Política General de Seguridad de la Información

Fidelizador SpA

Código	P01
Versión	2.0
Fecha de la versión	21/07/2023
Creado por	Oficial de Seguridad (CISO)
Aprobado por	Gerente General
Nivel de confidencialidad	Público

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
20/07/2023	2.0	AO	Se crea versión con nueva estructura en base a Política de Seguridad de la Información original.

Tabla de contenidos

Objetivo

Fidelizador SpA, empresa de servicios de arriendo de software en la nube para empresas (SaaS) fundada el 2007, reconoce la importancia y el valor de la información generada, almacenada y transportada tanto para el negocio como para sus clientes. Debido a esto, ha implementado un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO 27001, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

Alcance

Este SGSI tiene como objetivo el resguardo de la confidencialidad, integridad y disponibilidad de la información y los activos de información relacionados con la prestación del servicio de arriendo de software en la nube para empresas (SaaS) Fidelizador.com, en específico, los servicios de Fidelizador Email Marketing, Fidelizador Comunicaciones Internas, Fidelizador Relay, Fidelizador Docs, Fidelizador SMS y Fidelizador Whatsapp, así como también la seguridad de datos transferidos por los clientes a **Fidelizador SpA** y los datos capturados y almacenados por Fidelizador por orden de los clientes como parte de la prestación de los servicios.

Terminología

- **Activos de Información:** corresponden a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para **Fidelizador SpA**, colaboradores y sus partes interesadas. Es decir, cualquier cosa que tenga valor para la organización y que; a) sea información o b) que la almacene y/o la procese.

- **Información:** es la interpretación que se da a un conjunto de datos, pudiendo residir esta en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con la prestación de los servicios de **Fidelizador SpA**, así como antecedentes proporcionados tanto por colaboradores, internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

- **Información pública**: se refiere a la información que se puede compartir libremente tanto interna como externamente. No presenta riesgo si se difunde ampliamente.

- **Información restringida**: se refiere a la información que no es necesariamente confidencial, pero su acceso y distribución deben limitarse a ciertos individuos o departamentos dentro de la organización.

- **Información confidencial**: se refiere a la información cuya divulgación no autorizada podría generar perjuicios a la organización o a sus clientes. El acceso a esta información se restringe a individuos específicos que la necesitan para desempeñar sus tareas.

- **Información secreta**: es la clasificación de seguridad más alta y se aplica a la información cuya divulgación no autorizada podría causar un daño grave a la organización. Esto podría incluir planes estratégicos, secretos comerciales, información de propiedad exclusiva, o información altamente sensible del cliente.

- **Confidencialidad**: es la propiedad de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. Este concepto se aplica tanto a la información en tránsito como a la almacenada y a los procesos que la manejan. En términos sencillos, la confidencialidad se refiere a la protección de los datos contra la divulgación no autorizada.

- **Integridad**: es la propiedad de proteger la exactitud y completitud de los activos de información. Es el mantenimiento de la consistencia, coherencia y fiabilidad de los datos durante todo su ciclo de vida. En otras palabras, la integridad se refiere a la protección de los datos contra la modificación no autorizada.

- **Disponibilidad**: es la propiedad de estar accesible y utilizable a petición de una entidad autorizada. La disponibilidad se refiere a la garantía de que los usuarios autorizados tienen acceso a la información y a los recursos asociados cuando lo necesiten.

- **Uso aceptable**: todo uso respecto a un activo y/o información en el marco de su diseño y propósito y para quienes poseen acceso a este.

- **Oficial de seguridad** o Chief Information Security Officer **(CISO)**: autoridad máxima designada para la definición, diseño, implementación y supervisión de las medidas de seguridad de la información.

- **Norma o Estándar**: documento oficial publicado por una entidad reconocida a nivel internacional, como la Organización Internacional de Normalización (ISO), que proporciona directrices, reglas, o principios para las actividades o sus resultados y que ayudan a hacer operativas las directrices definidas por una organización. En el caso específico de la ISO 27001, esta norma proporciona un marco para la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI).

- **Política**: se refiere a los principios, reglas y directrices formuladas por la Alta Dirección de una organización para alcanzar sus objetivos a largo plazo. En el contexto de la seguridad de la información, una política es un documento que define el enfoque de la organización para manejar la seguridad de la información y los procedimientos específicos que deben seguirse.

