posto de trabalho para o desempenho de qualquer atividade profissional, por conta própria ou alheia, diferente da função desempenhada na Verisure Brasil. Para tais efeitos serão considerados incluídos na proibição os avisos, cruzamento de correspondências e similares que, ainda sem conteúdo diretamente profissional, colaboram na manutenção dessa atividade profissional alheia.
- Envio de mensagens em massa, e mensagens comerciais sem dispor da devida autorização ("spam").
- A suplantação da do endereço de e-mail, como por exemplo, seu uso para buscar respostas encaminhadas a outro destinatário legítimo.
- O reenvio de documentação própria do trabalho confidencial a contas de e-mails pessoais ou que não se encontrem sob o controle da empresa sem a devida autorização.

7.3.10.3. Uso inaceitável do acesso à Internet

- O acesso a páginas com conteúdo ilícito, material pornográfico, de conteúdo racista, sexual, ou qualquer material que possa atentar contra a dignidade.
- Alojamento de documentação própria de tratamento em sistemas externos de armazenagem que não estejam sob o controle da empresa.
- O download de qualquer objeto de fonte não suficientemente bem comprovada, de forma que possa colocar em risco a integridade dos sistemas de informação da Verisure Brasil.
- Desconsiderar as medidas de controle e filtragem de conteúdo em acesso à Internet

7.3.11. Blogs e redes sociais

Os empregados que participam em redes sociais e (qualquer tipo de publicação na Internet, como blogs, Twitter, Facebook, YouTube e meios de comunicação similares) devem ser conscientes de que suas mensagens, inclusive fora do trabalho, poderiam ter um efeito negativo para a Verisure Brasil.

- Os empregados devem respeitar os princípios do Código de Conduta Corporativo e, portanto, não devem publicar qualquer comentário discriminatório, difamatório, depreciativo nem ameaçador sobre a Verisure Brasil e/ou os empregados, clientes, fornecedores, outros sócios comerciais e concorrentes da companhia.
- Igualmente, os empregados não devem escrever, enviar fotos ou vídeos nem fazer referência a outros empregados, clientes, fornecedores nem sócios do negócio sem o consentimento da pessoa em questão.
- Os empregados não devem atribuir julgamentos nem opiniões pessoais em nome da Verisure

Brasil a menos que estejam previamente autorizados para isso. Tampouco poderão ser utilizados logotipos, marcas comerciais, copyrights ou outros direitos de propriedade intelectual da Verisure Brasil sem a requerida autorização.

- Caso um empregado expresse suas opiniões e crenças relacionadas à Internet, o empregado deve assumir que não está fazendo em nome da companhia, e portanto deve assumir o risco em caso de realização.

7.3.12. Proteção de informações de caráter pessoal

Fica estabelecida por meio da seguinte notificação as funções e obrigações que cada um dos usuários ou perfis de usuários com acesso às informações de caráter pessoal deve cumprir.

7.3.12.1. Obrigações.

Toda pessoa que tenha acesso a informações de caráter pessoal deverá considerar as seguintes normas:

- Comunicar o uso ou manutenção de arquivos de informações de caráter pessoal que a organização não tenha contemplado.
- Não poderá retirar da organização informações de caráter pessoal sem ter uma autorização para tal e sem aplicar mecanismos para garantir sua segurança como, por exemplo, a encriptação. Fica incluído dentro deste processo a informação e anexos trocados por meio de e-mail.
- Guardar com a devida diligência as informações de caráter pessoal às quais tem acesso.
- Não poderá distribuir nem armazenar informações utilizando sistemas alheios à companhia tais como Dropbox, OneDrive ou Google Drive, sem a devida comunicação e autorização. Caso ela tenha sido concedida, deve-se aplicar as medidas para garantir a todo o momento a confidencialidade das informações, aplicando mecanismos para impedir que alguém com acesso não autorizado possa ter acesso ao conteúdo carregado.
- Não poderá difundir a informação dos dados pessoais tratados, nem fazer um uso diferente daquele cometido para o qual se tenha solicitado.
- Cada pessoa tem em sua posse contas para o acesso às informações ou aplicações que dão suporte. Não poderão ser utilizadas contas genéricas que sejam empregadas por diferentes pessoas sem que exista a possibilidade de identificação. Garantir a segurança implica, entre outros aspectos a capacidade de realizar o traçado de acesso, permitindo que, em caso de incidência, possa conhecer quem ou como foi provocado.
- Não será possível eliminar informação sem uma autorização ou uma solicitação expressa para tal.
- Não será possível armazenar informações de caráter pessoal em um suporte temporário sem a aplicação das medidas necessárias. Será considerado um suporte temporário aqueles criados para a realização de trabalhos auxiliares. Se entenderá como exemplo de trabalho temporário a impressão de um documento com conteúdo de informações de caráter pessoal. Todo o conteúdo temporário deverá ser excluído ou destruído uma vez que tenha deixado de ser necessário para os fins que motivaram sua criação.
- Não será possível se desfazer dos suportes (temporários ou não) que tenham armazenado as informações de caráter pessoal sem aplicar medidas que garantam que eles não possam ser recuperados por qualquer metodologia.

