



Dirección Nacional  
de **CORREOS**  
del **PARAGUAY**

■ **GOBIERNO**  
■ **NACIONAL**

*Paraguay  
de la gente*

# POLÍTICA DE CIBERSEGURIDAD

Dirección Nacional de Correos del Paraguay

## “DINACOPA”

CERTIFICO QUE LA PRESENTE  
FOTOCOPIA ES EL REFLEJO  
DEL ORIGINAL QUE TENGO A  
LA VISTA.



Lic. Fernando Riveros  
Director  
Planificación y Proyectos



Norma de  
Requisitos Mínimos  
para Sistemas de  
Control Interno

Asunción - Paraguay 2022



Lic. Fernando Riveros  
Director  
Planificación y Proyectos



**RESOLUCIÓN N° 1895 /2022/DG/SG/MECIP/DT**

**POR LA CUAL SE APRUEBA LA POLÍTICA DE CIBERSEGURIDAD DE LA DIRECCION DE TECNOLOGIA DE LA DIRECCIÓN NACIONAL DE CORREOS DEL PARAGUAY- DINACOPA.**

Asunción, 14 de Diciembre de 2022

**VISTO:** Que en fecha 12 de febrero de 2021, se dictó el Decreto N°4845/2021, "POR LA CUAL SE REGLAMENTA LA LEY N°6562/2020 "DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL."

**CONSIDERANDO:** Que, en fecha 27 de octubre de 2022, se dictó Resolución N°1478/2022/DG/SG/MECIP, "POR LA CUAL SE CONFIRMA EL COMITÉ MULTIDISCIPLINARIO DE LA DIRECCION NACIONAL DE CORREOS DEL PARAGUAY, EN EL MARCO DE LA IMPLEMENTACIÓN DE LA LEY N°6562/2020 "DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL" Y EL DECRETO N°4845/2021 "POR EL CUAL SE REGLAMENTA LA LEY N°6562/2020" "DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL.-"

Que, en fecha 27 de octubre de 2022, se dictó Resolución N°1479/2022/DG/SG/MECIP, "POR LA CUAL SE ADOPTA, LO DISPUESTO EN LA LEY N°6562/2020 "DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL" Y EL DECRETO N°4845/2021 "POR EL CUAL SE REGLAMENTA LA LEY N°6562/2020" "DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL " EN LA DIRECCION NACIONAL DE CORREOS DEL PARAGUAY.-

Que la Ciberseguridad, es la Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afectan su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.-

Que, ante la existencia del Plan Nacional de Ciberseguridad configurándose como documento estratégico que sirve como fundamento para que Paraguay establezca una política pública de ciberseguridad, que integrando a todos los sectores involucrados en el desarrollo de las tecnologías de la información y comunicación (TIC), permita el crecimiento económico y la maximización de los beneficios de las mismas, logrando un ciberespacio más estable, seguro, confiable, y resiliente en base a políticas gubernamentales y nacionales que establece las líneas de acción a ser adoptadas por un país para fortalecer la seguridad de sus activos críticos y lograr un ciberespacio seguro, confiable y resiliente.-

Que, resulta necesario la elaboración de la normativa aplicable a la realidad Institucional en la DINACOPA, tomando en cuenta los estándares, resoluciones y buenas prácticas emitidas por el MITIC.-

Que, de acuerdo a la Ley Nro. 4016/2010, en su Capítulo III, Artículo 07 "Funciones", Inc. i) planificar y formular la política general de la DINACOPA, para el área comercial, operativa, administrativa y financiera"; y en el "Inc. j) diseñar, elaborar y proponer la normativa orgánica de la DINACOPA, para el mejor servicio y funcionamiento administrativo y operativo".-

Lic. Fernando Riveros  
Director  
Planificación y Proyectos

Luis Fernando  
Echeverría  
DINACOPA



**RESOLUCIÓN N° 1895 /2022/DG/SG/MECIP/DT**

**POR LA CUAL SE APRUEBA LA POLÍTICA DE CIBERSEGURIDAD DE LA DIRECCION DE TECNOLOGIA DE LA DIRECCIÓN NACIONAL DE CORREOS DEL PARAGUAY- DINACOPA.**

