



Política de Seguridad de la Información

Público

La impresión o descarga de este documento constituye una COPIA NO CONTROLADA.

Este documento contiene información de propiedad de ACEPTA COLOMBIA. Antes de utilizar alguna copia de este documento (digital / física), verifique que la versión sea igual a la última publicada en el Gestor Documental del SGSI de ACEPTA. De no ser válido, destruya la copia física o elimine la copia digital para asegurar que no se haga de ésta un uso no previsto.

HISTORIAL DE REVISIONES

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Oficial de Seguridad	Gerente General	Gerente General

HISTORIAL DE CAMBIOS

Nombre del Archivo	Versión	Resumen de cambios producidos	Fecha Aprobación
Política de Seguridad de la Información	1.0	Aprobación inicial	2018-05-15
Política de Seguridad de la Información	2.0	Revisión anual	2019-06-28
Política de Seguridad de la Información	2.1	Ajustes menores de redacción	2019-10-30
Política de Seguridad de la Información	3.0	Revisión anual	2020-03-15
Política de Seguridad de la Información	3.1	Ajustes punto 2.1	2020-11-12
Política de Seguridad de la Información	4.0	Revisión anual	2021-03-15

REFERENCIAS

Documentos Internos	
Título	Nombre del archivo
GG-F-06 Análisis FODA	GG-F-06 Análisis FODA.doc
Documentos Externos	
Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad, 2002/07/25	

INDICE

1.-	INTRODUCCIÓN.....	4
1.1.-	OBJETIVO	4
1.2.-	ALCANCE	4
1.3.-	RESPONSABILIDADES	4
1.4.-	TERMINOLOGÍA	4
2.-	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	5
2.1.-	ALCANCE DEL SGSI DE ACEPTA.....	5
2.2.-	ÁMBITO DEL SGSI DE ACEPTA	5
2.3.-	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE ACEPTA	5
2.4.-	DEPENDENCIAS DEL SGSI DE ACEPTA.....	6

1.- INTRODUCCIÓN

1.1.- OBJETIVO

El propósito de este documento es presentar la Política de Seguridad de la Información definida por la Gerencia General de ACEPTA S.A.S.

1.2.- ALCANCE

Esta política aplica a todos los elementos, registros y participantes que hacen parte del Sistema de Gestión de Seguridad de la Información.

1.3.- RESPONSABILIDADES

El Gerente General es responsable de la definición del contexto y alcance que tendrá el Sistema de Gestión de Seguridad de la Información (SGSI) en ACEPTA.

El Oficial de Seguridad es responsable de velar por el cumplimiento y el adecuado entendimiento por el personal tanto interno como externo de la Política de Seguridad de ACEPTA.

El personal interno de ACEPTA es responsable de velar por el entendimiento y aplicación de la Política de Seguridad, así como reportar al conducto adecuado cualquier falla de esta.

Los proveedores son responsables de seguir los lineamientos de seguridad definidos en los principios de seguridad para el alcance del SGSI a fin de no afectar su adecuado funcionamiento.

Los clientes y partes interesadas deben conocer la Política de Seguridad de la Información de ACEPTA.

1.4.- TERMINOLOGÍA

- SGSI: Sistema de Gestión de Seguridad de la Información
- Principios de seguridad de la información: Son los principios impartidos por la OCDE para la adecuada definición de la Política de Seguridad de la Información en las organizaciones

2.- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

2.1.- ALCANCE DEL SGSI DE ACEPTA

El alcance del SGSI de ACEPTA bajo la norma ISO/IEC 27001:2013 ha sido definido por parte de la Gerencia General como el Servicio de Emisión de Facturas Electrónicas y su validación, según declaración de aplicabilidad en vigor a la fecha de emisión del certificado” y considerando las dependencias conforme lo definido en el numeral 2.4.

2.2.- ÁMBITO DEL SGSI DE ACEPTA

El ámbito del SGSI es el personal de ACEPTA, sus proveedores, partes interesadas y los clientes asociados con los servicios cubiertos por el SGSI; siendo el Servicio de Emisión de Facturas Electrónicas conforme a los lineamientos impartidos por DIAN en Colombia

2.3.- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE ACEPTA

ACEPTA, asume el compromiso de desarrollar sus actividades según su Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013, en beneficio de sus clientes, accionistas, colaboradores y proveedores y orientado a cubrir los principios de Seguridad de la Información de la OCDE como buena práctica y que buscan proteger la Confidencialidad, Integridad y Disponibilidad de los activos de información de ACEPTA, en particular, orientándose a:

- Implementar un Sistema de Gestión de Seguridad de la Información que permita la mejora continua de la gestión de los activos de información
- Implantar un proceso de Gestión de la seguridad que permita analizar y valorar el riesgo de nuestros activos de información
- Impulsar, desde la Alta Gerencia, que el Sistema de Gestión de Seguridad de la Información logre sus resultados esperados
- Asignando los recursos necesarios para el adecuado funcionamiento y mejora continua del SGSI
- Comunicando la importancia del sistema de Gestión de Seguridad de la Información a los clientes, accionistas, colaboradores y proveedores de ACEPTA.

2.4.- DEPENDENCIAS DEL SGSI DE ACEPTA

Como parte del análisis de contexto realizado y documentado en “GG-F-06 Análisis FODA” se han identificado las dependencias e interfaces del SGSI y que allí se encuentran definidas.

