viafirma

Sistema de Gestión de la Seguridad de la Información

Política de seguridad de la información

ÍNDICE

CONTROL DE DOCUMENTO

Título:	Sistema de Gestión de la Seguridad de la Información		
Asunto:	Política de seguridad de la información		
Versión:	1.4	**Fecha:**	15-01-2019
Código:	PS-12	**Última revisión:**	10-02-2021
Idioma:	Es_ES	**Núm. Páginas:**	7

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	**Versión**	**Motivo del Cambio**
15-01-19	1.0	Primera versión
22-01-19	1.1	Se elimina el alcance y se hace referencia a los objetivos del SGSI.
08-04-19	1.2	Adaptación a eIDAS – PSC
20-09-19	1.3	Se incluye apartado en referencia a TSA
10-02-21	1.4	Se amplía la política de seguridad

Elaborado	**Revisado**	**Aprobado**
Mamen Maya Fernández	Comité de Seguridad	Antonio Cabrera Jiménez
Responsable de Seguridad de la información	Comité de seguridad	Director

1. INTRODUCCIÓN

Este documento describe la política de la seguridad de la información.

Seguridad significa disponer de medios que permitan reducir lo más que se pueda, la vulnerabilidad de la información y de los recursos; aunque no se puede alcanzar el 100% de seguridad, la tendencia debe ser llegar a ese valor extremo.

La información constituye uno de los recursos principales de una organización, por lo tanto, se la debe proteger, mediante un conjunto de actividades, controles y políticas de seguridad que se deben implementar en base a recursos humanos, hardware y software.

La seguridad de la información depende de la gestión y los procedimientos adecuados, de los empleados de la organización, proveedores, clientes, accionistas y del nivel de seguridad de los medios técnicos.

1.1. Ámbito de aplicación

La presente Política se aplicará a viafirma, vinculando a todo su personal, independientemente de la posición y función que desempeñe.

De conformidad con la política, viafirma podrá desarrollar procedimientos e instrucciones para implementar y dar cumplimiento a las obligaciones asumidas.

Asimismo, la aplicación de esta política es complementaria a otras normas internas de obligado cumplimiento, como el cumplimiento en materia de protección de datos personales y privacidad, y aquellas otras que regulen cuestiones relacionadas con la información de viafirma.

La presente política estará disponible en la carpeta pública del gestor documental OpenKM para todos los empleados y estará disponible para todos los grupos de interés de la organización en la web corporativa.

1.2. Activos de la organización

Los activos asociados a los sistemas de información de viafirma se clasifican de la siguiente manera:

Información: En este grupo podemos englobar las bases de datos, guías y manuales, procedimientos operativos o de soporte, planes de continuidad, información archivada, disposiciones de emergencia para la recuperación de información, entre otros.

Software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y utilitarios.

Equipos: servidores, HSM, equipos de empleados, dispositivos móviles, Router, Switches, SAI, etc.

Servicios: servicios de comunicaciones, de soporte, de desarrollo, de RRHH, aquí englobaríamos todos los servicios internos de la organización.

Servicios subcontratados: todos los servicios externos que la empresa subcontrata, aunque sean para gestión interna.

Personal: todos los empleados de la organización.

Edificios: oficinas, Datacenter externo y alojamiento cloud.

La seguridad debe permitir proteger las siguientes características de la información:

Confidencialidad, es decir, que la información sea conocida únicamente por personas autorizadas.

Integridad, cuyo contenido no debe ser alterado a menos que sea modificado por personal autorizado.

Disponibilidad, es decir, la capacidad de estar siempre disponible para ser procesado por personas autorizadas.

Autenticidad: La información es válida y utilizable.

Anualmente, si no hiciera falta antes, se lleva a cabo un análisis de riesgos con la herramienta PILAR donde conoceremos las amenazas que afectan a nuestros activos y las salvaguardas que debemos aplicar para reducir, asumir, transferir o mitigar los riesgos resultantes del análisis de riesgos.

2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Viafirma tiene implantado un sistema de gestión de seguridad de la información basado en la norma internacional ISO/IEC 27001/2013.

Este sistema permite identificar y minimizar los riesgos actuales a los que se expone la información, ayudando a reducir costes operativos e implementando una cultura de seguridad y una garantía de cumplimiento de estándares y regulaciones legales y contractuales en la organización.

Viafirma se constituye en Prestador Cualificado de Servicios de Confianza, ofreciendo en primera instancia un servicio cualificado de Sellado de Tiempo (Autoridad de Sellado de Tiempo: TSA - TimeStamp Authority). En los documentos "Viafirma_CP_Certificados_TSU" y "Viafirma_TSA_CPS", se recogen las políticas y declaración de prácticas del servicio de Sellado de Tiempo de Viafirma respectivamente, cuyo objeto es la expedición de sellos electrónicos cualificados de tiempo, así como los aspectos más relevantes y procedimientos definidos para la gestión del servicio.

Viafirma quiere asegurar la información en los servidores internos y los servidores de terceras partes que dan servicios a estas aplicaciones.

Viafirma ha establecido las siguientes políticas generales de seguridad de la información:

1. Existe un Comité de Seguridad de la Información, que es el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información.
2. Los activos de información de Viafirma son identificados y clasificados para establecer los mecanismos de protección necesarios.
3. Viafirma ha definido y ha implantado controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la organización.
4. Viafirma ha establecido unos objetivos de seguridad del SGSI, definidos en el PE-18-00_Objetivos de Seguridad.
5. Todas las personas de la organización son responsables de proteger la información a la que acceden y procesan, para evitar su pérdida, alteración, destrucción o uso indebido.
6. Se realizan auditorías y controles periódicos sobre el modelo de gestión de seguridad de la información y sus objetivos.
7. Es responsabilidad de todas las personas de Viafirma informar sobre los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
8. Viafirma cuenta con un Plan de Continuidad del Negocio que asegura la continuidad de las operaciones.

Además, viafirma ha desarrollado políticas específicas y que dan soporte a la política corporativa, como son:

- Política de teletrabajo.
- Política de dispositivos móviles.
- Política de puesto de trabajo.
- Política de controles de acceso.
- Política de gestión de contraseñas.
- Política de Backups y copias de seguridad.
- Política de destrucción segura de elementos de almacenamiento de la información.
- Política de controles criptográficos.
- Política de desarrollo seguro.
- Política de Prestador de Servicios de Confianza.
- Política de Sellado de Tiempo.

Fdo. Antonio Cabrera Jiménez (CEO viafirma)

En Sevilla, a 10 de febrero de 2021.