- **Proceso**: conjunto de actividades relacionadas o que interactúan que transforman entradas en salidas. Los Procesos ayudan a la organización a poner en práctica de manera efectiva una Política, un Estándar o un Control. Sin Procesos documentados, no habrá evidencia defendible de las prácticas de debida diligencia.

- **Riesgo**: se define como el efecto de la incertidumbre en los objetivos y se refiere a la posibilidad de que una amenaza explote una vulnerabilidad para causar daño a un activo de información.

- **Amenaza**: es un posible peligro que puede explotar una vulnerabilidad para violar la seguridad y causar daño a la organización. Las amenazas pueden ser de muchos tipos, como los hackers, los virus, los desastres naturales, etc.

- **Vulnerabilidad**: es una debilidad en un sistema que puede ser explotada por una amenaza. Las vulnerabilidades pueden ser de muchos tipos, como errores de software, configuraciones incorrectas, falta de formación del personal, etc.

- **Control**: en el marco de ISO 27001, un control es cualquier medio que se utilice para manejar los riesgos de seguridad de la información. Esto puede ser cualquier cosa, desde

políticas y procedimientos, hasta hardware o software, o incluso formación y concienciación. Los controles son los medios que se utilizan para mitigar/reducir los riesgos.

- **Control normativo**: es aquel control perteneciente a alguna norma o estándar y que la empresa decide aplicarlo. En el caso de la norma ISO 27001, los controles normativos corresponden a los listados en el Anexo A y su aplicabilidad en **Fidelizador SpA** se define en la Declaración de Aplicabilidad.

- **Declaración de aplicabilidad**: Es un documento que establece qué controles del Anexo A de la norma ISO 27001 la organización ha decidido aplicar o no aplicar, y las justificaciones para tales decisiones.

- **Métricas**: es una medida cuantitativa que se utiliza para evaluar el rendimiento o la efectividad de un proceso, control, sistema, etc. En la gestión de la seguridad de la información, las métricas pueden ser cualquier cosa desde el número de incidentes de seguridad hasta el tiempo medio de respuesta a incidentes, entre otros.

- **Objetivos de Seguridad:** son metas claras y definibles que una organización establece para mejorar y mantener la seguridad de la información. Estos objetivos se basan en las necesidades de seguridad de la organización y deben ser coherentes con la política de seguridad de la información de la organización. Son esenciales para medir el rendimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y su eficacia.

Responsabilidades

- **Alta Dirección**: Serán responsables de conocer los objetivos de seguridad de la información, velar por el cumplimiento de estos y disponer los recursos necesarios para su cumplimiento. Está integrado por el Gerente General, Gerente de Producto, Gerente de Clientes, Gerente de Administración y RRHH, y Gerente Comercial.

- **Gerencia General**: Responde ante el Directorio por la existencia y cumplimiento de las medidas que mantengan un nivel de seguridad de la información conforme los objetivos y alineados a las disposiciones legales y regulatorias. Además, y en conjunto con el CISO, define y gestiona los riesgos de seguridad de la información.

- **Oficial de Seguridad (CISO)**: Máxima autoridad en el Sistema de Gestión de Seguridad de la Información de **Fidelizador SpA**. Junto con el Gerente General se encarga de la definición, implementación y supervisión de los criterios de seguridad de la información, para lo cual deberá analizar periódicamente el nivel de riesgo existente, asesorando en sus soluciones. Además deberá definir normas y validar todo procedimiento de las áreas de negocios para garantizar y proteger los activos de la información. Una vez autorizada la implementación de las medidas, deberá coordinar con quienes corresponda su materialización oportuna y correcta. Responsable de evaluar y medir el cumplimiento del SGSI de los colaboradores de la organización y también de la eficiencia del sistema de gestión.

- **Comité de Seguridad**: Máximo responsable de entregar las directrices para conformar la Política de Seguridad de la Información. Debe evaluar el estado del sistema de gestión, su

nivel de madurez, riesgos y planes de mitigación. Responsable de identificar todos los objetivos y estrategias del SGSI, dirigir, controlar y aprobar los planes de acción relacionados con la seguridad de la información. El comité está integrado por: Oficial de Seguridad, Gerente General, Gerente de Clientes y Jefe de Operaciones.

