



INSTITUTO NACIONAL PENITENCIARIO

COMITÉ DE CONTROL INTERNO INSTITUCIONAL (COCOIN)

POLITICA DE TECNOLOGÍA

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 2 de 29

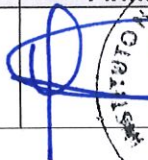
Elaboración del Documento

Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Ing. Ana Raquel Ruiz Triminio	Desarrollador de Sistemas	Departamento de Infotecnología	Noviembre 2024	

Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Msc. Nayla Johanna Díaz	Oficial Jurídico	SDDI	Noviembre 2024	

Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Ing. Moisés Rodríguez	Coordinador del Departamento de Infotecnología	Departamento de Infotecnología	Noviembre 2024	 

Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
Coronel de Infantería D.E.M. Ramiro Fernando Muñoz	Director Nacional	Instituto Nacional Penitenciario	Noviembre 2024	 

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 3 de 29

CONTENIDO

1. ANTECEDENTES	4
2. DECLARACION POLITICA DE TECNOLOGIA	7
3. MARCO LEGAL Y NORMATIVO	9
4. MARCO REFERENCIAL Y CONCEPTUAL.....	11
5. OBJETIVOS	14
6. ALCANCE	15
7.DIRECTRICES	16
8. LINEAMIENTOS PARA LA EJECUCIÓN DE LOS PLANES Y SUS RESULTADOS DE LA UNIDAD DE INFOTECNOLOGIA	21
9. RESPONSABILIDADES Y FUNCIONES.....	22
10. DIVULGACION.....	25
11. ACTUALIZACION	26
12. GLOSARIO.....	28

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 4 de 29

1. ANTECEDENTES

Los antecedentes para la creación de una política institucional de tecnología en el Instituto Nacional Penitenciario de Honduras (INP) se han visto impulsados, en gran medida, por la situación de emergencia en la que se encuentran los centros penitenciarios. Esta situación ha puesto de manifiesto la necesidad de fortalecer los mecanismos tecnológicos en varias áreas. Aquí se detallan algunos antecedentes específicos que justifican y motivan la creación de esta política:

1. Incremento de amenazas de seguridad interna y externa

La crisis de seguridad dentro de los centros penitenciarios ha resaltado la importancia de implementar controles tecnológicos robustos para prevenir incidentes, como fugas de información y ataques cibernéticos que comprometan la seguridad interna y externa. La necesidad de reforzar las tecnologías de vigilancia, monitoreo de comunicaciones y control de acceso se ha vuelto crucial para mantener el orden y garantizar la seguridad en los centros.

2. Deficiencias en infraestructura tecnológica y ciberseguridad

La infraestructura tecnológica del INP ha mostrado limitaciones para responder efectivamente a las demandas de un sistema penitenciario en emergencia. La falta de sistemas centralizados y de soluciones de ciberseguridad ha dificultado el control eficiente de las operaciones. Esto ha creado la urgencia de contar con una infraestructura tecnológica adecuada que permita una mejor gestión de la información y la protección de datos sensibles.

3. Necesidad de mejorar la gestión de la información y la trazabilidad

La emergencia ha expuesto carencias en los sistemas de administración de información en el INP. La falta de trazabilidad en las actividades de internos, personal y visitas, así como el registro de incidentes y eventos, ha complicado el seguimiento de operaciones y la toma de decisiones informadas. Una política de

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 5 de 29

tecnología busca, en este sentido, unificar y centralizar los sistemas de gestión de la información.

4. Adaptación a los cambios y normativas de seguridad

En respuesta a la emergencia, el gobierno hondureño ha implementado nuevas normativas y protocolos de seguridad para el sistema penitenciario

2. Componentes de la MARCI aplicados a la política de tecnología

Los componentes de la MARCI, adaptados a la creación de esta política, incluyen:

Ambiente de control: Define la estructura, roles y responsabilidades de quienes gestionarán los activos tecnológicos. Asegura que todos comprendan su rol en la protección y uso ético de los recursos tecnológicos.

Evaluación de riesgos: Identifica y evalúa riesgos tecnológicos, como amenazas cibernéticas, accesos no autorizados, o fallos en la infraestructura que puedan comprometer la seguridad y operatividad del INP.

