1. OBJETIVO

Definir los recursos mínimos requeridos de seguridad para la instalación de los sistemas informáticos de IGS.

2. ALCANCE

Aplica para toda la plataforma de tecnología en todos sus ambientes tales como; productivos, contingentes, desarrollo y pruebas.

3. DEFINICIONES

Ambiente de Pruebas: infraestructura de hardware y software necesaria para realizar la ejecución de pruebas de integración, sistema y funcionales para determinar el comportamiento de la aplicación en escenarios reales.

Ambiente de desarrollo: Es un conjunto de procedimientos y herramientas que se utilizan para desarrollar un código fuente o programa. Este ambiente es utilizado para escribir, generar, probar y depurar un programa.

Ambiente de contingencia: Es una Infraestructura con procedimientos y planes en las cuales están integrados todos los servicios tecnológicos críticos de la compañía.

Ambiente de Producción: El ambiente de Producción es donde están disponibles las funcionalidades necesarias tecnológicas y de procesos para la ejecución de los procedimientos.

4. CONDICIONES GENERALES

4. 1. Políticas

4. 1.1. Aplicables al Sistema de Gestion de S.I

Este procedimiento complementa la política; ***SGSI-POL-001 Política de seguridad de la informacion.***

5. RESPONSABILIDADES

Área de Tecnología

Implementar, analizar, planificar y gestionar los parámetros de seguridad para la instalación de los sistemas tecnológicos de IGS.

Jefe de Sistemas

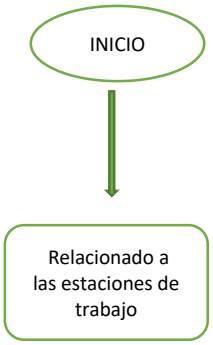
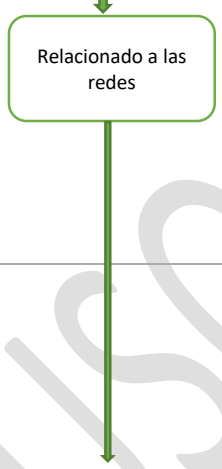
Planificar las actividades de trabajo a realizar para la instalación de seguridad en los sistemas.

Analista de Sistemas

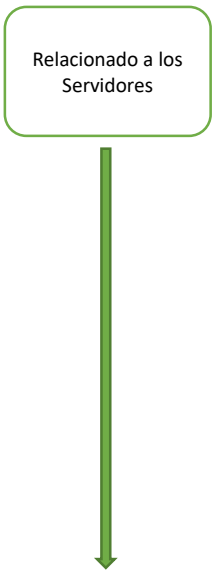
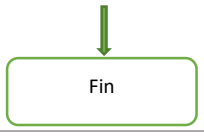
Ejecutar e instalar las medidas de seguridad en los sistemas.

USO INTERNO

6. DESCRIPCIÓN DE ACTIVIDADES

No	*Flujograma*	*Descripcion*	*Responsable*
1		Se deben tener las mínimas medidas de seguridad para la instalación de los sistemas en las estaciones de trabajo así: - Actualización de sistemas operativos S.O Update. - Instalación de parches. - Actualizar versiones de las aplicaciones. - Instalación de Antivirus. - Activación e instalación de Firewall. - Autenticación por contraseñas. - Creación de perfil de usuario. - Copia de respaldo de informacion. - Privilegios de acceso. - Activación del Log de auditoria. - Firmas Electrónicas. - Instalación de Certificados Digitales.	TI
2		Medidas de instalación para la seguridad en redes: - Control de acceso por usuario - Segmentar la red - Configurar Privilegios de acceso - Activar y respaldo de Log de auditoria - Activación de IDS Y IPS - Configuración del Firewall	TI
3		Medidas de instalación para la seguridad física: - Conexión en la red eléctrica regulada - Conexión a las UPS de respaldo.	TI

USO INTERNO

4		Medidas de instalación para los servidores: - Actualización de sistemas operativos S.O Update. - Instalación de parches. - Actualizar versiones de las aplicaciones. - Instalación de Antivirus. - Activación e instalación de Firewall. - Autenticación por contraseñas. - Creación de perfil de usuario. - Copia de respaldo de informacion. - Privilegios de acceso. - Activación del Log de auditoria. - Firmas Electrónicas. - Instalación de Certificados Digitales. - Protección de puertos - Autenticación basada en Hots - Detección de intrusos.	TI
9		Fin de la Guía.	TI

7. DOCUMENTOS DE REFERENCIA

• SI-POL-001 Política Seguridad de la Informacion.

8. HISTORIAL DE CAMBIOS

FECHA	VERSION	NATURALEZA DEL CAMBIO
23-10-2019	1.0	➢ Creación del documento.

USO INTERNO