Que, el Decreto N°32 de fecha 15 de agosto del 2018 de la Presidencia de la República del Paraguay, nombra al Abg. LUIS FERNANDO SERVIN COLMAN, como Director General de la Dirección Nacional de Correos del Paraguay.-

Que, en fecha 25 de Noviembre de 2022, se dictó Resolución N°1667/2022/DG/SG "POR LA CUAL SE DESIGNA ENCARGADO DE DESPACHO DE LA SECRETARÍA GENERAL DE LA DIRECCIÓN NACIONAL DE CORREOS DEL PARAGUAY (DINACOPA)".-

**EL DIRECTOR GENERAL DE LA DINACOPA**

**RESUELVE:**


**Art 1°: APROBAR** la Política de Ciberseguridad de la Dirección de Tecnología de la Dirección Nacional de Correos del Paraguay - DINACOPA, conforme el Anexo I, adjunto a la presente Resolución. -

**Art 2°: DISPONER** que por intermedio de la Asesoría de Comunicación, se proceda a la difusión y socialización correspondiente.-

**Art. 3°: COMUNICAR**, a quienes corresponda, cumplido archivar.-

  
Lic. FERNANDO J. RIVEROS RAMOS  
Encargado de Despacho  
Secretaría General

  
Abg. LUIS FERNANDO SERVIN COLMAN  
Director General  
Dirección Nacional de Correos del Paraguay  
Dinacopa.

 Dirección Nacional de <b>CORREOS del PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b> Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 1 de 16

## ***POLÍTICA DE CIBERSEGURIDAD***

Dirección Nacional de Correos del Paraguay- DINACOPA

### ***Elaboración:***

Coordinación Mecip-Departamento Mejora Continua: Sra. Monique Mireya Mora; Funcionaria

### ***Verificación:***

Coordinación Mecip: Abg. Laritza Cardozo; Coordinadora  
 Dirección de Tecnología: Lic. Synthia Pereira, Directora

### ***Aprobación:***

***Comite de Control Interno; Comité Multidisciplinario-DINACOPA***

### ***Diseño y Diagramación:***

Sra. Monique Mireya Mora, Funcionaria

CERTIFICO QUE LA PRESENTE FOTOCOPIA ES FIEL REFLEJO DEL ORIGINAL QUE TENGO A LA VISTA.

Dirección Nacional de Correos del Paraguay- DINACOPA

Dirección: 25 de Mayo esq. Yegros

Teléfono: (+595 21) 498112/13




Lic. Fernando Riveros  
 Director  
 Planificación y Proyectos

[www.correoparaguayo.gov.py](http://www.correoparaguayo.gov.py)

Asunción-Paraguay 2022



Lic. Fernando Riveros  
 Director  
 Planificación y Proyectos

 Dirección Nacional de <b>CORREOS</b> del <b>PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b>  Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 2 de 16

## ÍNDICE

<b>INTRODUCCIÓN</b>	<b>3</b>
<b>PRINCIPIOS</b>	<b>4</b>
OBJETIVOS	4
RESPONSABILIDADES	4
<b>RESOLUCIONES RELACIONADAS</b>	<b>5</b>
<b>DIMENSIONES DE LA SEGURIDAD.</b>	<b>6</b>
CRITERIOS PARA DEFINICIÓN DE NIVELES DE CRITICIDAD DE UN INCIDENTE CIBERNÉTICO.	6
<b>GESTIÓN DE ACTIVOS</b>	<b>8</b>
CICLO DE VIDA DE LA INFORMACIÓN	8
PREVENCIÓN DE FUGA DE LA INFORMACIÓN	8
BUENAS PRÁCTICAS CONTRA LA FUGA DE LA INFORMACIÓN.	9
GESTIÓN DE LA COPIA DE SEGURIDAD	10
• A NIVEL USUARIO:	10
• A NIVEL SERVIDOR:	10
<b>CONTROL DE ACCESO</b>	<b>10</b>
REQUISITOS PARA EL CONTROL DE ACCESO	11
NIVEL DE ACCESO	11
SEGURIDAD EN EL ÁMBITO DE DESARROLLO DE SISTEMAS	12
SEGURIDAD EN LOS PROVEEDORES	12
<b>REVISIÓN DE LA POLÍTICA</b>	<b>13</b>
<b>GLOSARIO</b>	<b>14</b>




