

Planeación del Sistema de Gestión de Seguridad de la Información

Gestión Tecnológica y Comunicaciones

29 de enero de 2018

INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL - INFOTEP

Av. Colombia, Barrio Sarie Bay

VERSIÓN:

PAGINAS:

ÚLTIMA ACTUALIZACIÓN:

Contenido

[1. Objetivo 3](#_Toc505002364)

[2. Objetivos Específicos: 3](#_Toc505002365)

[3. Alcance: 3](#_Toc505002366)

[4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. 3](#_Toc505002367)

[5. COMITÉ SEGURIDAD DE LA INFORMACIÓN. 3](#_Toc505002368)

[6. DESCRIPCIÓN DE LA METODOLOGÍA DE EVALUACIÓN DEL RIESGO. 4](#_Toc505002369)

[7. Matriz de Análisis de Riesgo 4](#_Toc505002370)

[8. Declaración de Aplicabilidad 4](#_Toc505002371)

1. Objetivo:

El Sistema de Gestión de Seguridad de la Información (SGSI), tiene como objetivo general aplicar en los procesos del área de Tecnologías de la Información y Comunicaciones (TIC´s) los estándares de seguridad de la información contemplados en la norma ISO 27001.

## Objetivos Específicos:

* + 1. Mantener la confidencialidad, integridad y disponibilidad de los activos de información de Coldeportes.
    2. Disminuir la posibilidad de ocurrencia de incidentes de seguridad de la información a partir de la identificación y tratamiento del riesgo.
    3. Mejorar y mantener un Sistema de Gestión de Seguridad de la Información para la entidad.

## Alcance:

Prestación de servicios de tecnología para el INFOTEP en el departamento Archipiélago de san Andrés y providencia islas

El logro de estos objetivos es responsabilidad de todos los funcionarios de la entidad en todos sus niveles, así como funcionarios, proveedores y contratistas que utilicen la plataforma tecnológica de la entidad.

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Las políticas de seguridad de la información son una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización. Estas conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón a lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos.

Manual de Políticas de Seguridad de la Información

## COMITÉ SEGURIDAD DE LA INFORMACIÓN.

Se debe generar una resolución por la cual se conforma el Comité Institucional de Desarrollo Administrativo y designar al funcionario líder de Gobierno en Línea.

## DESCRIPCIÓN DE LA METODOLOGÍA DE EVALUACIÓN DEL RIESGO.

* IDENTIFICACIÓN DE ACTIVOS DE TI
* VALORACIÓN DE ACTIVOS.
* CALCULO DEL VALOR DE LOS ACTIVOS.

Guía levantamiento de activos

* Criterions de Ponderation
* Indicadores ISO 27001

## Matriz de Análisis de Riesgo

Matriz de trabajo en la cual se identifican los riesgos de los activos de información de la entidad y se hace el tratamiento del riesgo tecnológico.

* Metodología Análisis y gestión de Riesgos Tecnológicos

## Declaración de Aplicabilidad

Este documento lista los objetivos y controles que se van a implementar o no en la entidad con su respectiva justificación.

* Declaración de Aplicabilidad

## CONTROL DE CAMBIOS

|  |  |  |
| --- | --- | --- |
| **FECHA** | **VERSIÓN** | **CAMBIOS** |
| Enero 2018 | 00 | Documento inicial |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **ELABORADO POR:** | **REVISADO POR:** | **APROBADO POR:** |
| **Silvio Hudgson Reeves**  Contratista Ingeniero de Sistemas Auditor en ISO 27001 |  |  |