

**DIRECCIÓN NACIONAL DE CORREOS DEL PARAGUAY - DINACOPA**  
**MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -**  
**COMPONENTE CORPORATIVO DE CONTROL ESTRATÉGICO**

COMPONENTE: ADMINISTRACION DE RIESGOS  
 ESTÁNDAR: IDENTIFICACION DE RIESGOS  
 FORMATO: Identificación de Riesgos- Macroprocesos  
 N°: 67

(1) MACROPROCESO	(2) OBJETIVO	(2) RIESGOS	(3) DESCRIPCION	(4) AGENTE GENERADOR	(5) CAUSAS	(6) EFECTOS
Gestión Tecnológica	Gestionar la aplicación de las TICS y mantener la fiabilidad y seguridad la información.	CAMBIOS CLIMÁTICOS	alteración en las condiciones climáticas	Personal, insumos, equipos, instalaciones, logística	lluvias, aumento de temperatura	interrupcion de suministro eléctrico o servicios de conectividad o sobrecargas eléctricas, degradación del rendimiento de equipos informáticos
		FALLAS DE SOFTWARE	defecto que puede presentarse en el conjunto de programas que ha sido diseñado para que la computadora pueda desarrollar su trabajo		sobrecargas de trabajos de servidores, cierres inesperados de sistema	disminución del ritmo de trabajo, perdida de información
		FALLAS DE HARDWARE	defecto que puede presentarse en los Comités de un sistema informático, que impide su correcto funcionamiento		apagado incorrecto, fin de tiempo de vida útil, acumulación de polvo	falla en el inicio de sistema; dificultad de operación; sobrecalentamiento
		VIRUS INFORMÁTICO	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 computarizado		phishing/spam; ejecución de programas inseguros; ataques intencionados	problemas de reputación en internet(correo electrónico); alteraciones en software/perdida de información; denegación de servicios web
		FALTA DE RECURSOS HUMANOS	Falta de personal para cumplir con tareas asignadas en una determinada área		insuficiencia de personal	imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
		SABOTAJE	destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o materias primas, con el fin de suspender o paralizar el trabajo		funcionarios insatisfechos; obtener ingresos de mala forma	interrupción de los procesos y servicios; perdida o robo de datos de usuarios

Elaborado por:  
 Sr. Rodrigo Toledo  
 Equipo Técnico MECIP

Fecha: 27/12/2023



Revisado por:  
 Ing. Enrique Godoy  
 Director de Tecnología

Fecha: 29/12/2023



Aprobado por:  
 Abog. Laritta Carozzo  
 Coordinadora MECIP

Fecha:



Dr. Nidia Lopez de González  
 Directora General  
 DINACOPA

Sr. Cesar Benítez  
 Secretario General  
 DINACOPA



**DIRECCIÓN NACIONAL DE CORREOS DEL PARAGUAY - DINACOPA**  
**MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -**  
**COMPONENTE CORPORATIVO DE CONTROL ESTRATÉGICO**

COMPONENTE: ADMINISTRACIÓN DE RIESGOS  
 ESTÁNDAR: IDENTIFICACIÓN DE RIESGOS  
 FORMATO: Identificación de Riesgos- Procesos  
 Nº: 68

