SGSI01 – Security Policy

Information classification:

Document level	Documentación General
File name	SGSI01-SecurityPolicy.docx
Type	Public reach
Distribution scope	All employees, clients, providers
Responsible	Security Information Officer

CHANGE CONTROL				
Date	**Version**	**Description**	**Reviewed by**	**Approved by**
02/08/2024	1.0	Preliminary version of the document and approval	Security Officer	Management

INDEX

1. INTRODUCTION

This document outlines the principles underlying the Security Policy of **ESTUDIO CACTUS MEDIA SL.** These sets of fundamental principles have been formulated based on valid business needs, recognition of the added value of the systems to be protected, and an understanding of the risks associated with these systems. It is important to note that this Policy will be maintained, updated, and tailored to the objectives of **ESTUDIO CACTUS MEDIA SL**, aligning with the organization's risk management context.

2. SCOPE

2.1. Employees

Information Security is a collective effort. It requires the involvement and participation of all members of the organization who work with Information Systems. Therefore, each employee must comply with the requirements of the Security Policy and its associated documentation. Employees who deliberately or negligently fail to adhere to the Security Policy will be subject to disciplinary actions as outlined in this document.

2.2. Information Systems

This policy applies to all information assets of the company, including personal devices or servers, networks, applications, operating systems, and business processes that belong to and/or are managed by **ESTUDIO CACTUS MEDIA SL.**

This policy addresses aspects most directly related to the responsibility and proper use by personnel.

2.3. Third Parties

This Security Policy must be known and adhered to by any external person from third-party entities who handles information owned by ESTUDIO CACTUS MEDIA SL.

Likewise, this Policy and its associated procedures are mandatory for third-party vendors contracted to perform professional services in relevant areas. If these vendors engage in any activity involving access to or handling of any system or information owned by ESTUDIO CACTUS MEDIA SL, they must comply with this Policy, as will be defined in their contracts.

3. MAINTENANCE, APPROVAL AND REVIEW OF THE POLICY

The Information Security Officer is responsible for creating, maintaining, and publishing the Information Security Policy. However, the approval of this Policy lies with the Management of **ESTUDIO CACTUS MEDIA SL**.

Any change or development that affects or could affect the content of the Information Security Policy will be recorded in a new approval document signature. This process formalizes and confirms the commitment of these entities to information security.

The validity and relevance of this policy will be reviewed periodically, and in any case, within a maximum period of one year. Necessary improvements, adaptations, or modifications will be implemented based on applicable organizational, technical, or regulatory changes.

4. DISTRIBUTION OF THE POLICY

The distribution of this document (Information Security Policy) will be done via email initially and will also be accessible to all personnel in a designated repository. Any substantial changes to the document will be distributed to all users through a formal notification sent by email and subsequently updated in the repository.

5. SANCTIONS

Any deliberate or negligent violation of security policies and standards that poses potential harm, whether accomplished or not, to **ESTUDIO CACTUS MEDIA SL** will be sanctioned according to the mechanisms established in the company's agreement and the current legal, contractual, and corporate regulations.

All employees who use information systems and services are required to report any incident, anomaly, or weakness related to information security to the appropriate responsible party. This communication should be made at the time the incident occurs or as soon as it becomes known.

The Security Officer, upon being informed of the security incident, will classify and detail it according to its severity and will attempt to resolve it as quickly as possible. Incidents are categorized as follows: VERY SEVERE, SEVERE, and MINOR, to facilitate the execution of appropriate actions.

Incidents with a low impact will be considered minor offenses, including the following:

- Forgetting to lock the computer by a user.
- Leaving documents containing personal or confidential data in printers, photocopiers, scanners, faxes, etc., without retrieving them.

Incidents with a considerable impact will be considered severe offenses, including the following:

- Attempts to access company resources without authorization.
- Degradation of service in protected domain systems.
- Unauthorized access to or reading of information contained in files or information systems, both automated and non-automated (paper-based).
- Misuse of user accounts and passwords.

Incidents with an extreme impact on company services will be considered very severe offenses, including the following:

- Unauthorized access to offices, files, cabinets, rooms, data centers, and premises housing information systems.
- Massive virus infection.
- Unauthorized access with theft of secret or confidential information.
- Leaks of confidential information.
- Unauthorized copying of information.
- Unauthorized deletion of information.

The maximum sanctions that may be imposed for the aforementioned offenses are as follows:

I. For minor offenses:

- Written reprimand.