Actividades de control: Implementación de controles específicos, tales como el acceso restringido a sistemas críticos, actualizaciones de seguridad periódicas, y uso de firewalls y antivirus en la infraestructura.

Información y comunicación: Asegura que haya canales de comunicación claros y efectivos para reportar incidentes tecnológicos y que el personal esté informado sobre políticas y prácticas seguras de uso de tecnología.

Monitoreo de actividades de control: Establece un mecanismo para revisar regularmente la efectividad de los controles implementados. Esto incluye auditorías, revisión de registros de actividad, y mejoras continuas en los sistemas tecnológicos.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 6 de 29

3. Principios de control interno en la política de tecnología

Los principios de control interno del INP, aplicados en esta política, son:

Integridad y ética: Los usuarios de la tecnología deben comprometerse con el uso ético y seguro de la infraestructura.

Responsabilidad: Cada área y usuario tendrá responsabilidades específicas en el uso de los sistemas y la protección de la información.

Transparencia: Todos los procesos tecnológicos deben estar documentados, y se deben establecer mecanismos de auditoría para asegurar la transparencia en su uso.

Seguridad: La protección de la información debe ser una prioridad, estableciendo políticas de seguridad cibernética y física en toda la infraestructura tecnológica.

4. Normas de control interno para la política de tecnología

Las normas de control interno en el desarrollo de esta política abarcan:

Norma de acceso y autorización: Define quiénes pueden acceder a diferentes sistemas y establece procedimientos de autorización para cada nivel de acceso.

Norma de seguridad de la información: Cubre la encriptación, respaldo y manejo seguro de datos, asegurando que se proteja la confidencialidad y disponibilidad de la información.

Norma de continuidad operativa: Incluye un plan de recuperación ante desastres y continuidad del negocio para la infraestructura tecnológica.

Norma de auditoría tecnológica: Especifica la periodicidad y alcance de las auditorías de sistemas, incluyendo la revisión de logs y análisis de vulnerabilidades.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 7 de 29

Implementación de la Política

Capacitación del personal: La política de tecnología debe ser acompañada de un programa de formación para asegurar que todos los usuarios comprendan su rol y responsabilidad en el uso seguro de los recursos tecnológicos.

Monitoreo y actualización continua: Realizar evaluaciones periódicas para ajustar la política de acuerdo con los cambios tecnológicos y las nuevas amenazas cibernéticas.

2. DECLARACION POLITICA DE TECNOLOGIA

La Política Institucional de Tecnología del Instituto Nacional Penitenciario de Honduras (INP) establece los lineamientos fundamentales para la adquisición, gestión, uso y protección de los recursos tecnológicos, con el fin de fortalecer la seguridad, eficiencia y transparencia en la administración penitenciaria. Esta política está orientada a garantizar que la infraestructura tecnológica del INP sea un soporte efectivo para el cumplimiento de sus objetivos de seguridad, orden y rehabilitación, promoviendo la interoperabilidad, integridad y confidencialidad de la información, y protegiendo los derechos y datos de todas las personas involucradas en el sistema penitenciario.

Objetivos de la Política de Tecnología:

- 1. Seguridad y control:** Asegurar la implementación de tecnologías avanzadas para proteger la seguridad interna y externa de los centros penitenciarios, mejorando el monitoreo y el control de acceso.
- 2. Gestión y trazabilidad de la información:** Optimizar la gestión y centralización de la información para garantizar la trazabilidad en las operaciones y la toma de decisiones informadas, en cumplimiento con las normativas de seguridad.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 8 de 29

3. Continuidad operativa: Establecer mecanismos y planes de continuidad de servicios tecnológicos, para garantizar la operatividad y resiliencia del INP incluso en situaciones de crisis o emergencia.

4. Interoperabilidad con instituciones de seguridad: Facilitar la integración tecnológica con otras instituciones de seguridad pública para una mejor coordinación y respuesta ante situaciones de riesgo.

5. Transparencia y rendición de cuentas: Proveer herramientas y procesos tecnológicos que aseguren la transparencia y permitan auditorías periódicas, contribuyendo a la rendición de cuentas en todas las operaciones relacionadas con la tecnología.