CERTIFICO QUE LA PRESENTE  
FOTOCOPIA ES FIEL REFLEJO  
DEL ORIGINAL QUE TENGO A  
LA VISTA.



Lic. Fernando Riveros  
Director  
Planificación y Proyectos



Lic. Fernando Riveros  
Director  
Planificación y Proyectos

 Dirección Nacional de <b>CORREOS del PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b> Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 3 de 16

## INTRODUCCIÓN

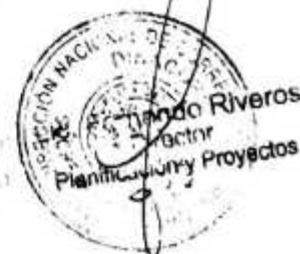
La naturaleza sin fronteras del internet, la economía digital, la creciente interdependencia por medio del IoT y la delincuencia informática, pintan una imagen legal y operativa compleja para la ciberseguridad. Casi todos los sectores utilizan TIC y dependen del internet para todo, desde las tareas más simples, hasta las más estratégicas.

Las cadenas de suministro globales están interconectadas cada vez más, y los sistemas TIC a lo largo de esas cadenas de suministro tienen dispositivos internos y externos que pretenden facilitar las operaciones de los negocios. Sin embargo, estos sistemas interconectados crean un paisaje complejo en el que combatir la delincuencia informática puede ser particularmente desafiante, conforme los actores maliciosos pueden explotar fácilmente las vulnerabilidades en los procesos de negocios y atacar empleados en lo individual, a lo largo de todas las partes de la cadena de suministro. Adicionalmente a los riesgos operativos y de comportamiento, las manifestaciones técnicas de los ataques cibernéticos, desde Malware hasta Ransomware.


Por ende, la ciberseguridad no es sólo un asunto técnico. También surgen nuevas estrategias organizacionales, políticas públicas y reglas de comportamiento en la red que constituyen conocimientos suaves y activos intangibles que son críticos para contar con un entorno de ciberseguridad eficaz y económicamente viable para la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.



CERTIFICO QUE LA PRESENTE  
 FOTOCOPIA ES FIEL REFLEJO  
 DEL ORIGINAL QUE TENGO A  
 LA VISTA.



Lic. Fernando Riveros  
 Director  
 Planificación y Proyectos

 Dirección Nacional de <b>CORREOS</b> del <b>PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b> Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 4 de 16

## PRINCIPIOS

Preservar la Confidencialidad, Integridad y Disponibilidad de la información de la entidad y de las partes interesadas que sea objeto de tratamiento, tanto en la red interna como en el ciberespacio.

## OBJETIVOS

Los objetivos de la presente política están orientados a salvaguardar los activos (información) en el entorno físico, de red local y los que se encuentran interconectados a través de internet.

- Asegurar la Confidencialidad, Integridad y Disponibilidad de los activos (información) a través de la ejecución de políticas, gestión de riesgos.
- Definir e implementar controles informáticos robustos para mitigar ataques cibernéticos conocidos, a los que se encuentran expuestas las aplicaciones y plataformas IT de la entidad..
- Planear y ejecutar un programa de auditoría (auditor informático interno) a fin de verificar la adecuada implementación de los controles de seguridad y ciberseguridad en las plataformas IT.
- Gestionar el riesgo a través del análisis de vulnerabilidades.