II. For severe offenses:

- Written reprimand.
- Suspension from employment and salary for two to ten days.

III. For very severe offenses:

- Written reprimand.
- Suspension from employment and salary for ten to sixty days.

The Security Officer will determine the root cause of the security incident, identifying the person or persons presumed responsible. They will ensure that the reported security incident does not conceal a more severe incident that could affect a larger number of assets or processes. Subsequently, they will study the best way to resolve the issue.

If the Security Officer believes they lack sufficient expertise, they may consider involving other company personnel or even external experts specialized in resolving such security incidents.

If the information system allows, efforts will be made to gather audit trails and similar evidence, including checking the file access logs, if available, and the most recent user activities.

Once the security incident has been resolved, it must be ensured that the affected area is left with all the security measures that have been established. A brief description of the alleged facts, their potential classification, and any applicable sanctions should be provided.

Finally, the Human Resources Officer will review security incidents caused by personnel, especially if they are severe or very severe, and will decide on the appropriate disciplinary procedure in each case.

Any actions compromising the security of **ESTUDIO CACTUS MEDIA SL** that are not covered by this policy must be reviewed by Management and the Information Security Officer to issue a resolution in accordance with the company's criteria and applicable legislation.

6. INFORMATION SECURITY POLICY

In response to a new technological environment where the convergence of IT and communications is facilitating a new productivity paradigm for businesses, **ESTUDIO CACTUS MEDIA SL** is highly committed to maintaining a competitive service by offering a responsible business model based on the ongoing pursuit of economic, social, and environmental balance. Developing good practices in Information Security is crucial to achieving the objectives of confidentiality, integrity, availability, and legality of all managed information.

Accordingly, **ESTUDIO CACTUS MEDIA SL** defines the following principles to be considered within the framework of the Information Security Management System (ISMS):

Confidentiality: The information handled by **ESTUDIO CACTUS MEDIA SL** will be known exclusively by authorized individuals, following identification, at the appropriate time, and through the designated means.

Integrity: The information handled by **ESTUDIO CACTUS MEDIA SL** will be complete, accurate, and valid, reflecting the content provided by the relevant parties without any manipulation.

Availability: The information handled by **ESTUDIO CACTUS MEDIA SL** will be accessible and usable by authorized and identified users at all times, ensuring its persistence against any anticipated contingencies.

Legality: ESTUDIO CACTUS MEDIA SL will ensure compliance with all applicable legislation or contractual requirements, specifically including current regulations related to the processing of personal data.

To effectively carry out its business functions, **ESTUDIO CACTUS MEDIA SL** relies on and processes various types of data and information, supported by systems, programs, communication infrastructures, files, databases, archives, etc. These elements constitute some of the primary assets of **ESTUDIO CACTUS MEDIA S**L, such that damage to or loss of them impacts service delivery and could jeopardize the organization's continuity. To prevent such scenarios, an Information Security Policy has been designed with the following main objectives:

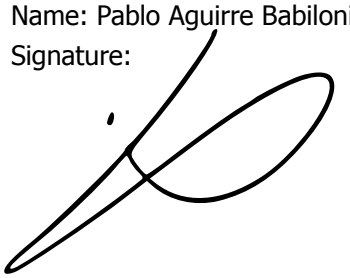
- Protect assets through controls and measures against threats that could lead to security incidents.
- Mitigate the effects of security incidents.
- Establish an information and data classification system to protect critical information assets.
- Define responsibilities for information security, creating the appropriate organizational structure.
- Develop a set of rules, standards, and procedures applicable to management, employees, partners, external service providers, etc.
- Specify the consequences of non-compliance with the Security Policy in the workplace.
- Assess risks affecting assets to adopt appropriate security measures and controls.
- Verify the effectiveness of security measures and controls through internal security audits conducted by independent auditors.
- Train users in security management and information and communications technologies.
- Monitor the flow of information and data through communication infrastructures or via optical, magnetic, or paper-based data carriers.
- Observe and comply with legislation related to data protection, intellectual property, labor, information society services, criminal law, etc., that affects **ESTUDIO CACTUS MEDIA SL**'s assets.
- Protect the organization's intellectual capital to prevent unauthorized disclosure or misuse.
- Reduce the risk of unavailability through proper use of organizational assets.
- Defend assets against internal or external attacks to prevent them from becoming security incidents.
- Monitor the performance of security measures by tracking the number, nature, and effects of incidents.