- **Comité de Contingencia**: En caso de contingencia, es la entidad responsable de planificar, coordinar, unificar puntos de vista y tomar líneas de acción de todas las áreas de **Fidelizador SpA** que tienen relación con la contingencia en curso. Esta entidad está conformada por: Gerente General, Gerente de Clientes, Jefe de Operaciones y Gerente de Productos.

- **Colaboradores**: responsables de cumplir con lo formalizado en este documento y aplicarlo en su entorno diario. Poseen la obligación de alertar de forma oportuna y adecuada cualquier incidente que atente contra la seguridad de la información.

Objetivos de Seguridad de la Información

Fidelizador SpA ha definido los siguientes objetivos generales de seguridad de la información:

1. **Seguridad de la información de los clientes**: Resguardar la confidencialidad, integridad y disponibilidad de la información cedida por nuestros clientes como parte de la prestación del servicio Fidelizador.com, medida en términos de la cantidad de incidentes de seguridad que afecten la información de los clientes.
2. **Cumplimiento de requerimientos de seguridad de los clientes**: Dar cumplimiento de los requerimientos mínimos de seguridad de la información solicitada por nuestros clientes como parte de la prestación de los servicios, medida en términos de porcentaje de cumplimiento de estos requerimientos.
3. **Cumplimiento de los niveles de servicio comprometidos** : Dar cumplimiento a los niveles de servicio contractuales comprometidos a los clientes, medida en términos de disponibilidad de los servicios y tiempos de respuesta a incidentes.

Para dar cumplimiento a los objetivos definidos, se identificarán todos los activos de información involucrados en los distintos procesos de negocios y procesos de soporte identificando al dueño de cada proceso y activo, las vulnerabilidades y amenazas de cada proceso y activo de información y, en función del impacto, determinar el riesgo existente, siempre bajo el alcance del sistema de gestión y, cuando aplica, a toda la organización de forma transversal. Con la información anterior, se aplicarán los controles necesarios que nos permitan gestionar debidamente el riesgo. **Fidelizador SpA** medirá el cumplimiento de todos los objetivos. El CISO es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos una vez al año, analizará, evaluará los resultados y los reportará a la Alta Dirección como material para la revisión por la Dirección. El CISO es responsable de registrar los detalles sobre los métodos de medición, periodicidades y resultados en el sistema de gestión de proyectos de **Fidelizador SpA**.

Política

Por medio de este documento la Alta Dirección presenta las directivas generales de **Fidelizador SpA** para con la seguridad de la información. Tiene el carácter de público y debe estar accesible tanto para colaboradores, clientes, proveedores y organizaciones relacionadas. Directivas o políticas específicas podrán complementar esta política general, pero no contradecirla ni anularla.

Requisitos de seguridad de la información

- La presente Política y el SGSI de **Fidelizador SpA** deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información y seguir los lineamientos de la norma ISO 27001:2013.

Apoyo al Sistema de Gestión de Seguridad de la Información

- A través del presente, la Alta Dirección de **Fidelizador SpA** declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

- La Alta Dirección deberá garantizar la revisión periódica de las políticas de seguridad (al menos una vez por año calendario), así como garantizar la existencia de mecanismos de difusión y educación en **Fidelizador SpA**.

Sobre clasificación de información y el uso aceptable de activos

- La información y todos sus accesos, usos y procesamiento deberán ser consistentes con las políticas y procesos emitidos por **Fidelizador SpA** en el contexto del presente SGSI.

- La información debe ser protegida, por sus responsables, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información.

- Toda la información creada y/o procesada por **Fidelizador SpA** o cedida al mismo como parte de la prestación de un servicio, debe ser considerada como “Confidencial”, a menos que se determine otro nivel de clasificación, pudiendo ser “Secreto”, “Restringido” o “Público”. Periódicamente se deberá revisar la clasificación, con el propósito de mantenerla o modificarla según se estime apropiado.

- Es responsabilidad de cada colaborador velar que toda información, cedida como parte de su labor, sea almacenada, procesada y transferida sólo con los proveedores y por los medios, aplicaciones y redes habilitados o autorizados por el área informática de la empresa para esos fines, siguiendo los protocolos establecidos.

- Los activos de información asignados o a los cuales se posee acceso deben ser empleados únicamente para la función y propósito inherente en el proceso en que estos existen. Cualquier otro uso es considerado “uso no aceptable” y será abordado conforme al impacto de este en términos de sanciones, normativo y/o legal de ser necesario.

