CONATEL
TETÃ MARANDUMBYRY ÑOMOIRU´ATY (TMÑA)

GOBIERNO DEL PARAGUAY | PARAGUÁI REKUÁI

RIESGOS

DE LA

UNIDAD DE

REDES Y SEGURIDAD

COMISIÓN NACIONAL DE TELECOMUNICACIONES

ADMINISTRACIÓN DE RIESGOS Y CONTROLES

DEPARTAMENTO DE INFORMATICA

(1)Proceso: GESTIÓN DE LA INFRAESTRUCTURA TECNOLOGICA

(2)Objetivo del Proceso: **Atender la infraestructura y los Servicios ofrecidos en cuanto a Redes y Sistemas, así como también, las incidencias, requerimientos o problemas que afectan el buen funcionamiento de los servicios y recursos de tecnologías de la información y comunicaciones**

(3)Procedimiento: Administración de la infraestructura de Red

Identificación de los riesgos				Análisis de los riesgos				Definición de los controles	
(4)ACTIVIDAD	**(5)DESCRIPCIÓN DEL RIESGO**	**(6)CAUSA**	**(7)EFECTO**	**(8)PROBABILIDAD**	**(9)IMPACTO**	**(10)CALIFICACIÓN**	**(11)EVALUACIÓN**	**(12)DESCRIPCIÓN DEL CONTROL EXISTENTE**	**(13)NUEVAS ACCIONES DE CONTROL**
1- Monitorear los estados de operación de los servidores, storage y switches	Error: Deficiencias en la operativa de los servicios.	*Desconocimiento realizar el monitoreo de la operativa. Falta de experiencia del personal	* Pérdida de tiempo en la generación de servicios de red.	2	10	20	Tolerable	Monitoreo periódico del estado de los equipos mediante herramientas de supervisión y revisión manual.	Implementar monitoreo automatizado con alertas en tiempo real y registros históricos de incidencias.
2- Solucionar inconvenientes de operación de los equipos de la infraestructura de red	Demora: Tardanza en la asignación de recursos para dar respuesta a la solicitud	*Desinterés * Burocracia	* Retrasos en la atención de la solicitud * Afectación económica la institución	2	10	20	Tolerable	Atención de incidencias conforme a la experiencia del personal técnico.	Establecer procedimientos documentados de atención de incidentes y tiempos de respuesta definidos.
3- Solicitar soporte externo por garantía de equipos o servicios	Error: No identificar los problemas a fin de brindar soluciones adecuadas	*Mala intención * Falta de conocimiento	*Retrasos y tensiones laborales	2	10	20	Tolerable	Gestión de solicitudes de soporte según necesidad detectada.	Mantener un registro actualizado de garantías, contratos y proveedores con responsables asignados.
4- Comunicar al Directorio en los casos de afectación, degradación o interrupción de los servicios de la infraestructura de red	Desinformación: Mala información a la hora de comunicar los efectos de las dificultades en la disposición de los servicios de la red.	* Falta de conocimiento * Desidia	Pérdidas económicas. Retrasos en los trabajos	2	10	20	Tolerable	Comunicación informal o reactiva ante eventos críticos.	Definir un protocolo de comunicación formal con niveles de impacto y tiempos de notificación.

5- Realizar copias de respaldo de los equipos de la infraestructura de red	Error: Toma de decisiones erradas en el momento de realizar la copia de seguridad de los sistemas y servicios	*Complejidad de aspectos técnicos * Falta de conocimientos y experiencia de los integrantes del Grupo de Trabajo	* Retrasos en iniciar la instalación de los equipos * Afectación negativa a la imagen institucional.	2	10	20	Tolerable	Ejecución de respaldos periódicos de configuraciones.	Automatizar los respaldos y verificar regularmente la restauración de la información.
6- Verificar las necesidades técnicas, licencias de operación y obsolescencia tecnológica de los equipos de la infraestructura.	Inexactitud: No identificar los problemas de obsolescencia y caducidad de licencias	*Desinterés * Burocracia * Falta de criterio	* Afectación negativa a la imagen	2	10	20	Tolerable	Evaluación técnica realizada de manera ocasional.	Elaborar un inventario tecnológico actualizado con alertas de vencimiento y obsolescencia.
7- Recepcionar pedido creación, modificación o eliminación de cuentas de usuario, correo, acceso a carpetas compartidas, puertos de red	Colapso de sistemas: Decrecimiento o disminución intensa de la interconexión de sistemas informáticos situados a distancia	Sistemas deficientes. Falta de tecnología actualizada	Daño de la información. Pérdida de imagen. Pérdidas económicas.	2	10	20	Tolerable	Recepción de solicitudes por medios formales (correo o nota).	Centralizar las solicitudes mediante un formulario o sistema de gestión de requerimientos.
8- Comprobar la disponibilidad de licencias para la creación de cuentas	El virus informático es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de diskettes o de la red telefónica de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas computarizados.	actos malintencionados, bulnerabilidad en los sistemas de seguridad	Daño de la información. Interrupción de servicios.	2	10	20	Tolerable	Verificación manual de licencias disponibles.	levar un control automatizado del uso y disponibilidad de licencias.