The Management of **ESTUDIO CACTUS MEDIA SL** assumes responsibility for supporting and promoting the implementation of the necessary organizational, technical, and control measures to ensure compliance with this Information Security Policy. They are also responsible for providing the resources needed to address non-conformities and information security incidents as swiftly and effectively as possible, and for implementing measures to prevent their recurrence.

This Policy will be maintained, updated, and aligned with the organization's objectives, in accordance with its risk management context. It will be reviewed at planned intervals or whenever significant changes occur to ensure its continued suitability, adequacy, and effectiveness.

Similarly, to manage the risks faced by **ESTUDIO CACTUS MEDIA SL**, a formally defined risk assessment procedure will be established.

All policies and procedures included in the ISMS will be reviewed, approved, and endorsed by the Management of **ESTUDIO CACTUS MEDIA SL**.

APPROVED BY: Management
Name: Pablo Aguirre Babiloni Signature:  Date: 02/08/24

SGSI01 – Política de Seguridad

Clasificación de la Información:

Nivel del Documento	Documentación General
Nombre del Fichero	SGSI01-PolíticaDeSeguridad.docx
Tipo	DIFUSIÓN LIMITADA
Ámbito de Difusión	Todos los empleados
Responsable	Responsable de Seguridad de la Información

CONTROL DE MODIFICACIONES				
Fecha	**Versión**	**Descripción**	**Revisado**	**Aprobado**
22/03/2022	1.0	Versión preliminar del documento	Responsable de seguridad	Dirección
23/06/2022	2.0	Aprobación del documento	Responsable de seguridad	Dirección
22/01/2024	3.0	Revisión y aprobación del documento	Responsable de seguridad	Dirección

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

En este documento se describen los principios donde se sostiene la Política de Seguridad de **ESTUDIO CACTUS MEDIA SL**. Estos conjuntos de principios fundamentales han sido formulados basándose en necesidades válidas de negocio, reconocimiento del valor añadido de los sistemas a proteger y una compresión de los riesgos asociados a estos sistemas.

Destacar que esta Política será mantenida, actualizada y adecuada a los fines de **ESTUDIO CACTUS MEDIA SL**, alineándose con el contexto de gestión de riesgos de la organización.

2. ALCANCE

2.1. Empleados

La Seguridad de la Información es un esfuerzo conjunto. Requiere la implicación y participación de todos los miembros de la organización que trabajan con Sistemas de Información. Por ello, cada empleado debe cumplir los requerimientos de la Política de Seguridad y su documentación asociada. Los empleados que deliberadamente o por negligencia incumplan la Política de Seguridad serán sujetos a acciones disciplinarias según se contempla en este documento.

2.2. Sistemas de Información

Esta Política afecta a todos los activos de Información de la empresa, tanto a equipos personales o servidores, redes, aplicaciones, Sistemas Operativos, procesos de la empresa que pertenecen y/o son administrados por **ESTUDIO CACTUS MEDIA SL**.

Esta política cubre los aspectos más directamente relacionados con la responsabilidad y buen uso del personal.

2.3. Terceras Partes

La presente Política de Seguridad es de extensible conocimiento y cumplimiento para cualquier persona externa perteneciente a terceras entidades que realice cualquier tipo de tratamiento sobre la información propiedad de **ESTUDIO CACTUS MEDIA SL**.

Asimismo, esta Política y sus procedimientos asociados serán de obligado cumplimiento para las empresas terceras proveedoras contratadas para la ejecución de servicios profesionales en los ámbitos que se consideren oportunos, en el caso de que realicen cualquier actividad que implique acceso o tratamiento a cualquier sistema o información propiedad de **ESTUDIO CACTUS MEDIA SL** y así se definirá contractualmente.

3. MANTENIMIENTO, APROBACIÓN Y REVISIÓN DE LA POLÍTICA

El Responsable de Seguridad de la Información es el responsable de construir, mantener y publicar la Política de Seguridad de la Información, si bien, es la Dirección de **ESTUDIO CACTUS MEDIA SL** la responsable de la aprobación de dicha Política.

Cualquier cambio o evolución que afecte o pudiera afectar al contenido de la Política de Seguridad de la Información quedará registrado en una nueva firma del documento de aprobación. De esta forma se concreta y confirma el compromiso de estas entidades por la seguridad de la información.