Principios Rectores:

Integridad y ética en el uso de la tecnología: Cada miembro del INP es responsable de usar los recursos tecnológicos de manera ética y en beneficio de la seguridad penitenciaria.

Protección de la información: Se implementarán mecanismos rigurosos de ciberseguridad y gestión de datos para asegurar la confidencialidad, integridad y disponibilidad de la información sensible.

Innovación y mejora continua: La tecnología debe ser actualizada y evaluada periódicamente para adaptarse a los cambios en el entorno de seguridad y para mejorar continuamente los servicios y procesos penitenciarios.

La Institución utilizara en forma intensiva y generalizada, la tecnología más avanzada, auspiciara la investigación y el desarrollo de nuevos sistemas, técnicas y procedimientos de trabajo, para cumplir con eficiencia y seguridad sus actividades al servicio de la ciudadanía, de los organismos públicos y privados, y de los usuarios internos.

	INSTITUTO NACIONAL PENITENCIARIO	
	POLÍTICA DE TECNOLOGÍA	I.N.P.
Versión "1.0"	Fecha: XX de Mes 20XX	9 de 29

3. MARCO LEGAL Y NORMATIVO

La política institucional de tecnología del Instituto Nacional Penitenciario de Honduras (INP) se fundamenta en un marco legal y normativo que asegura su alineación con las leyes nacionales, normativas de seguridad y estándares internacionales en el uso de la tecnología en entornos de seguridad pública. Este marco orienta el uso, protección y gestión de los recursos tecnológicos en el INP, garantizando su conformidad con los principios de legalidad, integridad, seguridad y transparencia.

1. Constitución de la República de Honduras

La Constitución establece la protección de los derechos fundamentales, como el derecho a la privacidad y la protección de datos personales, los cuales se deben respetar en todas las operaciones tecnológicas del INP.

2. Ley del Instituto Nacional Penitenciario (Decreto Legislativo No. 64-2012)

Esta ley establece el marco general de funcionamiento del INP, definiendo sus responsabilidades en la administración penitenciaria, incluidas la seguridad y el orden en los centros penitenciarios. La ley faculta al INP a implementar sistemas de control, supervisión y monitoreo, dentro de los límites de la legalidad.

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 10 de 29

3. Ley de Transparencia y Acceso a la Información Pública (Decreto No. 170-2006)

La ley regula el acceso a la información pública y establece las obligaciones del INP de asegurar la transparencia en sus operaciones, garantizando la confidencialidad de información sensible en el ámbito penitenciario.

4. Ley de Protección de Datos Personales (Decreto No. 25-2021)

Esta ley establece la regulación del tratamiento y protección de datos personales en Honduras, incluyendo obligaciones para la recolección, almacenamiento y uso de la información. El INP debe asegurar el cumplimiento de esta normativa en la gestión de datos de internos, personal y otras personas que interactúan con la institución.

5. Ley Especial de Ciberseguridad (Propuesta de Ley)

Aunque en proceso de aprobación, esta ley establece principios y normas para proteger la infraestructura cibernética nacional, lo cual incluye las plataformas tecnológicas del INP. Esta ley será relevante para fortalecer las medidas de ciberseguridad y proteger los sistemas contra amenazas externas e internas.

6. Reglamento de Seguridad de la Información

Establece lineamientos específicos para la implementación de medidas de seguridad en el tratamiento de la información y la tecnología utilizada en el INP, basándose en normativas internacionales de gestión de la seguridad de la información, como la **ISO/IEC 27001**.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 11 de 29

7. Políticas Institucionales del INP

La política de tecnología se alinea con las políticas internas del INP, como la política de talento humano y de compras y contrataciones, asegurando la competencia del personal y la adquisición adecuada de tecnologías y servicios, conforme a los principios de transparencia, eficacia y control interno.

8. Normativas Internacionales y Mejores Prácticas

ISO/IEC 27001: La norma internacional para la gestión de la seguridad de la información, utilizada para establecer un sistema de control de seguridad de la información en el INP.

NIST (National Institute of Standards and Technology): Normas y pautas para la gestión de la ciberseguridad, utilizadas como referencia para proteger la infraestructura tecnológica y los datos sensibles del INP.