SO: Gestión de Soporte tecnológico						
(1) PROCESOS	(2) OBJETIVO	(2) RIESGOS	(3) DESCRIPCIÓN	(4) AGENTE GENERADOR	(5) CAUSAS	(6) EFECTOS
Gestión de Infraestructura y Redes	gestionar la instalación y mantenimiento de la infraestructura de redes.	1. Cambios climáticos 2. Virus informático 3. Falta de recursos humanos. Humanos	1. alteración en las condiciones climáticas 2. 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 computarizado 3. Falta de personal para cumplir con tareas asignadas en una determinada área.	Personal, insumos, equipos, instalaciones, logística	1. lluvias, aumento de temperatura 2. phishing/spam; ejecución de programas inseguros; ataques intencionados 3. insuficiencia de personal	1. interrupción de suministro eléctrico o servicios de conectividad o sobrecargas eléctricas; degradación del rendimiento de equipos informáticos 2. problemas de reputación en internet (correo electrónico); alteraciones en software/perdida de información; denegación de servicios web 3. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Gestión de Sistemas	gestionar y desarrollar sistemas acordes a las necesidades de la institución	1. Fallos de software 2. Fallos de hardware 3. Falta de recursos humanos	1. alteración en las condiciones climáticas 2. 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 computarizado 3. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. lluvias, aumento de temperatura 2. phishing/spam; ejecución de programas inseguros; ataques intencionados 3. insuficiencia de personal	1. interrupción de suministro eléctrico o servicios de conectividad o sobrecargas eléctricas; degradación del rendimiento de equipos informáticos 2. problemas de reputación en internet (correo electrónico); alteraciones en software/perdida de información; denegación de servicios web 3. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Gestión de Seguridad de TIC	gestionar políticas de seguridad de TICS	1. Virus informático 2. Falta de recursos humanos 3. Sabotaje	1. 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 computarizado 2. Falta de personal para cumplir con tareas asignadas en una determinada área 3. destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o materias primas, con el fin de suspender o paralizar el trabajo	Personal, insumos, equipos, instalaciones, logística	1. phishing/spam; ejecución de programas inseguros; ataques intencionados 2. insuficiencia de personal 3. funcionarios insatisfechos; obtener ingresos de mala forma	1. problemas de reputación en internet (correo electrónico); alteraciones en software/perdida de información; denegación de servicios web 2. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos 3. interrupción de los procesos y servicios; pérdida o robo de datos de usuarios
Gestión Diagramación y Montaje	gestionar el cumplimiento de estándares técnicos y oficiales de publicaciones de la institución	1. Virus informático 2. Falta de recursos humanos 3. Sabotaje	1. 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 computarizado 2. Falta de personal para cumplir con tareas asignadas en una determinada área 3. destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o materias primas, con el fin de suspender o paralizar el trabajo	Personal, insumos, equipos, instalaciones, logística	1. phishing/spam; ejecución de programas inseguros; ataques intencionados 2. insuficiencia de personal 3. funcionarios insatisfechos; obtener ingresos de mala forma	1. problemas de reputación en internet (correo electrónico); alteraciones en software/perdida de información; denegación de servicios web 2. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos 3. interrupción de los procesos y servicios; pérdida o robo de datos de usuarios

Elaborado por:  
 Sr. Rodrigo Toledo  
 Equipo Técnico MECIP  
 Fecha: 27/12/2023

Revisado por:  
 Ing. Enrique Godoy  
 Director de Tecnología  
 Fecha: 28/12/2023



  
 Dra. Nidia López de González  
 Directora General  
 DINACOPA  
 Sr. César González  
 Secretario General  
 DINACOPA

DIRECCIÓN NACIONAL DE CORREOS DEL PARAGUAY - DINACOPA  
 MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -  
 COMPONENTE CORPORATIVO DE CONTROL ESTRATÉGICO

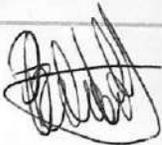
COMPONENTE: ADMINISTRACIÓN DE RIESGOS  
 ESTÁNDAR: IDENTIFICACIÓN DE RIESGOS  
 FORMATO: Identificación de Riesgos- Procesos  
 Nº: 69

MACROPROCESO: Gestión de Soporte Tecnológico  
 PROCESO: Gestión de Infraestructura y Redes

CÓDIGO: DT-F69-00-2023  
 CÓDIGO: DT-F69-00-2023

(1) SUBPROCESOS	(2) OBJETIVO	(2) RIESGOS	(3) DESCRIPCIÓN	(4) AGENTE GENERADOR	(5) CAUSAS	(6) EFECTOS
Gestión de Soporte Técnico y Atención al Usuario	Gestionar los pedidos de soporte y orientación de usuarios de TICs	1. Virus informático 2. Falta de recursos humanos	1. 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 computarizado 2. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. phishing/spam; ejecución de programas inseguros; ataques intencionados 2. insuficiencia de personal	1. problemas de reputación en internet (correo electrónico); alteraciones en software/perdida de información; denegación de servicios web 2. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos

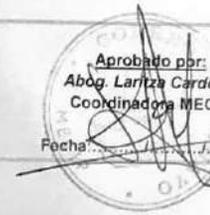
Elaborado por:  
 Sr. Rodrigo Toledo  
 Equipo Técnico MECIP  
 Fecha: 27/12/2023



Revisado por:  
 Ing. Enrique Godoy  
 Director de Tecnología  
 Fecha: 28/12/2023



Aprobado por:  
 Abog. Lariza Cardozo  
 Coordinadora MECIP  
 Fecha: .....



