unir
LA UNIVERSIDAD EN INTERNET

SGSI

ANSOLIDATA

Análisis de Riesgos Informáticos

Tema:

Metodología de gestión de riesgos de seguridad de la información de una organización

Desarrollado por:

Angel Ramón Paz López

unir
LA UNIVERSIDAD EN INTERNET

Contenido

INTRODUCCION

Las tecnologías de la Información y Comunicaciones (TIC) ha sido el motivo de cambio de una Sociedad de información hacia una sociedad basada en el conocimiento, en la cual el punto fundamental para una sociedad basada en el conocimiento es la Gestión. Toda gestión requiere de procesos eficaces, entradas de información fiables, proceso de retroalimentación, revisión y monitorización y métodos para corregir eventos no deseados para lograr los objetivos de una organización de manera eficaz. Por ende, se desarrollará un Sistema de Gestión de la Seguridad Informática a la Empresa ANSOLIDATA por la cual la metodología que se utilizará, describirá los procesos de las etapas en la cual se lleva a cabo la estructura de diseño, implementación y operación del Sistema de Gestión de la Seguridad Informática (SGSI) por lo cual utilizaremos el modelo ISO 27001 en la cual se refiere al establecimiento, implementación, operación, revisión de un Sistema de Gestión de la Seguridad Informática. Este informe se dividirá en dos partes: la primera parte se describirán los aspectos del sistema de seguridad y su implantación, el análisis, la gestión de los riesgos sobre los sistemas informáticos y sus respectivos controles a implementar y la segunda parte se describirá la estructura y contenido del Plan de Seguridad Informática.

OBJETIVO

La gestión en Seguridad Informática, gira en torno a tres ejes o puntos de la seguridad: la disponibilidad, la integridad y la confiabilidad de los datos, por lo cual es necesario que la empresa use las metodologías necesarias para la implementación de un SGSI para consolidar normas, políticas que regulen el manejo y acceso a la información y garantizar medidas de seguridad para los activos de la empresa.

ALCANCE

Este documento está dirigido a todas las personas involucradas con las tecnologías de información principalmente a la Gerencia de Desarrollo la cual su función es en base a las necesidades de los clientes, desarrolla soluciones web de alta calidad y orientada a la seguridad.

APROXIMACION BÁSICA

El SGSI es un proceso sistemático, protocolizado y manejado por personas interesadas y responsables en el área de la información que permite la confiabilidad, integridad y disponibilidad de la información de la misma, se diseña considerando los bienes informáticos que posee la empresa. Para garantizar la seguridad de la información el SGSI conlleva la conformación de estrategias, políticas, procedimientos, controles y mecanismos que garanticen el cumplimiento de confidencialidad, integridad y disponibilidad de la información, por lo cual para que esto se lleve a cabo de manera eficaz se debe partir de un análisis de riesgos que incluya: Determinar qué se trata de proteger, su probabilidad, implementar los controles de seguridad para protección de datos y revisar el proceso.

PRIMERA PARTE – SISTEMA DE GESTION DE SEGURIDAD INFORMATICA

METODOLOGIA DE IMPLEMENTACION

El proceso de implementación del SGSI, toma como base la norma 27001 para elaborar el plan estratégico para la implementación del SGSI, la cual se compone de cuatro procesos básicos:

1. Proceso de Planificación del SGSI

En esta primera etapa se crean los procedimientos para la realización del diseño, implementación, y gestión del Sistema de Seguridad Informática, con el fin de establecer las políticas, los procedimientos, estándares, procesos de seguridad para poder gestionar de manera eficaz los riesgos con el único objetivo de mejorar la seguridad informática. Los programas de gestión de la seguridad informática comienzas por proceso fundamental que es

la gestión de riesgos la cual establece los objetivos de la gestión analizando las amenazas y su potencial de impacto.

