SEGURIDAD DE LA INFORMACION

SGSI Y POLITICA PARA LA SEGURIDAD DE LA INFORMACION DEL SANATORIO DE CONTRATACION E.S.E

Elaborado por:

Angel Leonardo Calderón Franco
Encargado de Sistemas

Versión 1.0

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La información generada por el SANATORIO DE CONTRATACION E.S.E se constituye en uno de sus activos más importantes, por esto, es necesario protegerla de cualquier tipo de riesgo. Este documento pretende desarrollar un conjunto de directrices orientadas al buen uso de las tecnologías y a la concientización sobre la importancia de proteger la información de la entidad. La presente política de seguridad informática pretende dar cumplimiento a las normas en lo referente a la protección de los activos informáticos frente a los posibles riesgos derivados del uso de las nuevas tecnologías y así garantizar la seguridad en aspectos como DISPONIBILIDAD, CONFIDENCIALIDAD, ACCESIBILIDAD E INTERGRIDAD de los Activos informáticos de la entidad.

Así mismo, la política de seguridad de la información tiene como marco de referencia las normas NTC-ISO/IEC 27001 y NTC-ISO/IEC 27002 que describen los requisitos del Sistema de Gestión de Seguridad de la Información y las mejores prácticas para la implementación del Sistema de Gestión de Seguridad de la Información respectivamente; adicionalmente se tienen en cuenta objetivos de control establecidos en el estándar COBIT, y el documento MODELO DE SERGURIDAD PARA LA ESTRATEGIA DE GOBIERNO EN LINEA que plantea la estructura institucional recomendada que deberá tener el modelo de seguridad de la información.

2. ALCANCE / APLICABILIDAD

Esta política aplica a toda la entidad, sus dependencias, sus recursos, a los procesos internos y externos vinculados a través de contratos o acuerdos con terceros y a todo el personal vinculado al SANATORIO DE CONTRATACION E.S.E cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito, el nivel de las tareas que desempeñe y a la ciudadanía en general

3. POLITICA DE SEGURIDAD INFORMATICA SANATORIO DE CONTRATACION E.S.E

El Sanatorio de Contratación E.S.E para el cumplimiento de su misión, visión, objetivos estratégicos; y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad con los objetivos:

3.1 Objetivo General

Proteger los activos informáticos frente a los posibles riesgos derivados del uso de las nuevas tecnologías y así garantizar la seguridad en aspectos como disponibilidad, confiabilidad, accesibilidad e integridad de los mismos en el Sanatorio de Contratación E.S.E

3.2 Objetivos específicos

-Minimizar el riesgo en las funciones más importantes de la entidad.
-Cumplir con los principios de seguridad de la información y de la función administrativa.
-Cumplir con los principios -Mantener la confianza de sus clientes, socios y empleados. Apoyar la innovación tecnológica.
-Implementar el sistema de gestión de seguridad de la información.
-Establecer un entorno seguro sobre los activos informáticos.
-Establecer las políticas, procedimientos e instructivos, guías y mejores prácticas en materia de seguridad de la información.
-Crear la cultura de seguridad de la información en los funcionarios, terceros, y clientes del SANATORIO DE CONTRATACION E.S.E
-Garantizar la continuidad del negocio frente a incidentes.

3.3 Políticas de seguridad que soportan el SGSI del SANATORIO DE CONTRATACION E.S.E

Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Definir las Responsabilidades frente a la seguridad de la información las cuales deben ser compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, clientes, usuarios y terceros**.

Proteger la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos, del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

Salvaguardar la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta.

Proteger las instalaciones de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

Controlar la operación de sus procesos de negocio, garantizando la seguridad de los recursos tecnológicos y las redes de datos.

Implementar control de acceso a la información, sistemas y recursos de red.

Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información a través de una adecuada gestión del riesgo.

Garantizar el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas** por cada uno de **los empleados, proveedores, clientes, usuarios y terceros**.

Los funcionarios que conforman las diferentes áreas del Sanatorio de Contratación ESE, deben **clasificar** la información que tengan bajo su custodia.

4. RESPONSABILIDADES

La política de Seguridad de la información es de aplicación obligatorio para todo el personal del Sanatorio de Contratación E.S.E cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de tareas que desempeñe.

La gerencia del sanatorio aprueba esta Política y es responsable de la autorización de sus modificaciones.

El comité de gobierno en línea asumirá las funciones de comité de seguridad de la información y es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto de la política de seguridad de la información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del SGSI del Sanatorio.

El líder GEL será responsable de implementar e impulsar la implementación y el cumplimiento de la presente política.

El Comité de Seguridad de la Información será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI y supervisión del cumplimiento, dentro de cada dependencia, de aspectos inherentes a los temas tratados en la presente política.

Los funcionarios que tienen a cargo activos de información son responsables de la clasificación, mantenimiento y actualización de la misma, así como de

documentar y mantener actualizada la clasificación efectuada definiendo que usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencias. En general tienen la responsabilidad de mantener integro, confidencial y disponible el activo de información mientras es desarrollado, producido, mantenido y utilizado

El Jefe de recursos humanos cumple la función de notificar a todo el personal que se vincula contractualmente al Sanatorio, de las obligaciones respecto del cumplimiento de la política de seguridad de la información y darle a conocer los estándares, procesos, procedimientos, prácticas y guías que lo conforman.

El encargado de Sistemas debe seguir los lineamientos de la siguiente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la entidad. Corresponde a dicha dependencia consolidar el inventario de activos de información y recursos tecnológicos, el cual debe ser revisado y avalado por el Comité de Seguridad de la Información.

El Asesor jurídico debe verificar el cumplimiento de la presente política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo asesorar en materia legal a la entidad en lo que refiere a seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la información vigente.

La oficina de control interno es responsable de practicar auditorias periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta política y por las normas, procedimientos y prácticas que de ella surjan.

5 TÉRMINOS Y DEFINICIONES

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la Información y a los recursos relacionados con la misma, toda vez que lo requieran

Información: Toda forma de conocimiento objetivo con representación física o lógica explicita

Activo de Información: datos o información propiedad del Sanatorio que se almacena en cualquier tipo de medio y que es considerada como sensitiva o critica para el cumplimiento de los objetivos misionales

Sistema de Información: Conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como manuales.

Propietario de activos de información: en el contexto de la norma NTC 27001, un propietario de Activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.

Tecnología de la información: Conjunto de hardware y Software operados por la entidad, o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.

Evaluación de Riesgos: Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto

Reviso: EVER SANCHEZ FIGUEROA