Convenios Internacionales en Derechos Humanos y Tratamiento de Personas Privadas de Libertad: Como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos, que establecen estándares de respeto a los derechos de los internos, incluidos los relacionados con su privacidad y el uso de tecnología en centros de detención.

4. MARCO REFERENCIAL Y CONCEPTUAL

El marco referencial de la Política Institucional de Tecnología del Instituto Nacional Penitenciario de Honduras (INP) se sustenta en un conjunto de principios, normas y marcos legales nacionales e internacionales que orientan la gestión tecnológica, la ciberseguridad y la administración de riesgos. Estos elementos proporcionan el

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 12 de 29

contexto necesario para la formulación de una política robusta y alineada con los objetivos de seguridad y eficiencia del sistema penitenciario.

Normativa Nacional de Seguridad y Protección de Datos: Cumple con la legislación hondureña en materia de protección de datos y ciberseguridad, incluyendo leyes y reglamentos que protegen la confidencialidad y seguridad de la información en el sector público.

Estándares Internacionales de Gestión Tecnológica y Seguridad: Esta política está alineada con los estándares internacionales como la **ISO/IEC 27001** (sistemas de gestión de seguridad de la información) e **ISO 22301** (continuidad de negocio). Además, adopta buenas prácticas en ciberseguridad establecidas por el **NIST** (National Institute of Standards and Technology) y el **CIS** (Center for Internet Security)

Metodología de Administración de Riesgos y Control Interno (MARCI): La política de tecnología del INP adopta los principios y componentes de la MARCI para asegurar la integridad de sus procesos de control interno, fortaleciendo el ambiente de control, la evaluación de riesgos, y el monitoreo y seguimiento de actividades tecnológicas.

Política de Estado para el Sistema Penitenciario: La política se enmarca en los lineamientos generales del gobierno hondureño para el sistema penitenciario, priorizando la modernización tecnológica, la seguridad de los centros penitenciarios y el apoyo a la rehabilitación y reintegración de los privados de libertad.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 13 de 29

2. Marco Conceptual:

Para estructurar la Política Institucional de Tecnología, se define un marco conceptual que establece los términos clave y principios en los que se basa el uso de la tecnología dentro del INP.

Seguridad de la Información: Se refiere a las prácticas y sistemas implementados para proteger la confidencialidad, integridad y disponibilidad de los datos generados y gestionados por el INP. Esto incluye el uso de controles de acceso, encriptación y protocolos de seguridad.

Continuidad del Negocio: Conjunto de estrategias y planes que aseguran que las operaciones tecnológicas del INP puedan mantenerse o restaurarse rápidamente en caso de una interrupción, como parte del compromiso con la resiliencia y la respuesta ante emergencias.

Gestión de Riesgos Tecnológicos: Proceso de identificación, análisis y mitigación de riesgos asociados a la infraestructura tecnológica, que garantiza la minimización de amenazas y vulnerabilidades que puedan afectar la seguridad y operatividad del INP.

Interoperabilidad: Capacidad de los sistemas tecnológicos del INP para integrarse y trabajar en conjunto con las plataformas de otras instituciones de seguridad, permitiendo la colaboración y el intercambio de información en tiempo real.

Transparencia y Rendición de Cuentas: Implica que los sistemas tecnológicos se implementan de manera que permitan auditorías y revisiones, asegurando que las operaciones del INP sean verificables y los recursos se utilicen de forma ética y eficaz.

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 14 de 29

Ciberseguridad: Estrategias y acciones específicas para proteger la infraestructura tecnológica del INP frente a amenazas cibernéticas. Incluye medidas preventivas, detectivas y correctivas para mitigar riesgos de accesos no autorizados, ataques de malware y otros incidentes de seguridad.

Innovación Tecnológica: Fomento de la adopción de nuevas tecnologías y prácticas de vanguardia para mejorar la eficiencia operativa del INP, y adaptar la infraestructura a los cambios tecnológicos y normativos que impactan la administración penitenciaria.

Protección y Confidencialidad de la Información: Priorizar la seguridad de la información para garantizar la privacidad de los datos de internos, personal y todas las partes involucradas.