1.1. Preparación

Durante la preparación se crean las condiciones para el diseño e implementación del SGSI, considerando los aspectos de asegurar el compromiso de la dirección y selección de los miembros del equipo en la implementación del SGSI.

1.1.1. Compromiso de la Dirección con la Seguridad Informática

La Gerencia Ejecutiva de ANSOLIDATA junto con la Gerencia de Desarrollo apoyara activamente la seguridad dentro de la organización, mediante una orientación clara, compromiso y la asignación de responsabilidades para la aprobación e implementación de del SGSI.

1.1.2. Seleccionar y preparar los miembros del equipo que participará en el diseño de implementación del SGSI

El equipo de diseño e implementación se deberá conformar por el personal informático y técnico del área de la Gerencia de Desarrollo (Front End, Backend, Base de Datos, QA).

La estructura organizacional forma parte fundamental para el logro de los objetivos de ANSOLIDATA, esta se basa en un modelo funcional, en el cual cada uno de los puestos es ocupado por personas especializadas en cada una de las áreas lo cual garantiza un buen desempeño en todas sus áreas.

1.2. Determinación de las medidas de protección

Siendo la información el activo más valioso de una organización requiere medidas y controles de seguridad que permitan su confiabilidad, integridad y disponibilidad, por ello se ocupa realizar un análisis de riesgos para determinar la probabilidad de materialización de las amenazas, su impacto una vez materializados, la probabilidad de ocurrencia.

El proceso del Análisis de Riesgos consta de dos procesos:

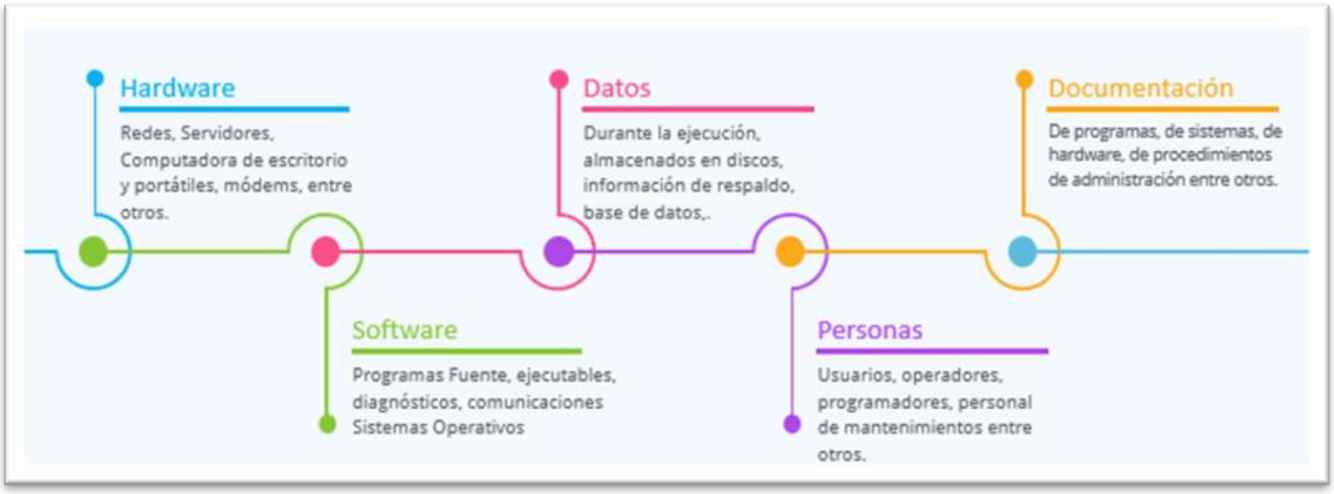
a) **Evaluación del Riesgo:** Es relacionar las amenazas con las vulnerabilidades en relación a la capacidad de respuestas y autogestión que pueda tener una organización para así determinar su importancia.

b) La Gestión de Riesgos: Implica la identificación, selección y aprobación de las medidas y controles de seguridad para hacer frente a los riesgos o amenazas evaluados. Las acciones que se pueden realizar son las siguientes: Reducir, retener, evitar y transferir el riesgo.