## RESPONSABILIDADES

Las responsabilidades en la entidad, frente a la seguridad de la información y la ciberseguridad se encuentran jerárquicamente establecidas de la siguiente manera:

- La Alta Dirección, revisa y aprueba de forma periódica la eficacia, eficiencia y aplicabilidad de la política de acuerdo con la dinámica de la Institución.
- Seguridad de TIC conjuntamente con el Área de Seguridad de la Información, diseña y gestiona la política de ciberseguridad y las políticas relacionadas.




CERTIFICO QUE LA PRESENTE FOTOCOPIA ES EL REFLEJO DEL ORIGINAL QUE TENGO A LA VISTA.

Lic. Fernando Riveros  
 Director  
 Planificación y Proyectos



Lic. Fernando Riveros  
 Director  
 Planificación y Proyectos

Survin

 Dirección Nacional de <b>CORREOS</b> del <b>PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b>  Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 5 de 16

- Seguridad de TIC conjuntamente con el Área de Seguridad de la Información, revisa y evalúa la aplicación de procedimientos de seguridad de la información y controles de ciberseguridad para asegurar la adecuada ejecución de las políticas relacionadas.
- La ciberseguridad es responsabilidad de todos y cada uno de los agentes involucrados en el ciberespacio de la Entidad.

## RESOLUCIONES RELACIONADAS

La Política de Ciberseguridad se encuentra sustentada mediante resoluciones emanadas por el MITIC, que tienen como propósito reglamentar el cumplimiento de la política de la ciberseguridad y un análisis de información de consultas a varios textos de la ciberseguridad.

- RESOLUCIÓN MITIC N° 346-2020 – Reporte Obligatorio de Incidentes
- RESOLUCIÓN MITIC N° 277-2020 – Guía de Controles Críticos de Ciberseguridad
- RESOLUCIÓN MITIC N° 733-2019 – Modelo de Gobernanza
- RESOLUCIÓN MITIC N° 699-2019 – Criterios de seguridad de software
- RESOLUCIÓN MITIC N° 218-2020 – Lineamientos del Portal Unico de Gobierno y Tramites en Línea




CERTIFICO QUE LA PRESENTE FOTOCOPIA ES DEL REFLEJO DEL ORIGINAL QUE TENGO A LA VISTA.



Fernando Riveros  
Director  
Planificación y Proyectos



 Dirección Nacional de <b>CORREOS</b> del <b>PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b>  Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 6 de 16

## DIMENSIONES DE LA SEGURIDAD.

A fin de poder determinar el impacto que tendría en la Entidad un incidente que afectara a la seguridad de la información de los activos de información, y de poder establecer el nivel de criticidad, se tendrán en cuenta las siguientes dimensiones de la seguridad:

- a) Disponibilidad
- b) Integridad
- c) Confidencialidad.

## CRITERIOS PARA DEFINICIÓN DE NIVELES DE CRITICIDAD DE UN INCIDENTE CIBERNÉTICO.

De manera a establecer el nivel de criticidad de un determinado incidente cibernético de seguridad, cada dimensión de seguridad afectada se adscribirá a uno de los niveles descriptos; bajo, medio o alto:

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Si ninguna dimensión de seguridad se ve afectada, no se adscribirá a ningún nivel.

- **Nivel alto:** Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad y supongan un perjuicio muy grave o total para los objetivos misionales de la entidad, sus activos críticos o los individuos afectados. Se entenderá por perjuicio muy grave o total:


1. La anulación de la capacidad de la Entidad para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
- 2- El daño muy grave, e incluso irreparable, de los activos de la organización, sean estos: financieros, de información, de imagen o de otra naturaleza.

COPIA QUE LA PRESENTE  
DINACOPA ES DEL REFLEJO  
DEL ORIGINAL QUE TENGO A  
LA VISTA



Lic. Fernando Riveros  
Director  
Planificación y Proyectos



 Dirección Nacional de <b>CORREOS del PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b> Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 7 de 16