9- Ejecutar la acción solicitada por el recurrente	Error: Toma de decisiones erradas en la ejecución de acciones solicitadas	* Desidia *Desinterés. *Burocracia	* Afectación negativa a la imagen del área	2	10	20		Ejecución directa por el personal técnico autorizado.	Aplicar el principio de doble verificación o aprobación previa para acciones críticas.
10-Remitir al usuario las credenciales de acceso creadas para el efecto	Demora Tardanza en la remisión de las credenciales de acceso	*Sobrecarga de trabajo * Desinterés	Afectación negativa a la imagen del área Pérdidas económicas	2	10	20		nvío de credenciales por medios institucionales.	Utilizar canales seguros y obligar al cambio de contraseña en el primer acceso.
11-Informar al usuario y al superior inmediato (si corresponde), la culminación del pedido	Desinformación: Mala información a la hora de comunicar los efectos y los resultados de los usuarios	* Falta de conocimiento * Desidia	Pérdidas económicas. Retrasos en los trabajos	2	10	20		Notificación al usuario al finalizar la solicitud.	Registrar la confirmación de cierre del pedido y conservar evidencia de la comunicación.
12-Cerrar el pedido de usuario de creación, modificación o eliminación de cuentas.	Inexactitud: No realizar la culminación de la atención realizada por falta de información	* Falta de conocimiento * Desidia	Pérdidas económicas. Retrasos en los trabajos	2	10	20			
13-Registrar el alta, modificación o eliminación en la base de datos de usuarios	Inexactitud: Información falsa o incompleta en la base de datos de los usuarios	Falta de información Desidia. Desinterés	Incongruecias. Afectación negativa a la imagen del área	2	10	20			

COMISIÓN NACIONAL DE TELECOMUNICACIONES

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -

COMPONENTE: CONTROL DE LA PLANIFICACION

PRINCIPIO: IDENTIFICACION Y EVALUACION DE RIESGOS

FORMATO: Identificación de Riesgos – Subprocesos

Nº: 69

Versión 2,0

(1) MACROPROCESO : GESTIÓN DE LAS TICS

(2) PROCESO: GESTIÓN DE LA INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN

(1) Subproceso	(2) OBJETIVO	(3) RIESGOS	(4) DESCRIPCIÓN	(5) AGENTE GENERADOR	(6) CAUSAS	(7) EFECTOS
Administración de la Infraestructura de Red	**Garantizar que los recursos de la red estén disponibles para los usuarios de manera efectiva y rápida**	Demora	Tardanza en la asignación de los recursos de red	personas, sistemas	Sobrecarga de trabajos. Atención de urgencias. Falta de personal capacitado	Retrasos en los procesos institucionales.
		Error	Deficiencias en la Asignación de recursos de la red	Personas	Falta de personal capacitado. Desatención. Falta de interés.	Retrasos en la entrega de los productos. Pérdidas económicas. Pérdida de imagen
		Colapso de sistemas	Decrecimiento o disminución intensa de la interconexión de sistemas informáticos situados a distancia	sistemas, entorno,	Sistemas deficientes. Falta de tecnología actualizada	Daño de la información. Pérdida de imagen. Pérdidas económicas.

COMISIÓN NACIONAL DE TELECOMUNICACIONES

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP

COMPONENTE: CONTROL DE LA PLANIFICACION

PRINCIPIO: IDENTIFICACION Y EVALUACION DE RIESGOS

FORMATO: Calificación y Evaluación de Riesgos - Procesos

Nº: 73

Versión 2,0

(1) MACROPROCESO : GESTIÓN DE LAS TICS

(2))Procesos	(3) Riesgos	CALIFICACIÓN			(7) Evaluación	(8) Medidas de Respuesta
		(4)	(5)	(6)		
		Probabilidad	Impacto	Calificación		
GESTIÓN DE LA INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN	Virus informáticos	1	20	20	Tolerable	Proteger a la institución. Compartir
	Demora	3	10	30	Importante	Prevenir el riesgo. Proteger a la institución. Compartir
	Colapso de sistemas	2	20	40	Importante	Prevenir el riesgo. Proteger a la institución. Compartir