Durante la determinación de las necesidades de protección del sistema informático es necesario: Caracterizar, Identificar las amenazas y Evaluar el Sistema Informático

1.2.1. Caracterización del Sistema Informático

Incluye la determinación de los bienes informáticos que se pretende proteger, su valoración y clasificación según su importancia. Es necesario establecer todas las características del entorno del SI (Edificaciones locales, donde están instalados los equipos, tipos de tecnologías, software instalado, documentación de software, planilla del personal entre otros) Agrupación por categorías de los bienes informáticos a proteger:



La valoración de los bienes informáticos nos servirá para determinar el grado de importancia de mediante su categorización, la determinación de la importancia de cada bien informático se puede realizar de manera descriptiva (Alto, Medio, Bajo) o de manera numérica (0 poca importancia, 10 máxima importancia).

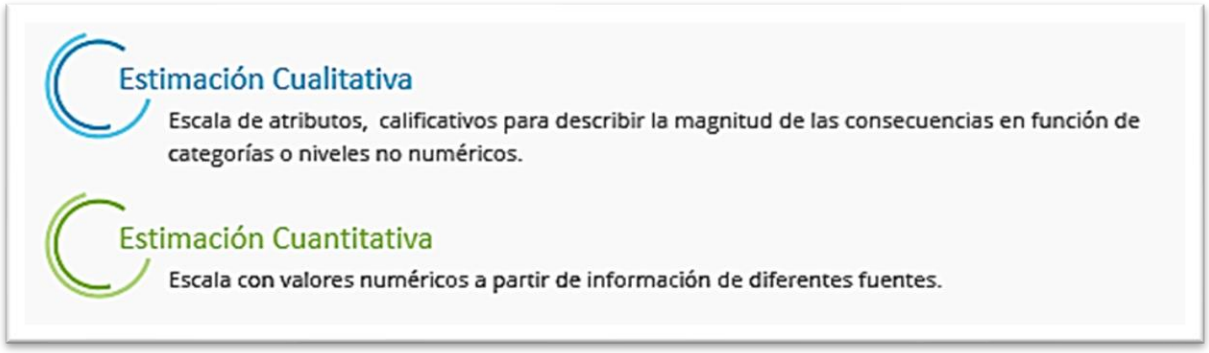
1.2.2. Identificación de las Amenazas

Podemos definir una Amenaza como cualquier evento que explota las vulnerabilidades de un sistema, Las amenazas más comunes: Perdida de Información, Alteración o modificación de la información, Divulgación de la información, Interrupción de los servicios. Por medio del

análisis del riesgo se comprende la naturaleza del riesgo y sus características, lo cual conlleva un estudio detallado de los riesgos tomando en consideración las incertidumbres, las fuentes del riesgo, las consecuencias, probabilidades de ocurrencia, los eventos, los distintos escenarios y la implementación de controles.

1.2.3. Estimación del Riesgo

Se determinan considerando las probabilidades de materialización de las amenazas y las metodologías a realizar son:



1.2.4. Evaluación del estado actual de la Seguridad Informática

Es necesario evaluar la efectividad de los controles existentes, los resultados del análisis de riesgos