Actualización y Mejora Continua: Mantener los sistemas tecnológicos actualizados, implementando mejoras conforme a los avances tecnológicos y las lecciones aprendidas en el uso de la infraestructura.

5. OBJETIVOS

Objetivo General:

Fortalecer la gestión penitenciaria mediante la integración y utilización de tecnologías avanzadas que optimicen los procesos internos, mejoren la seguridad en los centros penitenciarios y faciliten la rehabilitación y reinserción de los privados de libertad, en alineación con los principios de transparencia, eficiencia y protección de datos del Instituto Nacional Penitenciario (INP) de Honduras.

Objetivos Específicos:

1. Mejorar la Eficiencia Operativa: Automatizar y agilizar los procesos administrativos y operativos en los centros penitenciarios, reduciendo la carga laboral y aumentando la efectividad en la gestión de recursos.

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 15 de 29

2. Fortalecer la Seguridad: Implementar sistemas tecnológicos de control y vigilancia que contribuyan a garantizar la seguridad de internos, personal y visitantes, mediante el monitoreo continuo y la restricción de accesos no autorizados.

3. Optimizar la Gestión de Información: Crear una plataforma centralizada y segura para la gestión y almacenamiento de datos de internos y del personal penitenciario, que cumpla con los estándares de confidencialidad y acceso controlado.

6. ALCANCE

La política institucional de tecnología del Instituto Nacional Penitenciario (INP) de Honduras tiene como objetivo optimizar los procesos internos, mejorar la seguridad y facilitar la rehabilitación de los privados de libertad a través de sistemas tecnológicos avanzados. Sus principales alcances incluyen:

1. Automatización de Procesos: Simplificar y acelerar procesos administrativos y operativos dentro de los centros penitenciarios, promoviendo la eficiencia en la gestión de información y recursos.

2. Seguridad y Vigilancia: Implementar sistemas de vigilancia y control de acceso, como cámaras de seguridad, sistemas de monitoreo en tiempo real y controles biométricos, para garantizar la seguridad tanto de internos como del personal.

3. Gestión de la Información: Centralizar y proteger los datos relacionados con los internos, el personal y las operaciones penitenciarias, asegurando su confidencialidad y accesibilidad en línea con las leyes de protección de datos.

nuevas herramientas y soluciones para mejorar la administración penitenciaria.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 16 de 29

7.DIRECTRICES

Para asegurar el cumplimiento de la presente política de tecnología, se debe de considerar los siguientes aspectos clave, en alineación con la Política Penitenciaria:

1. Mantenimiento de Sistemas y Hardware

- a) **Frecuencia de Mantenimiento Preventivo:** Los equipos tecnológicos deberán recibir mantenimiento preventivo cada 6 meses, con el fin de garantizar su óptimo funcionamiento y evitar fallos imprevistos. El personal encargado deberá documentar todas las actividades de mantenimiento y almacenarlas de manera organizada en los archivos tanto físicos como virtuales del departamento.
- b) **Actualización de Seguridad (Antivirus y Licencias de Software):** Las actualizaciones de seguridad, tales como los antivirus y las licencias de software, se deberán realizar anualmente, garantizando la protección continua de los sistemas informáticos. Se deberá documentar el proceso de actualización y la renovación de licencias, archivando la información de manera física y digital para su seguimiento y control.
- c) **Procedimientos de Diagnóstico y Resolución de Problemas (Soporte Técnico):** El personal técnico deberá realizar un seguimiento diario de los problemas y fallos reportados en los equipos y sistemas tecnológicos del Instituto, asegurando que se tomen las acciones correctivas de manera oportuna. Esta documentación deberá ser archivada tanto de forma física como virtual para mantener un registro detallado de cada incidencia y su resolución.

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 17 de 29

- d) **Política de Reemplazo de Hardware Obsoleto:** El diagnóstico del hardware obsoleto será realizado por el personal técnico, quien emitirá un dictamen para la eliminación o reemplazo de los equipos que no cumplan con los estándares de funcionamiento. El dictamen debe ser entregado al usuario, quien lo remitirá al Departamento de Bienes Nacionales para su reemplazo.