- 3- El incumplimiento de alguna ley o regulación.
  - 4- Causar un perjuicio grave a individuos de difícil o imposible reparación.
  - 5- Otros de naturaleza análoga.
- **Nivel medio:** Se utilizará cuando las consecuencias de un incidente cibernético de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio parcial sobre las funciones de la Entidad, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio parcial:
1. La reducción parcial de la capacidad de la Entidad para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.
  - 2- El daño parcial de los activos de la Entidad, así sean estos financieros, de información, de imagen u otra naturaleza.
  - 3- Causar un perjuicio moderado a algún individuo.
  - 4- Otros de naturaleza análoga.
- **Nivel bajo:** Se utilizará cuando las consecuencias de un incidente cibernético de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio mínimo o incluso nulo sobre las funciones de la Entidad, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio mínimo:
- 1- Sin reducción de la capacidad de la Entidad para atender eficazmente
  - 2- Sin daño o con daño mínimo de activos de la Entidad, así sean estos financieros, de información, de imagen u otra naturaleza.
  - 3- Sin perjuicio a individuos.
  - 4- Otros de naturaleza análoga.



COPIA ES FIEL REFLEJO ORIGINAL QUE TENGO

Fernando Riveros  
 Director  
 Planificación y Proyectos



 Dirección Nacional de <b>CORREOS</b> del <b>PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b> Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 8 de 16

## GESTIÓN DE ACTIVOS

Se deberá realizar la clasificación de los activos en función del tipo de información que se encomienda para su tratamiento, de acuerdo con lo dispuesto en la política de seguridad de la información.

Las informaciones son guardadas en un servidor clasificadas por Dirección, Departamento, nombre del equipo, para su mejor y rápida identificación. Las copias de seguridad son realizadas en las dependencias que las soliciten y en las que se considera de suma importancia los datos y amerita el respaldo periódico.

Se deberá asignar un responsable encargado de realizar la gestión propia de los activos (información) durante todo el ciclo de vida. El responsable deberá mantener un registro formal de los usuarios con acceso autorizado y preservando la confidencialidad del mismo (no transferible) dicho activo.

Además, para cada activo o elemento de información deberá existir un responsable o propietario, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado, correctamente clasificado y adecuadamente protegido según lo dispuesto en la política de seguridad de la información.

## CICLO DE VIDA DE LA INFORMACIÓN

La entidad deberá gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos, recurrir a la política de seguridad de la información.

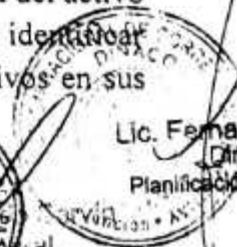
## PREVENCIÓN DE FUGA DE LA INFORMACIÓN

Se deberán analizar los vectores de fuga de información, en función de las condiciones y operativa de trabajo. Para ello, se deberán identificar los activos cuya fuga supone mayor riesgo, basándose en la criticidad del activo y el nivel de clasificación de la información. Además, se deberán identificar las posibles vías de robo, pérdida o fuga de cada uno de los activos en sus diferentes estados del ciclo de vida.




CERTIFICO QUE LA PRESENTE  
 COPIA OCUPA EL MISMO RELEVANCIA  
 DEL ORIGINAL QUE TENGO A  
 VISTA

Lic. Fernando Riveros  
 Director  
 Planificación y Proyectos



Lic. Fernando Riveros  
 Director  
 Planificación y Proyectos

 Dirección Nacional de <b>CORREOS del PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b> Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 9 de 16

## BUENAS PRÁCTICAS CONTRA LA FUGA DE LA INFORMACIÓN.

Se deberá asegurar la formación y capacitación de todos los servidores públicos de la entidad, en torno a buenas prácticas para la prevención de fugas de información. Especialmente se deberán tener en cuenta, al menos, los siguientes aspectos:

- Uso adecuado de dispositivos extraíbles como USBs, CD/DVDs o similares.
- Uso del correo electrónico Institucional diariamente.
- Poner especial atención en el tratamiento del correo electrónico, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc.
- No abrir mensajes de correo de remitentes desconocidos, desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial.
- Transmisión de información de forma oral (suma discreción).
- Impresión de documentación solo lo necesario.
- Salida de documentación.
- Uso de dispositivos móviles
- Uso de Internet
- Se deberá crear grupos de trabajos en el correo Institucional, con el fin de que la información y/o requerimiento llegue a todos los funcionarios dentro de sus respectivas áreas (Incluir el correo institucional de los funcionarios de la respectiva área y el correo institucional del Dpto., Dirección, Auditoría, Coordinación)