Dra. Nidia López de González  
 Directora General  
 DINACOPA

Sr. César González  
 Secretario General  
 DINACOPA



DIRECCION NACIONAL DE CORREOS DEL PARAGUAY  
**MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -**  
 COMPONENTE CORPORATIVO DE CONTROL ESTRATÉGICO

COMPONENTE: ADMINISTRACIÓN DE RIESGOS  
 ESTÁNDAR: IDENTIFICACIÓN DE RIESGOS  
 FORMATO: Identificación de Riesgos – Actividades  
 Nº: 70

(1) Proceso: Gestión de Infraestructura y Redes

(2) Subproceso:

(3) ACTIVIDADES	(4) OBJETIVO	(5) RIESGOS	(6) DESCRIPCIÓN	(7) AGENTE GENERADOR	(8) CAUSAS	(9) EFECTOS
Asistir en el uso de Herramientas Tecnológicas	Fomentar el uso correcto de Herramientas Tecnológicas, y potenciar las aplicaciones de las mismas mediante metodologías más técnicas	1. Falta de recursos humanos	Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Instalar y mantener aplicaciones de Ofimática y Seguridad	Asegurar la correcta instalación de Herramientas Ofimáticas y de seguridad, y el mantenerlas actualizadas	1. Falta de recursos humanos	Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Gestionar el movimiento de Equipos Informáticos	Acompañar el movimiento de equipos, asegurando la integridad de los mismos	1. Falta de recursos humanos	Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Gestionar el inventario de equipos Tecnológicos de la institución	Controlar el estado de los equipos tecnológicos institucionales, existencias y ubicaciones	1. Falta de recursos humanos	Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Administrar y Gestionar las conexiones a la Red de Datos	Realizar conexiones cableadas o inalámbricas, manteniendo el balanceo de la carga.	Cambios climáticos	alteración en las condiciones climáticas	Personal, insumos, equipos, instalaciones, logística	1. lluvias, aumento de temperatura	interrupción de suministro eléctrico o servicios de conectividad o sobrecargas eléctricas; degradación del rendimiento de equipos informáticos
Vigilar el correcto funcionamiento de la Red de datos de la Institución	Mantener la estabilidad de la red interna	Virus informático	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 computarizado	Personal, insumos, equipos, instalaciones, logística	phishing/spam, ejecución de programas inseguros, ataques intencionados	problemas de reputación en internet (correo electrónico), alteraciones en software/perdida de información, denegación de servicios web
Supervisar las acciones de proveedores de servicios de instalación	Asegurar el cumplimiento de los acuerdos con proveedores	1. Falta de recursos humanos	Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Establecer las políticas de uso correcto de herramientas ofimáticas	Establecer normas de uso adecuadas para proteger la integridad en el uso de herramientas ofimáticas	1. Falta de recursos humanos	Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos

Elaborado por:  
 Sr. Rodrigo Toledo  
 Equipo Técnico MECIP  
 Fecha: 27/12/2023



Revisado por:  
 Ing. Enrique Godoy  
 Director de Tecnología  
 Fecha: 28/12/2023



Aprobado por:  
 Abg. Lariza Cardozo  
 Coordinadora MECIP  
 Fecha: 28/12/2023

Dra. Nidia López de González  
 Directora General  
 DINACOPA  
 Sr. César González  
 Secretario General  
 DINACOPA

**DIRECCION NACIONAL DE CORREOS DEL PARAGUAY**  
**MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -**  
 COMPONENTE CORPORATIVO DE CONTROL ESTRATÉGICO

COMPONENTE: ADMINISTRACIÓN DE RIESGOS

ESTÁNDAR: IDENTIFICACIÓN DE RIESGOS

FORMATO: Identificación de Riesgos – Actividades

Nº: 70

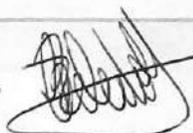
(1) Proceso: Gestión de SISTEMAS

(2) Subproceso:

