Visado digitalmente por:
HEIGHES SIFUENTES Alfonso Federico FAU 20546798152 soft
Cargo: ESPECIALISTA I EN SEGURIDAD DE LA INFORMACIÓN
Fecha: 11/06/2021 09:27

Visado digitalmente por:
INFANTES MONTALVO Ivette Melva FAU 20546798152 soft
Cargo: DIRECTOR DE SISTEMA ADMINISTRATIVO III DE LA OFICINA DE GESTION DEL TALENTO
Fecha: 11/06/2021 10:29

Visado digitalmente por: DOOR SALAS Marielle FAU 20546798152 soft
Cargo: DIRECTOR DE SISTEMA ADMINISTRATIVO III DE LA OFICINA DE ASESORIA JURIDICA
Fecha: 11/06/2021 11:57

Visado digitalmente por:
TUESTA EGUSQUIZA Jorge Martin FAU 20546798152 soft
Cargo: DIRECTOR DE SISTEMA ADMINISTRATIVO III DE LA OFICINA DE PLANIFICACIÓN Y PRESUPUESTO
Fecha: 11/06/2021 12:57

Visado digitalmente por:
LUJAN TORREALVA Franco Silvio FAU 20546798152 hard
Cargo: ASESOR II DE LA DIRECCIÓN EJECUTIVA
Fecha: 11/06/2021 13:25

Firmado digitalmente por:
TAPIA CASTILLO Jackeline FAU 20546798152 soft
Cargo: DIRECTOR DE SISTEMA ADMINISTRATIVO III DE LA OFICINA DE INNOVACION Y TECNOLOGIA
Fecha: 11/06/2021 10:23

Firmado digitalmente por:
BENITES AVALO Maricarmen FAU 20546798152 soft
Cargo: DIRECTOR DE SISTEMA ADMINISTRATIVO III OFICINA DE ATENCION AL CIUDADANO Y GESTION DOCUMENTARIA
Fecha: 11/06/2021 11:12

Plan de Seguridad de la Información - PRONABEC

SE	OBJETIVO	ACTIVIDADES	ENTREGABLES COMO PRODUCTO DE LAS ACTIVIDADES	2021										
				MAR	ABR	MAY	JUN	JUL	AGO	SET	O			
ación de un SGSI del PRONABEC														
FASE I ZACIÓN	Desarrollar las actividades principales para la dirección e inicio de la implementación del SGSI	Desarrollo de documentos requeridos para el Sistema de Gestión de Seguridad de la Información.	1. Procedimiento para la gestión de documentos y registros.	x										
E II N (PLANEAR)	Desarrollar las actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo.	Formulación del alcance del sistema de Gestión de Seguridad de la información.	2. Formulación del análisis de contexto y requerimiento de seguridad de las partes interesadas.	x										
			3. Alcance y límites del SGSI.											
		Declaración de la política y los objetivos de seguridad de la información.	4. Validación de la política y objetivos de seguridad de la información.		x									
			5. Reformulación de los roles y responsabilidades del SGSI.											
		· Definición de los criterios para la evaluación y aceptación de riesgos.	6. Metodología de gestión de riesgos.		x	x								
		Análisis y evaluación de los riesgos identificados y de las medidas correctivas existentes.	7. Inventario de activos de información.											
			8. Cuadro de análisis y evaluación de riesgos.			x	x	x						
			9. Cuadro de tratamiento de riesgos.											
			10. Informe sobre el resultado de la gestión de riesgos y el tratamiento de los riesgos.											
		Desarrollo de un plan de tratamiento de riesgos	11. Plan de tratamiento de riesgos.											
			12. Plan de concientización en seguridad de la información.						x	x	x			
		· Desarrollo de la declaración de aplicabilidad	13. Declaración de aplicabilidad.											
		Elaboración del plan de trabajo priorizado	14. Plan de trabajo priorizado, aprobado por los propietarios de los riesgos.											
E III DESPLIEGUE (HACER)	Desplegar las actividades de implementación del SGSI	· Desarrollo de documentos y registros necesarios.	15. Políticas o lineamientos específicos para la seguridad de la información.											
		· Implementación de los controles seleccionados del plan de tratamiento de riesgos.	16. Plan de tratamiento de riesgos implementado.			x	x	x	x	x	x	x		
		· Fortalecimiento de la gestión de incidentes	17. Procedimiento de gestión de incidentes de seguridad de la información.											
			18. Plan de concientización en seguridad de la Información implementado.											
FASE IV REVISION (VERIFICAR)	Realizar actividades de revisión del SGSI evidenciando el cumplimiento de los requisitos de la NTP ISO/IEC 27001:2014.	· Monitoreo del desempeño del SGSI	19. Informe de los resultados de la medición y monitoreo del SGSI.											
			20. Informe de la revisión de la alta dirección (Comité de Gobierno Digital).										x	x
		· Auditoría interna del SGSI	21. Programa de auditoría interna.											
			22. Informe de los resultados de la auditoría interna.											x
FASE V CONSOLIDACION (ACTUAR)	Implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la NTP ISO/IEC 27001:2014.	· Implementación de acciones correctivas y preventivas	23. Plan de acciones correctivas y preventivas.											
		· Desarrollo, corrección y mejora de la documentación del SGSI nueva y existente	24. Informe de resultados de las acciones correctivas implementadas.											
		· Desarrollo de las actividades para evidenciar la mejora continua del SGSI	25. Plan de mejora continua.											