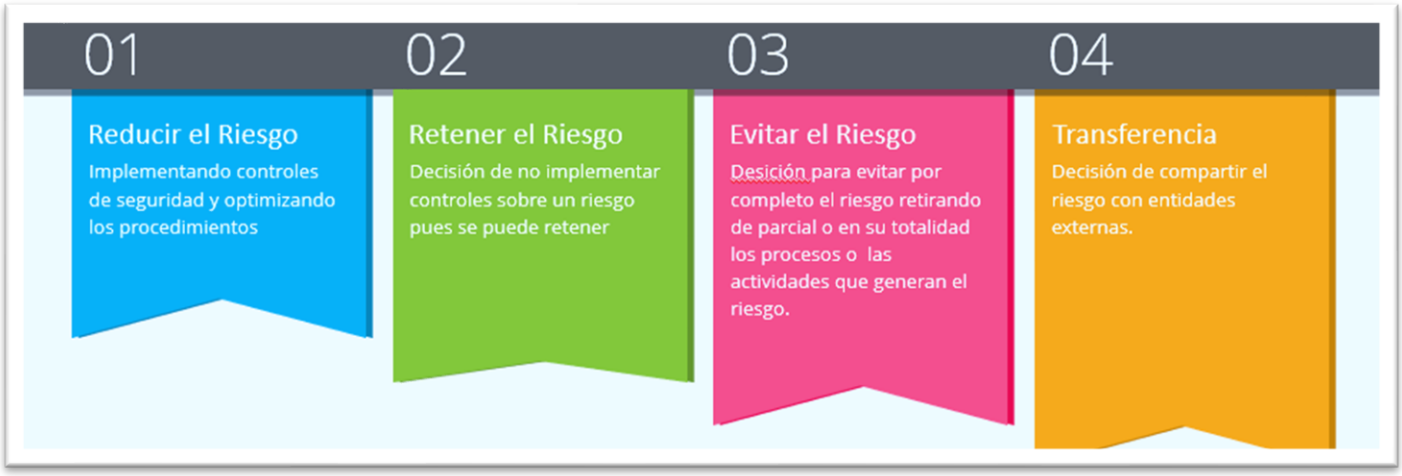
Evaluación de las consecuencias del riesgo y probabilidad de incidentes

Lista de escenarios de incidentes					Controles existentes y planificados	Eficacia e Implementación	Estado de utilización
identificación de amenazas	vulnerabilidades	activos afectados	consecuencias para los activos	procesos del negocio			

Los resultados de esta evaluación ayudaran a orientar y a determinar una apropiada acción gerencial y las prioridades para gestionar los riesgos, así como la implementación de los controles.

1.3. Selección de los controles de Seguridad Informática

Para cada uno de los riesgos identificados se tomará una decisión sobre su tratamiento.



1.3.1. Políticas de Seguridad

Las políticas de seguridad son un conjunto de reglas, normas que proporcionan orientación a la organización para velar por la seguridad informática de la información como ser:

- Los responsables deben proveer un entorno de procesamiento seguro en el que se mantenga la seguridad de la información.
- El acceso a las áreas de trabajo se permite exclusivamente al personal autorizado

1.3.2. Medias y Procedimientos de Seguridad

a) Medidas Administrativas: Implementación de contraseñas seguras
b) Medidas de Seguridad Física: Videovigilancia de acceso a las instalaciones.
c) Medidas de Seguridad Técnicas: Mecanismos de control de acceso con roles específicos a los usuarios para ingresar al sistema
d) Medidas Legales: Se sancionarán a los que no cumplan las políticas de seguridad.
e) Medidas de Recuperación: Backups para recuperación de la información.

Procedimientos de Seguridad Informática

Son descripciones detalladas de los pasos a seguir para llevar a cabo una determinada tarea.

Política, medida y procedimiento para su implementación

- Política: Los responsables deben proveer un entorno de procesamiento seguro en el que se mantenga la seguridad de la información.
- Medida: Los responsables deben utilizar la solución de antivirus de McAfee en todos los equipos de usuario.
- Procedimiento: Todos los usuarios de equipos deben establecer la actualización del antivirus corporativo con periodicidad semanal. Los pasos a seguir son los siguientes:

Ir al apartado **Seguridad para el PC y** Seleccionar **Actualizaciones automáticas**

Responsable: Empleados del Área y jefe de Seguridad Informática

1.4. Organización de la Seguridad Informática

Se establecerá un marco apropiado para la implementación del SGSI dentro de la organización por lo cual se detallará la Organización Interna, Coordinación, Responsabilidades.