- Se deberá considerar la existencia de un inventario y responsables de activos de información tecnológicos (aplicaciones e infraestructura) o no tecnológicos, así como procesos para mantenerlos.
- Se deberá considerar una definición y caracterización para la identificación, priorización y clasificación de los activos con el objetivo de proteger su confidencialidad, integridad y disponibilidad.

Sobre dispositivos móviles

- Los dispositivos móviles de los colaboradores que requieran acceder a Activos de Información de la empresa deben ser autorizados por el Jefe de Operaciones y deben ser usados de manera responsable y conforme a las políticas de la organización.
- Los dispositivos móviles NO deben almacenar información Confidencial o Secreta de la organización.
- Los dispositivos móviles utilizados para el acceso remoto deben cumplir con los requisitos de seguridad establecidos en la Política de Acceso Remoto.
- En caso de pérdida o robo de un dispositivo móvil, se debe informar de inmediato a la organización para que se tomen las medidas necesarias.

Sobre redundancia y alta disponibilidad

- Como regla general, todos los equipos físicos (hardware) son susceptibles (riesgo inherente) a fallar por causas naturales (derrame de líquidos, cortes eléctricos), humanos (mala manipulación, caída, robo, sabotaje), falla de fábrica o fin de vida útil, por lo que la Información que esta contiene y/o procesa puede ver afectada su disponibilidad, confidencialidad e integridad. Las mantenciones periódicas, reemplazos programados y otros cuidados a estos equipos podrían reducir este riesgo, pero la Alta Dirección de **Fidelizador SpA** considera que no son controles suficientes para dar el correcto tratamiento.
- Dado lo anterior, se debe cumplir:
    - La **redundancia de almacenamiento** para todos aquellos Activos cuya información almacenada se catalogue como “Alta” o superior en la categoría “Integridad” del Inventario de Activos. Es decir, los datos deben estar almacenados en al menos dos lugares físicos a la vez.
    - La **alta disponibilidad** de procesamiento y acceso a la información para todos aquellos Activos cuya información que procesen se catalogue como “Muy Alta” en la categoría “Disponibilidad” del Inventario de Activos. Es decir, los datos deben ser procesados y quedar accesibles desde al menos dos rutas diferentes.
- En caso de que el dueño del Activo sea un proveedor externo, este debe asegurar que cuenta con la redundancia y alta disponibilidad requerida.

Gestión de Riesgos

- Se deberán identificar las amenazas y vulnerabilidades potenciales de los activos, calificando los riesgos según probabilidad de ocurrencia y criticidad, de tal forma de establecer controles, tanto normativos como propios de la empresa, con el fin de darle tratamiento a estos riesgos.

Información de Clientes, Partners y Proveedores

- Dada la naturaleza de los servicios que **Fidelizador SpA** provee, se compromete a asegurar que la información cedida como parte de la prestación de los servicios no será divulgada sin previa autorización y estará protegida de igual manera que la información interna.

- En caso de que, como parte esencial de la prestación de algún servicio, **Fidelizador SpA** requiera ceder total o parcialmente la información antes cedida, el Cliente deberá ser debidamente informado de esta cesión en el contrato del servicio prestado.

Auditorías

- Con el fin de velar por el correcto uso de los activos de información de su propiedad, **Fidelizador SpA** se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los activos de información.

- **Fidelizador SpA** se reserva el derecho de tomar medidas administrativas y/o judiciales en contra el o los colaboradores que no den cumplimiento a lo dispuesto en la presente política, las políticas específicas que se deriven de esta y en su documentación de referencia, acciones que pueden ser solicitadas por el Comité de Seguridad.

Deberes de los Colaboradores

- La información y los activos de información deben ser usadas sólo para propósitos relacionados con su rol y labor en **Fidelizador SpA** debiéndose aplicar criterios de buen uso en su utilización.

- Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.

- El personal está en la obligación de alertar a su jefatura directa o el CISO, de manera oportuna y adecuada, cualquier incidente potencial o consumado que atente contra lo establecido en esta política y la seguridad de la información.

- Está absolutamente prohibido a los colaboradores de **Fidelizador SpA**, divulgar cualquier información que esté catalogada como “Secreta”, “Confidencial” o “Restringida”.