2. Respaldo y Recuperación de Datos

- a) **Respaldo de Datos Automatizado:** El respaldo de los datos institucionales será realizado de manera automática todos los últimos viernes de cada mes. Se debe asegurar que todos los datos relevantes sean respaldados correctamente en los servidores institucionales.
- b) **Recuperación de Datos:** La recuperación de datos se realizará únicamente en caso de pérdida o corrupción de la información. El personal técnico deberá documentar todo el proceso de recuperación y archivar la información generada en formatos físicos y digitales para garantizar la trazabilidad.

3. Seguridad de la Información

a) Contraseñas Seguras:

El Departamento de Tecnología establecerá requisitos estrictos para la creación y gestión de contraseñas seguras, incluyendo:

- a) **Longitud mínima** de la contraseña.
- b) **Complejidad de los caracteres** (incluyendo mayúsculas, minúsculas, números y caracteres especiales).
- c) **Frecuencia de cambio de contraseñas.**

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 18 de 29

- b) Gestión de Parches de Seguridad:** Se establecerá un proceso regular y oportuno para la gestión y aplicación de parches de seguridad, con el fin de mitigar las vulnerabilidades en todos los sistemas y aplicaciones del Instituto.

4. Gestión de Redes

- a) Monitoreo y Control de Red:** El monitoreo continuo de la red será realizado de forma diaria, utilizando herramientas especializadas (como Fortinet) para prevenir accesos no autorizados y garantizar la seguridad de las comunicaciones.

- b) Inventario de Activos de Red:** Se llevará un inventario actualizado de todos los activos de red (dispositivos, servidores, routers, switches, etc.) de manera diaria, para garantizar la trazabilidad y seguridad de la infraestructura de red.

- c) Registros de Actividad de Red:** Se generarán reportes diarios sobre la actividad de la red, para evaluar el tráfico y detectar posibles amenazas o problemas de conectividad.

5. Desarrollo de Software

- a) Desarrollo de Sistemas:** Cuando una unidad o departamento requiera la creación o modificación de un sistema, se debe seguir un proceso de desarrollo que asegure que la solución tecnológica satisface de manera efectiva las necesidades específicas de cada área, cumpliendo con los estándares de calidad y alineándose con los objetivos estratégicos del Instituto.
- b) Manuales de Usuario y Documentación Técnica:** Cada sistema desarrollado debe incluir un manual que contenga información detallada sobre el diseño del sistema.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 19 de 29

- c) **Mantenimiento de Sistemas Desarrollados:** El mantenimiento de los sistemas desarrollados para el Instituto será realizado cada 6 meses, para asegurar que continúan operando de manera eficiente y conforme a los requerimientos.

6. Solicitud de Información sobre Personas Privadas de Libertad

a) **Recepción de Solicitudes de Información:** Las solicitudes de información sobre personas privadas de libertad deberán ser enviadas formalmente mediante memo oficial al Departamento de Infotecnología, especificando la información requerida (perfil penitenciario, estatus legal, antecedentes, etc.).

b) **Elaboración del Perfil Penitenciario:** La información será obtenida de las bases de datos institucionales, garantizando la precisión y la actualización.

c) **Archivo y Registro de Solicitudes:** Todas las solicitudes y respuestas (memos y perfiles penitenciarios) serán archivadas de manera organizada en los sistemas del Departamento de Infotecnología, para mantener la trazabilidad y facilitar auditorías futuras.

7. Data Center

a) **Acceso al Data Center:** el acceso al Data Center será restringido únicamente a los técnicos encargados y al jefe de infraestructura informática, garantizando la seguridad física y lógica del centro de datos.

b) **Condiciones del Data Center:** el Data Center debe contar con una planta eléctrica que permita la operación continua durante cortes de energía y mantener una temperatura estable por debajo de los 18°C para garantizar la seguridad de los equipos.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 20 de 29

c) Evaluaciones de Riesgo en el Data Center: Se deberán realizar evaluaciones de riesgos cada 15 días utilizando el Fortinet, para garantizar que las condiciones de seguridad cibernética sean óptimas.

d) Auditorías y Revisiones del Data Center: se deberán realizar auditorías y revisiones mensuales del Data Center, para asegurar que todo el hardware y las condiciones de seguridad sean adecuadas.

