UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

PLAN DE AUDITORIA DE SISTEMAS

Equipo auditor

Mas Mendoza, Katerin Estrellita

Líder auditor - Oblitas Diaz, Helen

Tarapoto, setiembre 2024

INTRODUCCIÓN

El área de Tecnologías de la Información desempeña un papel fundamental en la mejora de la gestión pública, permitiendo a la Dirección Regional de Agricultura San Martín atender de manera más eficiente y efectiva las necesidades de los ciudadanos. Las TIC son una herramienta clave para incrementar la eficiencia, la eficacia y la transparencia en la administración pública, además de fomentar la participación ciudadana y crear oportunidades de desarrollo para la región.

En este contexto, el presente plan de auditoría dirigido al área de TI de la Dirección Regional Agricultura San Martín (DRASAM) tiene como objetivo evaluar el cumplimiento de las políticas, procedimientos y controles establecidos para asegurar la correcta implementación y funcionamiento de las TIC en apoyo a los objetivos institucionales. Esta evaluación se llevará a cabo bajo un enfoque sistémico, considerando la interacción de los diferentes componentes tecnológicos para garantizar que se alineen con los objetivos estratégicos de la institución.

La auditoría se realizará en coordinación con el responsable y jefe del área, de acuerdo con los lineamientos establecidos en el Decreto Supremo N° 054-2018-PCM, que aprueba los Lineamientos de Organización del Estado [1].

CAPÍTULO I

La Organización

Datos generales de la organización

Razón social: Dirección Regional de Agricultura San Martín

Área: Área de Tecnologías de la Información

Rubro: Agricultura

Dirección: Jr. Ángel Delgado Morey S/N - Tarapoto - San Martín.
Referencia: Altura Cdra 15 Jr. Leguia.

Representante legal: Ing. Mario Enrique Rivero Herrera

Representante del área: Ing. Llaker Carbajal Saboya

Descripción de las principales actividades de la organización

Visión

Al 2030, ser modelo de región en bienestar social, competitividad y valoración de nuestros recursos naturales y diversidad.

Misión

Promover el desarrollo integral y sostenible de la región de manera inclusiva, competitiva y solidaria; en el marco de la modernización, con enfoque territorial y gestión de cuencas.