(3) ACTIVIDADES	(4) OBJETIVO	(5) RIESGOS	(6) DESCRIPCIÓN	(7) AGENTE GENERADOR	(8) CAUSAS	(9) EFECTOS
Diseñar, desarrollar o implementar sistemas o aplicaciones para uso interno Institucional	Fortalecer la funciones de la Institución mediante aplicaciones diseñadas para funciones específicas.	1. Falta de recursos humanos	1. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Gestionar el funcionamiento de sistemas implementados dentro de la Institución	Vigilar la continuidad de la aplicaciones instaladas en la institución y su correcto uso y funcionamiento de las mismas.	1. Fallas de software 2. Fallas de hardware	1. alteración en las condiciones climáticas 2. 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 computarizado	Personal, insumos, equipos, instalaciones, logística	1. lluvias, aumento de temperatura 2. phishing/spam, ejecución de programas inseguros, ataques intencionados	1. interrupción de suministro eléctrico o servicios de conectividad o sobrecargas eléctricas, degradación del rendimiento de equipos informáticos 2. problemas de reputación en internet (correo electrónico), alteraciones en software/perdida de información, denegación de servicios web
Asistir el diseño de aplicativos a ser implementados o adquiridos por la institución	indicar y controlar que los sistemas a ser adquiridos o diseñados para la institución cumplan con los estándares compatibles con las aplicaciones utilizadas en la institución	1. Falta de recursos humanos	1. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Elevar sugerencias de digitalización de servicios de la institución	elevar la calidad de los servicios prestados por la institución mediante la digitalización de los procesos manuales	1. Falta de recursos humanos	1. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Capacitar usuarios de aplicación	realizar capacitaciones respecto al uso de aplicaciones propias de la institución.	1. Falta de recursos humanos	1. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos

Elaborado por:  
Sr. Rodrigo Toledo  
Equipo Técnico MECIP

Fecha: 27/12/2023



Revisado por:  
Ing. Enrique Godoy  
Director de Tecnología

Fecha: 28/12/2023



Aprobado por:  
Abog. Laritza Gardezo  
Coordinadora MECIP

Fecha: 28/12/2023



Dra. Nidia López de González  
Directora General  
DINACOPA

Sr. César González  
Secretario General  
DINACOPA



**DIRECCION NACIONAL DE CORREOS DEL PARAGUAY**  
**MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -**  
**COMPONENTE CORPORATIVO DE CONTROL ESTRATEGICO**

COMPONENTE: ADMINISTRACIÓN DE RIESGOS  
 ESTÁNDAR: IDENTIFICACIÓN DE RIESGOS  
 FORMATO: Identificación de Riesgos – Actividades  
 Nº: 70

(1) Proceso: Gestión de Seguridad TIC

(2) Subproceso:

(3) ACTIVIDADES	(4) OBJETIVO	(5) RIESGOS	(6) DESCRIPCIÓN	(7) AGENTE GENERADOR	(8) CAUSAS	(9) EFECTOS
Configurar accesos a sistemas, equipos y bases de datos de la institución	Asegurar la integridad de datos pertenecientes a la institución, mediante los controles de accesos a los mismos.	1. Falta de recursos humanos	1. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Ejecutar un análisis de riesgos informáticos y adecuar las políticas a la realidad de la institución.	Conocer los potenciales riesgos informáticos y determinar medidas y procedimientos de seguridad.	1. Falta de recursos humanos	1. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Confeccionar normativas del uso y políticas de seguridad de los equipos y sistemas de red.	Establecer los requisitos mínimos de seguridad de TICs de la institución.	1. Falta de recursos humanos 2. Sabotaje	1. Falta de personal para cumplir con tareas asignadas en una determinada área 2. destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o materias primas, con el fin de suspender o paralizar el trabajo	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal 2. funcionarios insatisfechos, obtener ingresos de mala forma	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos 2. interrupción de los procesos y servicios; pérdida o robo de datos de usuarios
Administrar medidas de seguridad y contingencia para los datos institucionales.	Contar con capacidad de respuesta ante incidentes informáticos.	1. Sabotaje	1. destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o materias primas, con el fin de suspender o paralizar el trabajo	Personal, insumos, equipos, instalaciones, logística	1. funcionarios insatisfechos, obtener ingresos de mala forma	1. interrupción de los procesos y servicios; pérdida o robo de datos de usuarios
Vigilar la continuidad de redes y sistemas de información	Proteger la continuidad de los servicios y conectividad de la red	1. Virus informático 2. Sabotaje	1. 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 computarizado 2. destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o materias primas, con el fin de suspender o paralizar el trabajo	Personal, insumos, equipos, instalaciones, logística	1. phishing/spam, ejecución de programas inseguros, ataques intencionados 2. funcionarios insatisfechos, obtener ingresos de mala forma	1. problemas de reputación en internet (correo electrónico), alteraciones en software/pérdida de información, denegación de servicios web 2. interrupción de los procesos y servicios; pérdida o robo de datos de usuarios
Gestionar las publicaciones y el contenido de página web institucional.	Disponer de la información e imagen pública de la institución mediante el portal web	1. Falta de recursos humanos 2. Sabotaje	1. Falta de personal para cumplir con tareas asignadas en una determinada área 2. destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o materias primas, con el fin de suspender o paralizar el trabajo	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal 2. funcionarios insatisfechos, obtener ingresos de mala forma	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos 2. interrupción de los procesos y servicios; pérdida o robo de datos de usuarios