Periódicamente, y en todo caso no superando el plazo de un año, se revisará la vigencia y razonabilidad de la presente política y se llevarán a cabo las mejoras, adaptaciones o modificaciones requeridas en función de los cambios organizativos, técnicos o regulatorios aplicables**.**

4. DISTRIBUCIÓN DE LA POLÍTICA

La distribución del presente documento (Política de Seguridad de la Información), se realizará mediante correo electrónico en primera instancia y, además, quedará accesible para todo el personal en un repositorio dispuesto al efecto.

Cualquier cambio sustancial en el documento será distribuido a todos los usuarios a través de una notificación formal, enviada por correo electrónico y seguidamente será actualizado en el repositorio.

5. SANCIONES

Cualquier violación premeditada o negligente de las políticas y normas de seguridad y que suponga un potencial daño, consumado o no a **ESTUDIO CACTUS MEDIA SL,** será sancionada de acuerdo con los mecanismos habilitados en el convenio de Empresa y en la normativa legal, contractual y corporativa vigentes.

Todos los empleados, que sean usuarios de los sistemas y servicios de información tienen la obligación de notificar al responsable correspondiente cualquier incidencia, anomalía o debilidad asociada a la seguridad de la información. Dicha comunicación se deberá realizar en el momento en que se produzca la incidencia o desde el momento en que se tenga conocimiento de la misma.

El Responsable de Seguridad, nada más comunicado el incidente de seguridad, lo catalogará y especificará su detalle, atendiendo a la gravedad del mismo, intentará solucionarlo a la mayor brevedad posible.

Se categorizan las incidencias en los siguientes términos: MUY GRAVE, GRAVE y LEVE, para facilitar la ejecución de las acciones a tomar frente a las mismas.

Se considerarán faltas leves, los incidentes con un impacto bajo, señalando las siguientes:

- Olvido del bloqueo de ordenador por parte de un usuario.
- Olvido de documentos en impresoras, fotocopiadoras, escáneres, faxes, etc. que contienen datos personales o confidenciales y no han sido retirados.

Se considerarán faltas graves, los incidentes con un impacto considerable, señalando las siguientes:

- Intentos de acceso no autorizado a recursos de la empresa.
- Degradación de servicio en los sistemas del dominio protegible.
- Acceso o lectura no autorizada de información contenida en ficheros o sistemas de información, tanto automatizados como no automatizados (soporte papel).
- Uso indebido de las cuentas y contraseñas de usuario.

Se considerarán faltas muy graves, los incidentes con un impacto extremo en los servicios de la empresa, señalando las siguientes:

- Accesos no autorizados a despachos, archivos, armarios, salas, CPD y a dependencias en las que residen sistemas de información.
- Infección masiva por virus.
- Accesos no autorizados con robo de información secreta o confidencial.

- Fugas de información confidencial.
- Copia no autorizada de la información.
- Borrado no autorizado de la información.

Las sanciones máximas que podrán imponerse por la comisión de las faltas señaladas son las siguientes:

I. Por faltas leves:

- Amonestación por escrito.

II. Por faltas graves:

- Amonestación por escrito.
- Suspensión de empleo y sueldo de dos a diez días.

III. Por faltas muy graves:

- Amonestación por escrito.
- Suspensión de empleo y sueldo de diez a sesenta días.

El Responsable de Seguridad determinará la raíz del incidente de seguridad, identificando a la persona o personas presuntamente responsables, velando por que el incidente de seguridad notificado no esté encubriendo un incidente de seguridad de mayor gravedad que pueda afectar a un mayor número de activos o procesos y posteriormente, estudiará la mejor forma de solucionarlo.

En caso de que estime que no tiene los conocimientos suficientes, podrá estimar necesaria la participación de otro personal de la empresa o incluso de personal ajeno a la misma especializado en la resolución de ese tipo de incidentes de seguridad.

En caso de que el sistema de información del fichero lo permita, se intentarán recoger pistas de auditoría y otras evidencias similares, consultando, entre otros, el registro de accesos al fichero en caso de estar disponible, junto a las últimas operaciones realizadas por los usuarios.

Se debe asegurar que, una vez finalizada la resolución del incidente de seguridad, la parte afectada se ha dejado con todas las medidas de seguridad que hayan sido establecidas para el mismo, realizando una descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponderle.

Y finalmente, el Responsable de Recursos Humanos analizará los incidentes de seguridad causados por el personal, en el caso de que hayan sido graves o muy graves, y decidirá el procedimiento disciplinario a aplicar en cada caso.