Descripción de las principales actividades del área

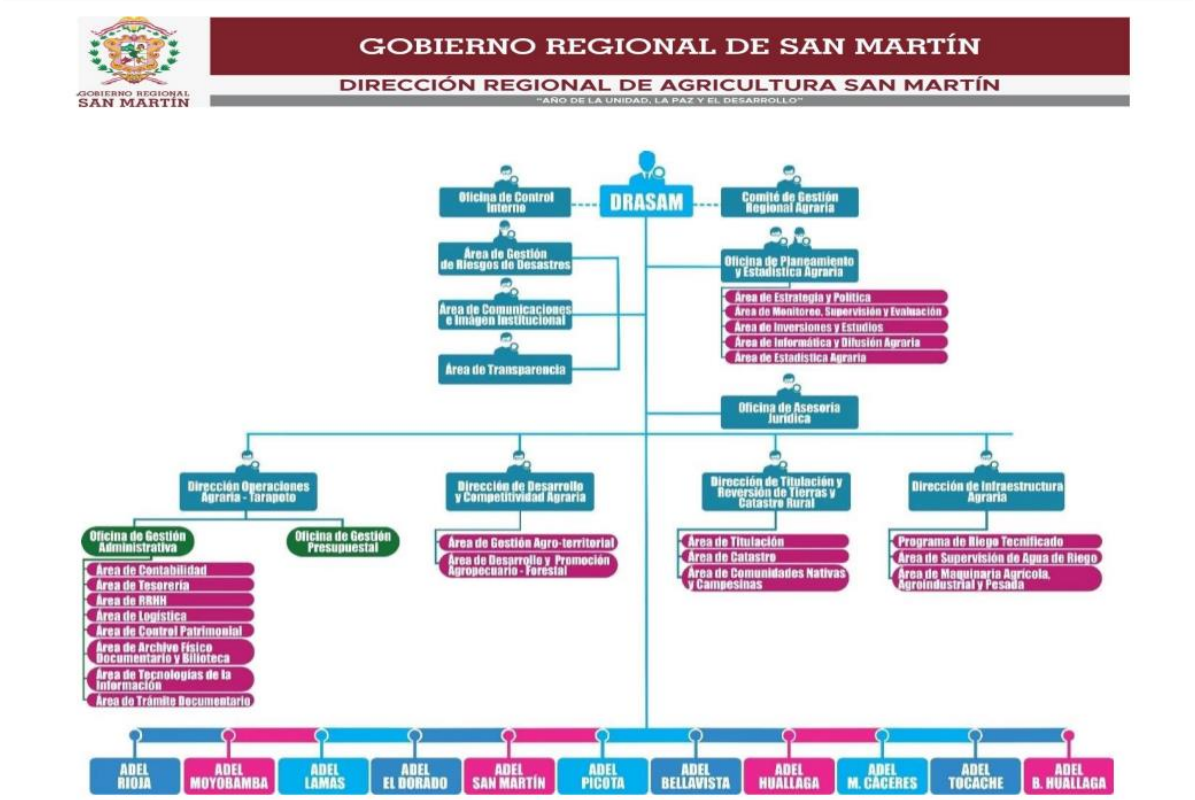
Visión

"Ser un área líder en innovación tecnológica, impulsando la transformación digital de la Dirección Regional de Agricultura de San Martín, mediante soluciones eficientes, seguras y sostenibles que contribuyan al desarrollo regional y al bienestar de los ciudadanos."

Misión

"Proporcionar servicios tecnológicos de alta calidad, garantizando la eficiencia, seguridad y disponibilidad de la información. Facilitar la digitalización de procesos, promover la interoperabilidad y mejorar la gestión pública, alineándose con los objetivos estratégicos de la institución y atendiendo las necesidades de la ciudadanía."

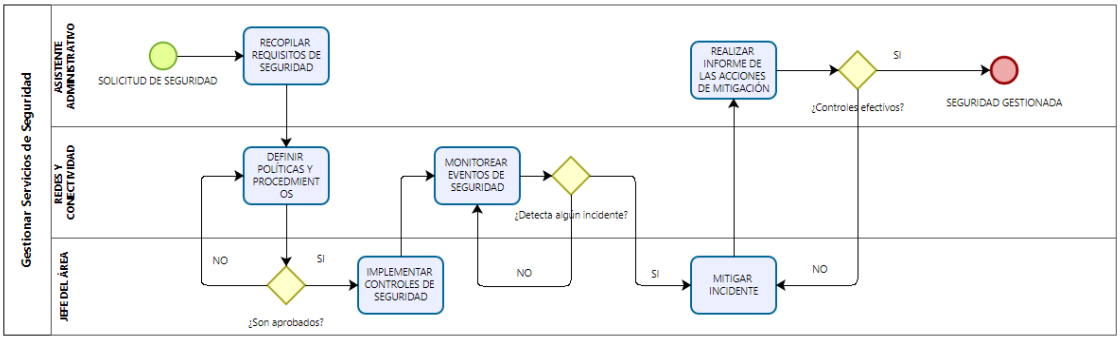
Organigrama de la institución



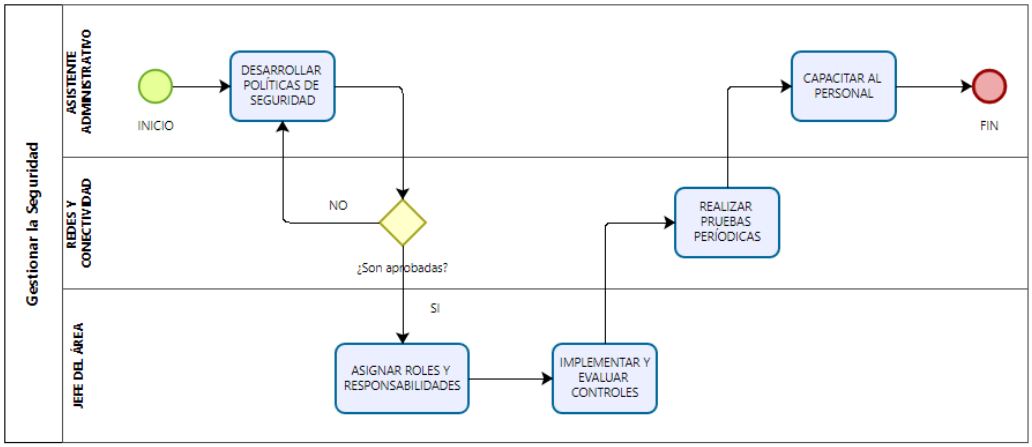
Organigrama del área de ATI

Flujo del proceso a Auditar

Entregar, dar Servicio y Soporte - DSS05 Gestionar Servicios de Seguridad



Alinear, Planificar y Organizar - APO13 Gestionar la Seguridad



CAPÍTULO II

Auditoría de Sistemas

Objetivos y Alcance de la Auditoría de Sistemas

Objetivo general

Evaluar los servicios de seguridad implementados en el Área de Tecnologías de la Información de la Dirección Regional de Agricultura San Martín (DRASAM) con el fin de prevenir, detectar y responder ante amenazas de seguridad, incluyendo malware y ataques como el ransomware.