8. Plan Operativo Anual (POA)

a) Elaboración del POA: El Departamento de infotecnología deberá formular el Plan Operativo Anual (POA) de acuerdo con las prioridades estratégicas y los proyectos tecnológicos a ejecutar durante el año. Este plan debe incluir todos los proyectos de infraestructura tecnológica, mantenimiento de sistemas y hardware, desarrollo de software, gestión de seguridad de la información, y administración de redes y bases de datos.

b) Entrega del POA a UPEG: Una vez elaborado, el POA deberá ser entregado a la Unidad de Planeamiento y Evaluación de la Gestión (UPEG) para su revisión y aprobación. El POA debe ser entregado a UPEG en la fecha que ellos lo solicitan, para asegurar la correcta integración con los planes nacionales y sectoriales de desarrollo.

c) Monitoreo y Reporte de Avances: El Departamento de Tecnología debe informar a UPEG de los avances trimestrales de los proyectos establecidos en el POA, con el fin de garantizar el seguimiento y la alineación con los objetivos institucionales.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 21 de 29

9. Plan Anual de Compras y Contrataciones (PACC)

a) Elaboración del PACC: El Plan Anual de Compras y Contrataciones (PACC) del Departamento de Infotecnología debe detallar todas las adquisiciones y contrataciones necesarias para la ejecución de los proyectos tecnológicos definidos en el POA. Esto incluye la compra de equipos de hardware, software, licencias, infraestructura de red, y servicios externos como consultorías y mantenimiento

b) Envío del PACC al Departamento de Adquisiciones para Aprobación: El PACC (Plan Anual de Compras y Contrataciones) debe ser entregado al Departamento de Adquisiciones para su revisión y aprobación, con el fin de asegurar que las adquisiciones y contrataciones necesarias estén alineadas con los objetivos estratégicos del POA y se ajusten a los recursos disponibles.

8. LINEAMIENTOS PARA LA EJECUCIÓN DE LOS PLANES Y SUS RESULTADOS DE LA UNIDAD DE INFOTECNOLOGIA

- 1. Elaboración de informes periódicos:** El Departamento de Infotecnología es responsable de la elaboración de informes periódicos (mensuales y trimestrales) dirigidos a la Subdirección de Desarrollo. Estos informes tienen como objetivo dar seguimiento y evaluar el cumplimiento de las funciones asignadas a cada uno de los miembros del departamento, asegurando que las actividades y objetivos establecidos se estén cumpliendo de acuerdo con los plazos y estándares establecidos.
- 2. Manuales de Usuario:** Una vez completado el proyecto, se debe realizar la documentación que contenga información detallada sobre el diseño del sistema. Asimismo, este manual de usuario debe de ser claro y accesible para los usuarios finales.
- 3. Asignación de Responsabilidades:** Se debe asignar un equipo responsable para cada proyecto, con roles y responsabilidades claramente

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 22 de 29

definidos, los encargados de cada proyecto deberán coordinar con las demás unidades de la institución para garantizar la alineación y la ejecución eficaz de los planes.

- 4. Evaluaciones de Riesgo:** Se deberán realizar evaluaciones periódicas de riesgos en la infraestructura tecnológica, así como auditorías de seguridad, para detectar vulnerabilidades y aplicar medidas preventivas.

9. RESPONSABILIDADES Y FUNCIONES

Para el cumplimiento de la presente política de planificación, se establecen las siguientes responsabilidades y funciones:

formato sugerido:

Sección de Soporte Técnico

- Inspeccionar y mantener los equipos tecnológicos, asegurando que no haya fallos imprevistos.
- Asegurar que todos los sistemas sean actualizados con las últimas versiones de software de seguridad, incluyendo antivirus y licencias.
- Mantener un registro detallado de las licencias y su renovación, archivando la información tanto en formatos físicos como digitales.
- Resolver problemas reportados de manera oportuna, garantizando que todos los equipos y sistemas funcionen correctamente.
- Registrar y documentar todos los incidentes técnicos y sus soluciones.