1.4.1. Organización Interna

Para una eficaz implementación del SGSI la dirección general aprobará las políticas de seguridad, la cual asignará roles de seguridad la cual coordinara y revisaran mediante monitoreos la eficacia de la implementación.

1.4.2. Coordinación de la Seguridad

La seguridad informática será coordinada por el personal técnico responsables de cada gerencia (Ventas, Desarrollo, Administrativa, TI) con el objetivo de asegurar todas las actividades en relación a la seguridad de acuerdo a todas las políticas establecidas en cada área y en general

1.4.3. Asignación de Responsabilidades de la Seguridad Informática

Se definirán las responsabilidades de seguridad de informática al personal que está vinculado o tenga participación directa con los sistemas informáticos.

1.4.4. Elaboración Plan de Seguridad Informática

El objetivo es establecer los requisitos de seguridad del sistema, los controles que se implementaran en cada área, responsabilidades y el comportamiento de los usuarios que accedan al sistema.

2. Proceso de Implementación del SGSI

El Objetivo principal es garantizar la implementación de los controles seleccionados y su correcta aplicación. Se garantizará que el personal tenga sus responsabilidades definidas en el SGSI, por lo cual primero se realizaran capacitaciones para hacer conciencia y saber los roles que tienen que cumplir dentro del SGSI. Se precisará el procedimiento y las mediciones de eficacia de los controles seleccionados y se especificaran como se van a emplear y

finalmente implementar los procedimientos y controles que se requieren detectar y dar respuesta y el tratamiento oportuno a los eventos negativos de seguridad.

2.1. Programa de Desarrollo de la Seguridad Informática

Se realizará un programa de desarrollo para la implementación de los controles señalando los plazos para su cumplimiento ya sea a mediano o largo plazo, la preparación de las capacitaciones del personal en materia de seguridad, auditorias entre otros.

3. Proceso de Verificación del SGSI

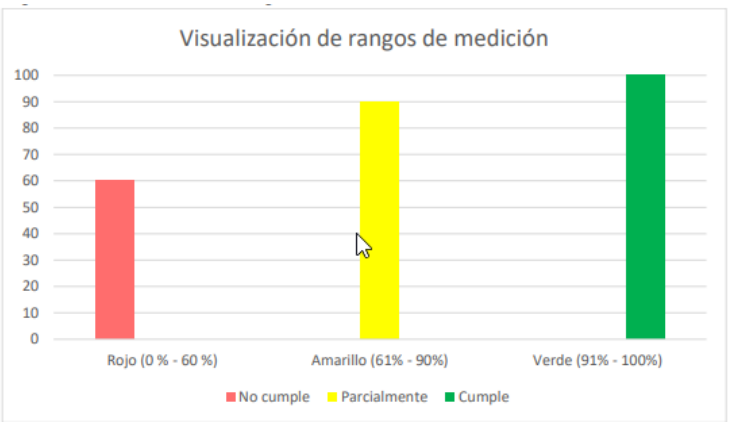
El objetivo de este proceso es revisar y evaluar la ejecución de los procedimientos de monitorización y revisión para detectar los errores o fallas que se han detectado en el procesamiento de la información. En este proceso se deberán hacer revisiones periódicas de indicadores, de los riesgos, realizar auditorías y comunicar los resultados

3.1. Métodos de Medición

Los métodos de medición se utilizan para poder cuantificar un objeto de medición la cual puede ser subjetivo u objetivo. Los subjetivo se basan en la cuantificación basada en el juicio humano y los objetivos se basan en reglas numéricas.

3.2. Indicadores de Medición

Registros o evidencias que permiten verificar el correcto funcionamiento del SGSI, cada indicador debe tener asociado valores que representen las metas a cumplir.