Objetivos específicos

- ❑ Detección de amenazas: verificar si cuentan con herramientas de antivirus y sistemas de detección de intrusos en la infraestructura de TI.
- ❑ Revisar las medidas de prevención: analizar las políticas y configuraciones de seguridad que previenen la ejecución de malware y ataques de ransomware.
- ❑ Evaluar la respuesta ante incidentes: comprobar que el área de ATI cuenta con un protocolo efectivo de respuesta a incidentes que permita la rápida contención y mitigación de daños.
- ❑ Revisión de la gestión de vulnerabilidades: validar que se realicen evaluaciones regulares para identificar y corregir vulnerabilidades en la infraestructura de TI.

Alcance de la Auditoría

Evaluar la implementación y efectividad de las políticas y procedimientos de seguridad de TI, así como la conformidad y el rendimiento de los sistemas y herramientas tecnológicas utilizados por el área.

Descripción de la situación actual del área a evaluar

Nombre del área: ATI (Área de tecnologías de la información).

Descripción de las principales actividades / funciones

- ✓ Implementar controles de seguridad en red, dispositivos, aplicaciones y datos sensibles de la institución.
- ✓ Monitorear el funcionamiento seguro de los sistemas informáticos.
- ✓ Mantener todos los equipos de TI en un buen estado operativo.

- ✓ Identificar eventos que puedan atentar cintra la integridad, confidencialidad y disponibilidad de la información.

Relación de puestos y principales funciones por puesto

Jefe del área: Es el encargado de implementar las políticas de seguridad y supervisar las actividades del área.

Encargado de soporte administrativo: Brinda asistencia en incidentes y mantiene actualizados los sistemas con medidas preventivas.

Encargado de redes y conectividad: Gestiona y configura los controles de acceso y seguridad en la red institucional.

Descripción de los sistemas, equipos e instalaciones

- ✓ Equipamiento
- ✓ Seguridad física
- ✓ Software
- ✓ Políticas de seguridad (documentación)
- ✓ Conectividad
- ✓ Contingencia y recuperación
- ✓ Historial de incidentes
- ✓ Personal y sus roles de función

Descripción de las áreas (puntos de evaluación) que contempla la Auditoría de sistemas

DSS05 Gestionar los servicios de Seguridad

Este proceso requiere establecer políticas y buenas prácticas de seguridad dentro del Área. Esto implica implementar controles de seguridad continuos y mecanismos de prevención, detección y respuesta ante incidentes de seguridad, como el malware y el ransomware.

COBIT menciona que se debe realizar un monitoreo constante de la infraestructura y sistemas, que incluya actividades como la gestión de accesos y la detección de amenazas en tiempo real. Adicionalmente, se deben llevar a cabo evaluaciones periódicas de vulnerabilidades y gestionar de manera efectiva la respuesta a incidentes, de forma que se minimicen los impactos en las operaciones de TI.

APO13 - Gestión de la Seguridad

Este proceso establece que es fundamental definir políticas de seguridad alineadas con los objetivos de la organización y gestionar los riesgos de seguridad de manera óptima.

COBIT sugiere incluir evaluaciones periódicas de los riesgos de seguridad, la definición de roles y responsabilidades en materia de seguridad, y el desarrollo de programas de concientización y capacitación en seguridad para todo el personal.

Cronograma de la auditoría

Procesos	Días	Fecha	Septiembre	Octubre	Noviembre
Fase 1: Elaboración del problema	2	DSS05, MEA01	X		
Fase 2: Ejecución de la auditoría	3	DSS05	X	X	
Fase 3: Evaluación de rendimiento y conformidad	2	MEA01		X	X
Fase 4: Elaboración del dictamen final	2	DSS05, MEA01			X

Presupuesto de la auditoria

Concepto	Cantidad	Costo Unitario (PEN)	Total (PEN)
Honorarios del Equipo Auditor	7 días	1,100	7.700
Capacitación en Seguridad y Conformidad	1	900	900
Software de Seguridad y Evaluación de Conformidad	1	1.300	1.300
Gastos de Transporte	4 días	185	740
Gastos de Alimentación	7 días	110	770
Gastos Administrativos	1	400	400
Total Estimado			**11810**

Referencias bibliográficas o Anexos

[1] C. Villanueva and M. Vizcarra, “Decreto Supremo N.° 054-2018-PCM,” 2018, Accessed: Oct. 23, 2024. [Online]. Available: https://www.gob.pe/institucion/pcm/normas-legales/3104-054-2018-