Elaborado por:  
 Sr. Rodrigo Toledo  
 Equipo Técnico MECIP

Fecha: 27/12/2023



Revisado por:  
 Ing. Enrique Godoy  
 Director de Tecnología

Fecha: 28/12/2023



Aprobado por:  
 Abog. Lariza Catilano  
 Coordinadora MECIP

Fecha:



Dr. María Leticia de González  
 Directora General  
 DINACOPA

César González  
 Secretario General  
 DINACOPA

DIRECCION NACIONAL DE CORREOS DEL PARAGUAY  
**MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -**  
 COMPONENTE CORPORATIVO DE CONTROL ESTRATÉGICO

COMPONENTE: ADMINISTRACIÓN DE RIESGOS  
 ESTÁNDAR: IDENTIFICACIÓN DE RIESGOS  
 FORMATO: Identificación de Riesgos – Actividades  
 N°: 70

(1) Proceso: Gestión de Diagramacion y Montaje

(2) Subproceso:

(3) ACTIVIDADES	(4) OBJETIVO	(5) RIESGOS	(6) DESCRIPCIÓN	(7) AGENTE GENERADOR	(8) CAUSAS	(9) EFECTOS
Diseñar Publicaciones Oficiales de la Institucion	Diseñar las Publicaciones Oficiales conforme a lo establecido en las normas vigentes	1. Falta de recursos humanos	1. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Diseñar publicaciones Postales	Diseñar productos postales de acuerdo a lo establecido en las normas vigentes	1. Falta de recursos humanos	1. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos
Adecuar presentaciones segun normas vigentes	Realizar correcciones a Publicaciones de acuerdo a las normas vigentes	1. Falta de recursos humanos 2. Sabotaje	1. Falta de personal para cumplir con tareas asignadas en una determinada área 2. destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o matenas primas, con el fin de suspender o paralizar el trabajo	Personal, insumos, equipos, instalaciones, logística	1. insuficiencia de personal 2. funcionarios insatisfechos; obtener ingresos de mala forma	1. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos 2. interrupción de los procesos y servicios; perdida o robo de datos de usuarios

Elaborado por:  
 Sr. Rodrigo Toledo  
 Equipo Tecnico MECIP

Fecha: 27/12/2023



Revisado por:  
 Ing. Enrique Godoy  
 Director de Tecnologia

Fecha: 28/12/2023



Aprobado por:  
 Abog. Larissa Cardozo  
 Coordinadora MECIP

Fecha:

*Dra. Nidia López de González*  
 Directora General  
 DINACOPA

*Sr. César González*  
 Secretario General  
 DINACOPA



DIRECCION NACIONAL DE CORREOS DEL PARAGUAY  
**MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -**  
 COMPONENTE CORPORATIVO DE CONTROL ESTRATÉGICO

COMPONENTE: ADMINISTRACIÓN DE RIESGOS

ESTÁNDAR: IDENTIFICACIÓN DE RIESGOS

FORMATO: Identificación de Riesgos – Actividades

Nº: 70

(1) Proceso: Gestión de Infraestructura y Redes

(2) Subproceso: Gestión de Soporte Técnico y Atención a Usuarios

(3) ACTIVIDADES	(4) OBJETIVO	(5) RIESGOS	(6) DESCRIPCIÓN	(7) AGENTE GENERADOR	(8) CAUSAS	(9) EFECTOS
Gestionar Pedidos de soporte y Orientar a usuarios de TICs	Gestionar los pedidos de soporte y orientación de usuarios de TICs	1. Virus informático 2. Falta de recursos humanos Humanos	1. 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 computarizado  2. Falta de personal para cumplir con tareas asignadas en una determinada área	Personal, insumos, equipos, instalaciones, logistica	1. phissing/spam; ejecución de programas inseguros; ataques intencionados 2. insuficiencia de personal	1. problemas de reputación en internet (correo electrónico); alteraciones en software/perdida de información; denegación de servicios web 2. imposibilidad de atender todos los pedidos de soporte y cumplimiento de fechas para trabajos

Elaborado por:  
Sr. Rodrigo Toledo  
Equipo Técnico MECIP



Fecha: 27/12/2023

Revisado por:  
Ing. Enrique Godoy  
Director de Tecnología

Fecha: 28/12/2023



*Dra. Nidia López de González*  
Directora General  
DINACOPA

*Sr. César González*  
Secretario General  
DINACOPA