4. Proceso de Actualización del SGSI

En este proceso se realizará el debido mantenimiento y correcciones del SGSI con el objetivo de realizar los cambios necesarios para mantener al máximo el rendimiento del SGSI. Circunstancia de la necesidad de un nuevo análisis de riesgos: Instalación de nuevos tipos de redes, cambios de la estructura y topología de las mismas, implementación de nuevas tecnologías, ocurrencia de algún evento no deseado

SEGUNDA PARTE – ESTRUCTURA Y CONTENIDO DEL PLAN DE SEGURIDAD

PRESENTACION DEL PLAN DE SEGURIDAD

Ítem	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado				
Aprobado.				
Revisado.				
Confeccionado				
ITEM	ELABORADO	REVISADO	APROBADO	ELABORADO
NOMBRE				
CARGO				
FIRMA				
FECHA				

ESTRUCTURA DEL PLAN DE SEGURIDAD INFORMATICA

1. Alcance del Plan de Seguridad

El presente Plan de Seguridad Informática es aplicable en su totalidad en el área de Desarrollo y TI los cuales se encuentran en el edificio HANDALS situado en la calle avenida La Independencia, segundo piso y tercer piso.

Las políticas expresadas en este plan son de obligatorio cumplimiento para todo el personal de la Empresa ANSOLIDATA, lo cual todo el personal que trabajan en estas áreas debe cumplir todas las políticas de seguridad implementadas.

2. Caracterización del Sistema Informático

- Bienes informáticos, su destinación e importancia.
- Aplicaciones en explotación.
- Características del procesamiento, transmisión y conservación de la información, teniendo en cuenta el flujo interno y externo y los niveles de clasificación de la misma.

3. Resultados de Analisis de Riesgos

Los bienes informáticos más importantes a proteger son:

• La red de trabajo interno de la Oficina de TI y Desarrollo

• El servidor de aplicaciones.

• Las bases de datos del sistema que se desarrolla y del Sistema Web Ansolidata

• El acceso no autorizado a la red y a cada aplicación

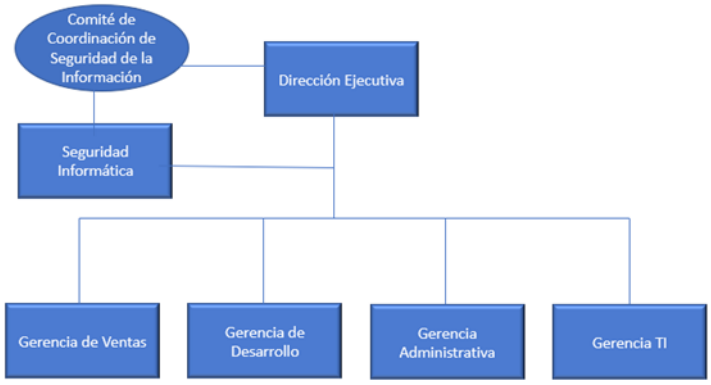
4. Políticas de Seguridad Informática

a) Se creará una comisión o comité encargada de la supervisión e implementación de todas las políticas y medidas de seguridad para ver si el SGSI cumple con sus funciones.

b) Los responsables deben proveer un entorno de procesamiento seguro en el que se mantenga la seguridad de la información e informar al Jefe de Seguridad Informática cualquier incidente o violación a la seguridad.

c) El acceso a las áreas de trabajo se permite exclusivamente al personal autorizado

5. Responsabilidades



Estructura organizacional transitoria propuesta para la administración de la seguridad de información

Organización del comité de coordinación de seguridad de la información

ROL	FUNCION	NOMBRE
Jefe de Seguridad Informática	Difusión de la importancia del cumplimiento de las políticas de seguridad de información al personal de la empresa. También tiene la responsabilidad de evaluar el estado de la seguridad que se brida a la información, para tomar medidas correctivas si es necesario.	Edgar Paredes

6. Medidas y Procedimientos

6.1. Clasificación y control de los bienes informáticos.

- Se realizarán auditorías periódicas para comprobar el control de Tecnologías Informáticas.
- Cada ordenador contara con un expediente técnico donde se registrarán todos los cambios que ocurran con el equipo.