Organización de la seguridad de información

- Se deberán definir las responsabilidades específicas en materia de seguridad de la información de las diferentes unidades internas, considerando: la responsabilidad de las unidades de negocios en relación con el cumplimiento de las políticas y normas de seguridad.

Seguridad por defecto

- La "Seguridad por defecto" es uno de los principales enfoques de **Fidelizador SpA** respecto a la Seguridad de la Información el cual debe ser aplicado de forma diligente y tan estricto como el sentido común y el negocio lo permita. Se deben considerar al menos los siguientes aspectos:

    - **Minimización de Funcionalidades**: Sólo se deben instalar y habilitar las funciones, servicios y componentes necesarios para cumplir con el propósito del sistema o aplicación. Cualquier función o componente innecesario debe ser deshabilitado para minimizar la superficie de ataque.

    - **Configuraciones Seguras**: Las configuraciones predeterminadas deben ser las más seguras posible. Esto puede incluir contraseñas fuertes, cifrado habilitado, el uso de protocolos de red seguros, la desactivación de cuentas de usuario predeterminadas, entre otros.

    - **Control de Acceso**: Por defecto, los derechos y privilegios de los usuarios deben ser los mínimos necesarios para cumplir con sus responsabilidades laborales (principio de mínimo privilegio). El acceso a la información y las funcionalidades del sistema deben ser otorgadas sobre una base de necesidad de conocer.

    - **Actualizaciones y Parches de Seguridad**: Los sistemas y aplicaciones deben estar configurados para recibir y aplicar automáticamente las actualizaciones y parches de seguridad, siempre que sea posible.

    - **Cifrado**: siempre que sea posible, la comunicación entre servicios y aplicaciones en red debe quedar cifrada, siendo obligatorio cuando esta red trafica datos fuera de la red local de la organización.

    - **Monitorización y Registro**: Los sistemas y aplicaciones deben estar configurados para registrar y monitorizar automáticamente las actividades de los usuarios y los eventos de seguridad.

Registro, monitoreo, detección y alerta

- Se debe enfocar el SGSI en la detección y alerta temprana de debilidades, amenazas, vulnerabilidades que puedan afectar la seguridad de la información. Es decir, un SGSI orientado a la prevención y detección, sin desmedro de contar con sistemas y planes de contingencia y mitigación de incidentes adecuados para cada eventualidad.

Gestión de Incidentes de seguridad de la información

- Se deberá mantener registro de incidentes, eventos y vulnerabilidades. Adicionalmente deberán estar definidos los procesos y equipos de respuesta a un evento de seguridad, así como para el análisis forense de los incidentes de seguridad relevantes tendientes a

identificar la causa raíz y establecer planes de acción. En los casos que sea necesario se deberán considerar pruebas ante amenazas de Seguridad de la Información y Ciberseguridad.

Excepciones

Cualquier excepción a esta política debe ser justificada, documentada y aprobada por Oficial de Seguridad (CISO).

Revisión y actualización

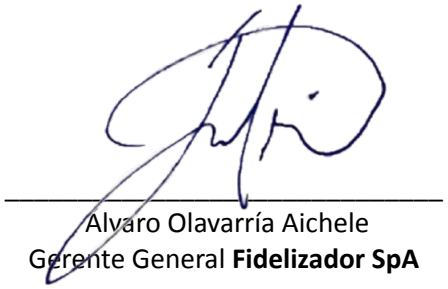
Esta política debe ser revisada y actualizada por el Comité de Seguridad al menos una vez al año o cuando sea necesario para reflejar los cambios en los sistemas y servicios de la empresa, las amenazas y vulnerabilidades de seguridad, y las mejores prácticas de la industria.

Cumplimiento

Todas las áreas de **Fidelizador SpA** son responsables del cumplimiento de esta política. El Comité de Seguridad revisará al menos una vez por año las prácticas de seguridad de la información en relación al cumplimiento de la presente política y sus objetivos.

Difusión

Se debe difundir la política a todos los colaboradores de **Fidelizador SpA** cada vez que se realice un cambio relevante, vía correo electrónico, con un breve resumen de los cambios incorporados. El encargado de esta difusión es el CISO. También se deberá comunicar vía correo electrónico a cada nuevo colaborador, cliente, proveedor o partner. También su versión más reciente debe estar disponible para descarga en el sitio web oficial y en la intranet.



Alvaro Olavarría Aichele
Gerente General **Fidelizador SpA**