COMISIÓN NACIONAL DE TELECOMUNICACIONES

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP

COMPONENTE: CONTROL DE LA PLANIFICACION

PRINCIPIO: IDENTIFICACION Y EVALUACION DE RIESGOS

FORMATO: Calificación y Evaluación de Riesgos - Subprocesos

Nº: 74

Versión 2.0

(1) MACROPROCESO : GESTIÓN DE LAS TICS

(2) PROCESO: GESTIÓN DE LA INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN

(3) Subprocesos	(4) Riesgos	CALIFICACIÓN			(8) Evaluación	(9) Medidas de Respuesta
		(5) Probabilidad	(6) Impacto	(7) Calificación		
Administración de la Infraestructura de Red	Demora	2	20	40	Importante	Prevenir el Riesgo. Proteger la Institución. Compartir
	Error	1	20	20	Tolerable	Proteger la Institución. Compartir
	Colapso de sistemas	2	20	40	Importante	Prevenir el Riesgo. Proteger la Institución. Compartir

COMISIÓN NACIONAL DE TELECOMUNICACIONES

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP

COMPONENTE:	**CONTROL DE LA PLANIFICACIÓN**
PRINCIPIO:	**IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS**
FORMATO:	**Ponderación Subprocesos y Riesgos**
Nº:	**79**

Versión 2.0

(2) PROCESO: GESTIÓN DE LA INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN

PONDERACIÓN SUBPROCESOS			**PONDERACIÓN DE RIESGOS SUBPROCESOS**	
(1) Subprocesos	**(3) Ponderación %**		**(4) Riesgos**	**(5) Ponderación %**
Administración de la Infraestructura de Red	**50%**		Demora	31%
Administración de la Seguridad Informática	**50%**		Error	15%
			Colapso de sistemas	31%
			Virus informáticos	23%
Total:	**100%**		**Total:**	**100%**

COMISIÓN NACIONAL DE TELECOMUNICACIONES

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP

COMPONENTE: CONTROL DE LA PLANIFICACIÓN

PRINCIPIO: IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS

FORMATO: Priorización Riesgos y Procesos

Nº: 84

Versión 2.0

(1) MACROPROCESO : GESTIÓN DE LAS TICS

(2) PROCESO: GESTIÓN DE LA INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN

(1) Riesgos	(A) Subprocesos	Administración de la Infraestructura de Red		Administración de la Seguridad Informática		(3) Total Puntaje Riesgo	(4) Priorización de Riesgo
	(B)% Ponderación Subproceso	50%		50%			
	(2) % Ponderación Riesgo	Calificación	Peso	Calificación	Peso		
Demora	31%	**40**	**6,15**	**40**	**6,15**	**12,31**	**1**
Error	15%	**20**	**1,54**	**20**	**1,54**	**3,08**	**3**
Colapso de sistemas	31%	**40**	**6,15**	**40**	**6,15**	**12,31**	**1**
Virus informáticos	23%			**60**	**6,92**	**6,92**	**2**
(C) Total Subproceso	100%		**13,85**		**20,77**	**34,62**	
(D) Priorización de Subproceso							

COMISIÓN NACIONAL DE TELECOMUNICACIONES

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP

COMPONENTE: CONTROL DE LA PLANIFICACION

PRINCIPIO: IDENTIFICACION Y EVALUACION DE RIESGOS

FORMATO: Mapa de Riesgos - Procesos

Nº: 88

Versión 2.0

(2) PROCESO: GESTIÓN DE LA INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN			
(1) RIESGOS	**(2) DESCRIPCIÓN**	**(3) TOTAL PUNTAJE RIESGO**	**(4) PRIORIZACIÓN DEL RIESGO**
Virus informáticos	el virus informático es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de diskettes o de la red telefónica de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas computarizados.	6,15	1
Demora	Tardanza en atender a los usuarios de redes y sistemas y brindar soluciones oportunas a sus requerimientos.	1,54	2
Colapso de sistemas	Decrecimiento o disminución intensa de la interconexión de sistemas informáticos situados a distancia	6,15	1

COMISIÓN NACIONAL DE TELECOMUNICACIONES

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP-

COMPONENTE: CONTROL DE LA PLANIFICACION

PRINCIPIO: IDENTIFICACION Y EVALUACION DE RIESGOS

FORMATO: Mapa de Riesgos - Subprocesos

Nº: 89

Versión 2.0

(1) MACROPROCESO : GESTIÓN DE LAS TICS

(2) PROCESO: GESTIÓN DE LA INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN

(3) SUBPROCESO: Administración de la Infraestructura de Red

(1) RIESGOS	(2) DESCRIPCIÓN	(3) TOTAL PUNTAJE RIESGO	(4) PRIORIZACIÓN DEL RIESGO
Demora	Tardanza en la asignación de los recursos de red	6,15	1
Error	Deficiencias en la Asignación de recursos de la red	1,54	2
Colapso de sistemas	Decrecimiento o disminución intensa de la interconexión de sistemas informáticos situados a distancia	6,15	1

COMISIÓN NACIONAL DE TELECOMUNICACIONES

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP

COMPONENTE: CONTROL DE LA PLANIFICACION

PRINCIPIO: IDENTIFICACION Y EVALUACION DE RIESGOS

FORMATO: Definición Políticas Administración de Riesgos - Objetivos Institucionales

Nº: 91

Versión 2.0

(1) MACROPROCESO : GESTIÓN DE LAS TICS

(2) PROCESO: GESTIÓN DE LA INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN

(3) SUBPROCESO: Administración de la Infraestructura de Red

(5) Objetivos Institucionales/Macroproceso/Proceso/Subproceso (X) ACTIVIDAD	(6) Riesgos	(7) Puntaje	(8) Políticas Administración de Riesgos
1- Monitorear los estados de operación de los servidores, storage y switches	Demora	6,15	El control y seguimiento al registro de solicitudes de asistencia técnica Mitigar el impacto del riesgo de error: mediante la capacitación del personal y disminuir la rotación del personal en esta área, de manera a mejorar la experiencia Mitigar el impacto del riesgo de Colapso de sistemas: mediante el seguimiento y backup de los sistemas
2- Solucionar inconvenientes de operación de los equipos de la infraestructura de red			
3- Solicitar soporte externo por garantía de equipos o servicios			
4- Comunicar al Directorio en los casos de afectación, degradación o interrupción de los servicios de la infraestructura de red			
5- Realizar copias de respaldo de los equipos de la infraestructura de red	Error	1,54	
6- Verificar las necesidades técnicas, licencias de operación y obsolescencia tecnológica de los equipos de la infraestructura.			
7- Recepcionar pedido creación, modificación o eliminación de cuentas de usuario, correo, acceso a carpetas compartidas, puertos de red			
8-Comprobar la disponibilidad de licencias para la creación de cuentas			

COMISIÓN NACIONAL DE TELECOMUNICACIONES

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP

COMPONENTE: CONTROL DE LA PLANIFICACION

PRINCIPIO: IDENTIFICACION Y EVALUACION DE RIESGOS

FORMATO: Definición Políticas Administración de Riesgos - Objetivos Institucionales

Nº: 91

Versión 2.0

(1) MACROPROCESO : GESTIÓN DE LAS TICS

(2) PROCESO: GESTIÓN DE LA INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN

(3) SUBPROCESO: Administración de la Infraestructura de Red

(5) Objetivos Institucionales/Macroproceso/Proceso/Subproceso (X) ACTIVIDAD	(6) Riesgos	(7) Puntaje	(8) Políticas Administración de Riesgos
9- Ejecutar la acción solicitada por el recurrente	Colapso de sistemas	6,15	El control y seguimiento al registro de solicitudes de asistencia técnica Mitigar el impacto del riesgo de error: mediante la capacitación del personal y disminuir la rotación del personal en esta área, de manera a mejorar la experiencia Mitigar el impacto del riesgo de Colapso de sistemas: mediante el seguimiento y backup de los sistemas
10-Remitir al usuario las credenciales de acceso creadas para el efecto			
11- Informar al usuario y al superior inmediato (si corresponde), la culminación del pedido			
12-Cerrar el pedido de usuario de creación, modificación o eliminación de cuentas.			
13-Registrar el alta, modificación o eliminación en la base de datos de usuarios			

Elaborado por:

FERNANDO RAMIRO NUÑEZ SOSA

Firmado digitalmente por FERNANDO RAMIRO NUÑEZ SOSA
Nombre de reconocimiento (DN): c=PY, o=CERTIFICADO NO CUALIFICADO PARA SERVIDORES PÚBLICOS, ou=FIRMA ELECTRÓNICA, sn=NUÑEZ SOSA, givenName=FERNANDO RAMIRO, serialNumber=CI4415430, cn=FERNANDO RAMIRO NUÑEZ SOSA
Fecha: 2026.01.13 14:19:16 -03'00'

Revisado por: RODNEY ALBERTO COLMAN ALVARENGA

Digitally signed by RODNEY ALBERTO COLMAN ALVARENGA
Date: 2026.01.14 07:32:38 -03'00'

Aprobado por el Directorio de la CONATEL