CERTIFICO QUE LA PRESENTE FOTOCOPIA ES FIEL REFLEJO ORIGINAL QUE TENGO A LA VISTA



Fernando Riveros  
 Director  
 Planificación y Proyectos



Fernando Riveros  
 Director  
 Planificación y Proyectos

 Dirección Nacional de <b>CORREOS</b> del <b>PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b> Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 10 de 16

## GESTIÓN DE LA COPIA DE SEGURIDAD

- **A NIVEL USUARIO:**

Ante la necesidad de realizar copias de seguridad por reinstalación de los equipos, se deberán ubicar en lugares seguros con acceso restringido (Carpeta con acceso restringido en el servidor solo personal de TIC).

Se establece un período de retención de las copias de seguridad siendo esta de veinte 20 días, periodo por el cual se deberá verificar si falta algún archivo para realizar la reinstalación del mismo.) posteriormente se procede a su destrucción.

- **A NIVEL SERVIDOR:**

Se deberán realizar copias de seguridad de la información, del software y del sistema y se deberán verificar de forma trimestral. Para ello, se deberán realizar copias de seguridad de aplicaciones, ficheros y bases de datos con una periodicidad, al menos, de forma mensual, salvo que en dicho periodo no se hubiese producido ninguna actualización. En su caso, se podrá establecer una frecuencia más alta de realización de copias de seguridad, si la información a salvaguardar es de alto impacto.

Las copias de seguridad deberán recibir las mismas protecciones de seguridad que los datos originales, asegurándose su correcta conservación, así como los controles de acceso adecuados, se deberán ubicar en lugares seguros con acceso restringido (Carpeta con acceso restringido en el servidor solo personal de TIC).

Se establece un período de retención de las copias de seguridad siendo esta de seis (6) meses, posteriormente se procede a su destrucción.

## CONTROL DE ACCESO

Todos los sistemas de información de la DINACOPA deberán contar con un sistema de control de acceso a los mismos. Asimismo, el control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas.




CERTIFICO QUE LA PRESENTE  
FOTOCOPIA ES FIEL REFLEJO  
DEL ORIGINAL QUE TENGO A  
VISTA

Lic. Fernando Riveros  
Director  
Planificación y Proyectos



Lic. Fernando Riveros  
Director  
Planificación y Proyectos

 Dirección Nacional de <b>CORREOS</b> del <b>PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b>  Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 11 de 16

## REQUISITOS PARA EL CONTROL DE ACCESO

Los encargados de brindar accesos a sistemas deberán asumir una serie de requisitos, que serán al menos las siguientes:

- Los usuarios deberán ser únicos y no podrán ser compartidos. Asimismo, los privilegios de los usuarios serán inicialmente asignados mediante el principio de mínimo privilegio.
- Se prohibirá el uso de usuarios genéricos. En su defecto, se utilizarán cuentas de usuario asociadas a la identidad nominal de la persona asociada.

### NIVEL DE ACCESO

El encargado de TIC deberá implementar controles de acceso que garanticen que a los usuarios sólo se les otorguen privilegios y derechos necesarios para desempeñar su función.

Los niveles de acceso deberán ser establecidos en función de:

- Control de acceso basado en roles: deberán establecerse perfiles o roles de acceso por aplicación y/o sistemas para poder asignar los mismos a los diferentes usuarios.
- Necesidad de saber: Sólo se permitirá el acceso a un recurso cuando exista necesidad verificada y verificable para el desarrollo de la actividad.
- Privilegios mínimos: los permisos otorgados a los usuarios deberán ser los mínimos.
- Apartar funciones: deberá asegurarse un correcto apartado de funciones para desarrollar y asignar derechos de acceso.

