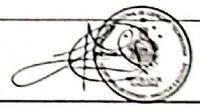


 IHCIETI Instituto Hondureño de Ciencia Tecnología y la Innovación	INSTITUTO HONDUREÑO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN (IHCIETTI)	 INFOTECNOLOGÍA SENACYT
	DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES	
PR-TIC-001	MANUAL DE PROCEDIMIENTO	IHCIETI
Versión 1.0	Fecha: 25 de Abril 2025	25 de 78

11. Gestión del Riesgo

 IHCIETI Instituto Hondureño de Ciencia Tecnología y la Innovación	INSTITUTO HONDUREÑO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN	IHCIETI/141-03 IHCIETI/142-00												
	MATRIZ PARA LA EVALUACIÓN, ANÁLISIS Y RESPUESTA A LOS RIESGOS													
PROCESO:		ADMINISTRACIÓN DEL SERVIDOR DE CORREO ELECTRÓNICO INSTITUCIONAL (ADMINISTRACIÓN DE CUENTAS DEL SERVICIO DE CORREO ELECTRÓNICO)												
NOMBRE DEL SUBPROCESO:		no aplica												
OBJETIVO:		Administrar de manera eficiente el servidor de correo electrónico institucional creando y gestionando cuentas de usuario con un tiempo de respuestas máximo de 24 horas para solicitudes.												
(1) No.	(2) Etapa del proceso	(3) Descripción del Riesgo	Riesgo Inherente		(6) Zona de Riesgo Preliminar	(7) Controles obligatorios para mitigar los riesgos	(8) Controles que existen en la entidad	(9) Controles pendientes por establecer para mitigar los riesgos	Efectividad de los controles existentes		Riesgo Residual		(14) Zona de Riesgo Final	(15) Respuesta a los Riesgos
			(4) P	(5) I					(10) P	(11) I	(12) P	(13) I		
1	Recepción de solicitud de creación, modificación ó deshabilitación a cuentas de usuario de correo electrónico	Pérdida de conectividad por fallos de red o infraestructura de telecomunicaciones no detectados a tiempo, afectando la operatividad de los servicios.	2	2	B	Monitoreo proactivo de infraestructura y revisiones semanales para mantenimiento preventivo.	Software de monitoreo de red	Ninguno	2	2	2	2	B	Aceptar
2	Validación de datos	Exposición de datos sensibles o acceso no autorizado debido a configuración deficiente o falta de actualización en políticas de seguridad.	2	2	B	Implementación de autenticación de múltiples factores y revisiones mensuales de políticas de seguridad y permisos de acceso.	Autenticación de dos factores y revisión periódica de accesos	Ninguno	2	2	2	2	B	Aceptar
3	Crear, modificar, deshabilitar	Interrupción de operaciones institucionales por fallas en equipos críticos debido a falta de mantenimiento o inspección de componentes desgastados.	2	2	B	Mantenimiento preventivo programado y revisión exhaustiva de equipos críticos cada seis meses.	Programa de mantenimiento de equipos críticos implementado	Ninguno	2	2	2	2	B	Aceptar
4	Configuración de cuenta de correo a usuario final	Fallos técnicos durante eventos oficiales por mal funcionamiento de equipo audiovisual, impactando la calidad de las presentaciones.	2	2	B	Pruebas de funcionamiento de equipo y configuración previa al evento, con equipo de respaldo disponible.	Inspección y pruebas previas de equipo audiovisual	Ninguno	2	2	2	2	B	Aceptar
5	Registro y documentación	Cortes o problemas de transmisión en	2	2	B	Optimización de red para tráfico de	Monitoreo de ancho de banda y ajustes en	Ninguno	2	2	2	2	B	Aceptar
Elaborado por: Oscar Padilla.						Revisado por: Marcial Casido			Aprobado por: Luther Castillo					
Firma: 						Firma: 			Firma: 					
Fecha:						Fecha:			Fecha:					