Procedimiento No. 1: Alta de Medios Informáticos para su uso.

- Instalar el software autorizado a utilizar en el área a la que fue asignado el medio informático, dejando constancia en el Registro de software autorizado que incluye el Expediente Técnico del medio informático.

Responsable: Gerente de Sistemas

- Capacitar al personal encargado de la operación y protección del medio informático en materia de Seguridad Informática.

Responsable: jefe de Seguridad Informática

6.2. Seguridad Física y Ambiental

Objetivo fundamental es evitar el acceso a personas no autorizadas

Clasificación de las áreas

Área controlada	Categoría	Medidas especificas
	Limitadas	
	Restringidas	

Medidas generales para todas las áreas con tecnologías informáticas:

- Contar con fuentes de respaldo de energía y estabilizadores de voltaje para cada computadora.

- Los usuarios antes de conectar o desconectar los equipos de la red eléctrica chequearán que estos estén apagados.

6.3. Identificación y Control de Accesos

Objetivo Fundamental es gestionar el acceso a la información de forma segura.

Medidas:

- Se establecerán identificadores de usuarios en las PCs, sistemas y servicios informáticos en la red.

Procedimiento No. 1: Control de la Identificación de usuario

- Se tiene que crear los usuarios correspondientes al personal de desarrollo y después Otorgar/Retirar acceso de personas a las Tecnologías de Información, se revisara que los identificadores que se están utilizando correspondan con la situación de los trabajadores autorizados a trabajar con las tecnologías informáticas.

Responsable: Gerente de Sistemas

Procedimiento No. 2: Autentificación de usuario

- Las computadoras contarán con un login que bloqueen el acceso a su entorno.
- La cuenta de administrador estará deshabilitada para mayor seguridad.

Responsable: Gerente de Sistemas

6.4. Seguridad ante programas malignos

Objetivo mantener actualizado el equipo y evitar programas que dañen el equipo.

Medidas:

Todo el personal es responsable la revisión de todos los soportes de propiedad personal o de otra entidad que se autoricen introducir en el ordenador antes de su utilización.

La actualización del Software Antivirus de las máquinas y Servidores de la Red se realizará diariamente, de forma programada.

Procedimiento No. 23: Actualización del Software Antivirus en el Servidor.

- Diariamente se descarga a las 5:00 am de forma automática la actualización del Antivirus
- Verificar periódicamente las actualizaciones del Antivirus.

Responsable: jefe de Seguridad Informática.

CONCLUSIONES

Es importante resaltar que la seguridad es un proceso que debe estar en un proceso de mejora continua por lo que los controles establecidos y las políticas mencionadas en el informe con el objetivo de la protección de la información deben revisarse y de ser necesario adecuarse ante los nuevos riesgos que vayan apareciendo.

RECOMENDACIONES

- Todos los empleados de la Gerencia de Desarrollo deben ser responsables y cumplir con las políticas de seguridad.
- Las políticas de seguridad son de carácter obligatorio para todo el personal de la organización.

BIBLIOGRAFIA

- *Infomed.* (s.f.). Obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf
- Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (1.ª ed.). Editorial Científica 3Ciencias. https://doi.org/10.17993/IngyTec.2018.46
- *ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información*. (2015, enero 28). PMG SSI - ISO 27001. https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/
- Moreno, D. R. E., & León, C. C. T. (2017). MODELO DE MEDICIÓN PARA EL SGSI DE LAS ENTIDADES GUBERNAMENTALES, QUE HAN SEGUIDO LOS LINEAMIENTOS ESTABLECIDOS POR LA ESTRATEGIA DE GOBIERNO EN LÍNEA. 129.