Asimismo, ningún usuario podrá acceder por sí mismo a un sistema de información controlado sin la debida autorización del responsable del propio usuario (Director de área o Jefe inmediato).



CERTIFICO QUE LA PRESENTE  
COPIA ES FIEL REFLEJO  
DE LO QUE EN TENGO

Fernando Riveros  
Director  
Planificación y Proyectos



W. Fernando Riveros  
Director  
Planificación y Proyectos

W. Fernando Riveros  
Director  
Planificación y Proyectos



Dirección Nacional  
de **CORREOS**  
del **PARAGUAY**

## POLÍTICA DE CIBERSEGURIDAD

Dirección Nacional de  
Correos del Paraguay  
Dinacopa

Código: PCS-DT-2022

Versión: 01

Aprobado por  
Resolución:

Fecha de  
Aprobación:

Página: 12 de 16

En caso de acceso a sistemas externos a la Dinacopa, en la cual no es potestad del encargado de TIC la designación de roles que fueran utilizados por Direcciones, Asesorías, Auditoría, Coordinaciones con rango Directivo, se realizará el acta de confidencialidad, en el cual se mencionara el compromiso de los usuarios y la responsabilidad del mismo con sus contraseñas, la finalidad del usuario que tiene acceso al sistema, quedando en resguardo del Área de Seguridad de la Información

### SEGURIDAD EN EL ÁMBITO DE DESARROLLO DE SISTEMAS

Toda la adquisición, desarrollo y mantenimiento de los sistemas deberá contar con unos requisitos mínimos de seguridad necesarios para el desarrollo de software, los sistemas y los datos acorde con las buenas prácticas del sector. Además, deberá realizarse una gestión de pruebas, seguimiento de los cambios y el inventario del software.

### SEGURIDAD EN LOS PROVEEDORES

Se deberá poner especial atención en evaluar la criticidad de todos los servicios susceptibles de ser subcontratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad del contrato de prestación de servicios


Sobre los proveedores de estos servicios se deberán cuidar los procesos de selección, requerimientos contractuales como la terminación contractual, la monitorización de los niveles de servicio, la devolución de datos y las medidas de seguridad implantadas por dicho proveedor, que deberán ser, al menos, equivalentes a las que se establecen en la presente política.

CERTIFICO QUE LA PRESENTE  
FOTOCOPIA ES FIEL REFLEJO  
DEL ORIGINAL QUE TENGO A  
SU DISPOSICIÓN EN ESTA



Lic. Fernando Riveros  
- Director  
Planificación y Proyectos

Lic. Fernando Riveros  
Director  
Planificación y Proyectos

 Dirección Nacional de <b>CORREOS</b> del <b>PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b>  Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 13 de 16

## REVISIÓN DE LA POLÍTICA

La aprobación de esta Política implica que su implantación contará con el apoyo de la Máxima Autoridad Institucional a fin de lograr todos los objetivos establecidos en la misma, como también cumplir con todos sus requisitos.

La presente Política de ciberseguridad, será revisada y aprobada anualmente. No obstante, si tuvieran lugar cambios relevantes en la sociedad o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así, que la Política permanezca adaptada y adecuada en todo momento a la realidad institucional.



CERTIFICO QUE LA PRESENTE  
FOTOCOPIA ES FIEL REFLEJO  
DEL ORIGINAL QUE TENGO A  
LA VISTA



Abg. Lito Fernando Servino  
Director General  
DINACOPA




Lic. Fernando Riveros  
Director  
Planificación y Proyectos



Lic. Fernando Riveros  
Director  
Planificación y Proyectos



 Dirección Nacional de <b>CORREOS</b> del <b>PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b>  Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 14 de 16

## GLOSARIO

**Ciberseguridad:** conjunto de procedimientos y herramientas que se implementan con el fin de proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

**Ciberespacio:** espacio artificial creado por el conjunto de Sistemas de Información y Telecomunicaciones que utilizan las TIC, es decir por un conjunto de redes de ordenadores y de telecomunicaciones interconectados directa o indirectamente a nivel mundial, donde las personas puedan comunicarse e interactuar por medio de softwares, plataformas u otros servicios de información.