7.3.12.2. Funções.

Serão funções de toda pessoa que fizer tratamento de informações de caráter pessoal:

- Fazer uso razoável e proporcional da informação tratada.
- Utilizar corretamente os sistemas de informação necessários para o tratamento de informações de caráter pessoal, de acordo com as condições de segurança definidas pela companhia.
- Comunicar ao responsável correspondente a necessidade de saída de dados de informações de caráter pessoal da organização. Esta saída não poderá ser realizada sem a devida autorização.
- Deve-se informar sobre aquelas incidências que tenham acontecido com as informações de caráter pessoal. Serão entendidas como exemplo de incidência toda alteração generalizada da informação existente, o desaparecimento de diversos registros do banco de dados ou acessos ilícitos à informação.
- Comunicar a recepção de exercícios de direitos de Acesso, Retificação, Cancelamento ou Oposição (ARCO) à área de Segurança Corporativa por meio de canais estabelecidos para permitir contestação tal e como exige a normativa de proteção de informações.

7.4. Regime disciplinar

Por meio deste documento, a Verisure Brasil disponibiliza a seus empregados e colaboradores as normas para o uso dos sistemas de informação.

O uso inapropriado, abusivo, ou que fuja dos hábitos tolerados dos serviços de comunicação e dos meios tecnológicos levará à retirada do acesso aos recursos e a aplicação de sanções disciplinares derivadas pelo não cumprimento dos termos e condições oriundos da relação trabalhista, de acordo com os convênios coletivos aplicáveis.

7.5. Definições

Sistemas de informação: Conjunto de recursos direcionados à coleta, tratamento, manutenção, uso, disposição e distribuição de informações e informação, organizados e prontos para cobrir uma necessidade ou objetivo.

Política de uso: Conjunto de disposições que regulam a utilização aceitável dos sistemas de informação e recursos tecnológicos destinados ao cumprimento dos objetivos da empresa.

Usuário: Se refere a toda pessoa que utiliza, dentro do âmbito profissional, os sistemas de informação e os recursos tecnológicos de propriedade da empresa.

Administrador de sistemas: Responsável da gestão e administração dos sistemas de informação, assim como de atentar ao estrito cumprimento da política de uso de meios tecnológicos.

Área de Segurança de TI: Responsável por dirigir as medidas e ações para o cumprimento desta política, assim como de resolver problemas e incidências de segurança oriundos da utilização dos sistemas de informação.

Código de Conduta: Normativa interna que reúne os princípios que conformam a cultura corporativa da Verisure Brasil e que definem o comportamento ético e a integridade pessoal e profissional como forma de entender e desenvolver sua atividade.

Política de Classificação da Informação: Normativa interna que define e formaliza os graus de confidencialidade e os procedimentos de uso da informação tratada pela Verisure Brasil, de acordo com a sua natureza.



VERISURE BRASIL MONITORAMENTO DE ALARMES S.A.

Avenida Brigadeiro Faria Lima, 1485
Conj. 51, Torre Norte
São Paulo - SP

T +55 11 4002 7222