Todas las acciones en las que se comprometa la seguridad de ESTUDIO CACTUS MEDIA SL y que no estén previstas en esta política, deberán ser revisadas por la Dirección y por el

Responsable de Seguridad de la Información para dictar una resolución sujetándose al criterio de la empresa y la legislación prevista.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones están facilitando un nuevo paradigma de productividad para las empresas, **ESTUDIO CACTUS MEDIA SL**, está altamente comprometido con mantener un servicio competitivo a través de ofrecer un modelo de negocio responsable basado en la búsqueda permanente del equilibrio económico, social y ambiental, donde el desarrollo de buenas prácticas en Seguridad de la Información es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad y legalidad de toda la información gestionada.

En consecuencia, a lo anterior, **ESTUDIO CACTUS MEDIA SL**, define los siguientes principios de aplicación a tener en cuenta en el marco del Sistema de Gestión de Seguridad de la Información (SGSI):

- **Confidencialidad**: La información tratada por **ESTUDIO CACTUS MEDIA SL** será conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.
- **Integridad**: La información tratada por **ESTUDIO CACTUS MEDIA SL** será completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.
- **Disponibilidad**: La información tratada por **ESTUDIO CACTUS MEDIA SL** estará accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.
- **Legalidad**: **ESTUDIO CACTUS MEDIA SL**, garantizará el cumplimiento de toda legislación o requisito contractual que le sea de aplicación. Y en concreto, la normativa en vigor relacionada con el tratamiento de datos de carácter personal.

ESTUDIO CACTUS MEDIA SL para el correcto desempeño de sus funciones de negocio se basa y ayuda del tratamiento de diferentes tipos de datos e información, sustentados por los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyendo éstos, uno de los activos principales de **ESTUDIO CACTUS MEDIA SL**, de tal manera que el daño o pérdida de los mismos inciden en la realización de sus servicios y

pueden poner en peligro la continuidad de la organización. Para que esto no suceda, se ha diseñado una Política de Seguridad de la Información cuyos fines principales son:

- **Proteger**, mediante controles/medidas, **los activos** frente a amenazas que puedan derivar en incidentes de seguridad.
- **Paliar** los efectos de **los incidentes** de seguridad.
- **Establecer** un sistema de **clasificación de la información** y los datos con el fin de proteger los activos críticos de información.
- **Definir las responsabilidades** en materia de seguridad de la información generando la estructura organizativa correspondiente.
- **Elaborar** un conjunto de **reglas, estándares y procedimientos** aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- **Especificar** los efectos que conlleva el **incumplimiento** de la Política de Seguridad en el ámbito laboral.
- **Evaluar los riesgos** que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- **Verificar** el funcionamiento de las **medidas/controles de seguridad** mediante auditorías de seguridad internas realizadas por auditores independientes.
- **Formar a los usuarios en la gestión de la seguridad** y en tecnologías de la información y las comunicaciones.
- **Controlar el tráfico de información y de datos** a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- **Observar y cumplir la legislación** en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los activos de **ESTUDIO CACTUS MEDIA SL**.
- **Proteger el capital intelectual de la organización** para que no se divulgue ni se utilice ilícitamente.
- **Reducir** las posibilidades de **indisponibilidad** a través del uso adecuado de los activos de la organización.

- **Defender los activos** ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- **Controlar el funcionamiento de las medidas de seguridad** averiguando el número de incidencias, su naturaleza y efectos.

La Dirección de **ESTUDIO CACTUS MEDIA SL** asume la responsabilidad de apoyar y promover el establecimiento de las medidas organizativas, técnicas y de control necesarias para el cumplimiento de la presente Política de Seguridad de la Información. Así como, de proveer de aquellos recursos que sean necesarios para resolver con la mayor rapidez y eficacia posible, las no conformidades e incidentes de seguridad de la información que pudiesen surgir, y la puesta en funcionamiento de las medidas necesarias para que éstas no vuelvan a ocurrir.

Esta Política será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos de la organización. A este efecto se revisará a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

De igual forma, para gestionar los riesgos que afronta **ESTUDIO CACTUS MEDIA SL** se establece un procedimiento de evaluación de riesgos formalmente definido.

Por su parte, todas las políticas y procedimientos incluidos en el SGSI serán revisados, aprobados e impulsados por la Dirección de **ESTUDIO CACTUS MEDIA SL**.

APROBADO POR: Dirección

Nombre: Pablo Aguirre Babiloni

Firma:

Fecha: 22/01/24