**Activos de información:** recursos utilizados por un sistema de seguridad de la información para que la Institución funcione y consiga sus objetivos. Los mismos incluyen, pero no se limitan a: los archivos de la Entidad, ya sea en formato electrónico o no; los sistemas, cuentas, equipos y redes en los que se almacenan, procesan y/o transmite la información institucional, así como también el conocimiento específico acerca de estos activos

**Disponibilidad:** se refiere al acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran

**Integridad:** se refiere a la exactitud y fiabilidad de los datos (información), estos deben estar completos, sin variaciones.

**Confidencialidad:** se refiere al acceso a la información por parte únicamente de quienes estén autorizados.

**Incidente Cibernético de Seguridad ("Incidente"):** es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad).




FOTOCOPIA ES FIEL REFLEJO  
DEL ORIGINAL QUE TENGO A  
SU CARGA

Lic. Fernando Rivas  
Director  
Planificación y Proyectos



Lic. Fernando Rivas  
Director  
Planificación y Proyectos

 Dirección Nacional de <b>CORREOS del PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b> Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 15 de 16

**Usuario:** persona que utiliza una computadora o un servicio de red.

**Software:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

**Servidor:** conjunto de computadoras capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

**Sistema Informático:** Es el conjunto constituido por los elementos físicos y lógicos (software) necesarios para captar información, almacenarla y procesarla -realizar operaciones con ella.

**Fuga de Información:** Es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.

**Vulnerabilidad:** Debilidad o falta de un control o medida.

**Actor malicioso:** entidad parcial o totalmente responsable de un incidente, que afecta o tiene el potencial de afectar la seguridad de una organización.

**Amenaza:** Peligro que un agente amenaza pueda explotar una vulnerabilidad.

**Riesgo:** Probabilidad de que un agente amenaza explote una vulnerabilidad y el impacto asociado con el negocio.

**Control o medida:** Control que se pone en marcha para reducir el riesgo, también llamado contramedida.

**Exposición:** Presencia de una vulnerabilidad que expone a la entidad a una amenaza.


**TIC:** Tecnología de la Información y Comunicación, conjunto de equipos, cables y medios técnicos que transportan los servicios de comunicaciones desde los puntos de interconexión de los diferentes servicios.



FOTOCOPIA ES FIEL REFLEJO DEL ORIGINAL QUE TENGO A MI DISPOSICIÓN

Lic. Fernando Rivero  
 Director  
 Planificación y Proyectos



 Dirección Nacional de <b>CORREOS del PARAGUAY</b>	<b>POLÍTICA DE CIBERSEGURIDAD</b> Dirección Nacional de Correos del Paraguay Dinacopa	Código: PCS-DT-2022	
		Versión: 01	Aprobado por Resolución:
		Fecha de Aprobación:	Página: 16 de 16

**IOT (Internet of Things):** Internet de las Cosas, red colectiva de dispositivos conectados y a la tecnología que facilita la comunicación entre los dispositivos y la nube, así como entre los propios dispositivos.

**Delitos informáticos:** son todas las acciones dirigidas a lesionar la integridad, disposición y confiabilidad de datos y de sistemas informáticos, así como aquellas conductas que atentan contra el patrimonio de las personas físicas o jurídicas, utilizando herramientas tecnológicas e informáticas.

**Explotación de Vulnerabilidades:** conocido como exploit, es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware para hacerse con el control de los ordenadores o robar datos de red.

**Malware:** palabra inglesa y significa software malicioso

**Ransomware:** es un tipo de malware que impide el acceso a ficheros, cifrando o encriptando todos los archivos tanto del equipo como del sistema, bloqueando su acceso.

CERTIFICO QUE LA PRESENTE FOTOCOPIA ES FIEL REFLEJO DEL ORIGINAL QUE TENGO A LA VISTA.






**Fernando Riveros**  
 Director  
 Planificación y Proyectos



**Lic. Fernando Riveros**  
 Director  
 Planificación y Proyectos