Departamento de Bienes Nacionales

- Recibir los dictámenes de hardware obsoleto del personal técnico del departamento de Infotecnología e iniciar el proceso de reemplazo de equipos.
- Gestionar la eliminación de equipos obsoletos conforme a los procedimientos establecidos.

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 23 de 29

Sección de Infraestructura Tecnológica

- Configurar y verificar el sistema de respaldo automatizado, asegurando que todos los datos relevantes estén respaldados correctamente.
- Monitorear y verificar la integridad de los respaldos.
- Establecer los requisitos para la creación y gestión de contraseñas seguras.
- Proveer capacitación al personal sobre el manejo seguro de contraseñas.
- Asegurar que se apliquen de manera regular los parches de seguridad necesarios en todos los sistemas.
- Limitar el acceso al Data Center a personal autorizado, como técnicos y jefes de infraestructura.
- Regular la temperatura dentro del Data Center para proteger los equipos.
- Realizar evaluaciones periódicas de riesgos y revisar los sistemas de seguridad cibernética.
- Realizar evaluaciones de riesgos periódicas cada 15 días.
- Generar reportes sobre las condiciones de seguridad del Data Center y recomendar medidas correctivas si es necesario.
- Ejecutar auditorías mensuales para asegurar que el hardware y la infraestructura cumplen con los estándares de seguridad.

Sección de Desarrollo de Software

- Recoger los requisitos de los departamentos solicitantes para el desarrollo de nuevos sistemas o la modificación de los existentes.
- Desarrollar, probar e implementar sistemas conforme a los estándares de calidad.
- Asegurar que los sistemas desarrollados sean funcionales y se alineen con los objetivos estratégicos del Instituto.
- Realizar pruebas y actualizaciones periódicas de los sistemas.
- Detectar y corregir errores o fallos en los sistemas existentes.

	INSTITUTO NACIONAL PENITENCIARIO	
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 24 de 29

- f) Asegurar que los sistemas continúen cumpliendo con los requerimientos del Instituto.
- g) Desarrollar manuales de usuario claros y fáciles de entender.

Sección de Estadística

- a) Gestionar y procesar las solicitudes de información sobre personas privadas de libertad.
- b) Asegurar la veracidad y actualización de la información en las bases de datos.
- c) Elaborar los perfiles penitenciarios solicitados conforme a los datos disponibles en las bases institucionales.
- d) Garantizar la protección de la privacidad y la seguridad de la información solicitada.

Jefe del Departamento de Infotecnología

- a) Identificar oportunidades para automatizar procesos que beneficien el control interno.
- b) Garantizar el cumplimiento de normas y procedimientos en el uso de tecnologías.
- c) Aportar conocimientos específicos sobre las necesidades y desafíos de la unidad en relación con los sistemas informáticos.
- d) Contribuir a la identificación de necesidades específicas de la unidad en términos de sistemas operativos.

Departamento de Infotecnología

- a) Desarrollar Informes periódicos a Subdirección de Desarrollo Institucional para evaluar el cumplimiento de las funciones asignadas a cada uno de los miembros del departamento
- b) Desarrollar el Plan Operativo Anual que incluya proyectos de infraestructura tecnológica, seguridad de la información, y desarrollo de software.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 25 de 29

- c) Colaborar con la Unidad de Planificación y Evaluación de la Gestión (UPEG) para garantizar que el POA sea alineado con los objetivos estratégicos institucionales.
- d) Elaborar el Plan Anual de Compras y Contrataciones (PACC) del departamento de Infotecnología de acuerdo con las necesidades y la disponibilidad del presupuesto.

Unidad de Planificación y Evaluación de la Gestión

- a) Revisión y aprobación del POA tecnológico.
- b) Evaluar la coherencia del POA con los planes nacionales y sectoriales de desarrollo
- c) Monitorear y evaluar el cumplimiento de los planes a nivel institucional, incluyendo el PEI, POA y otros planes, asegurando que se alcancen los objetivos establecidos y proponiendo ajustes cuando sea necesario.

Unidad de Auditoría Interna

- a) Dar estricto seguimiento al efectivo cumplimiento de la presente POLÍTICA e informar al respecto y oportunamente a las instancias correspondientes, entre ellos, el Comité de Control Interno Institucional.

10. DIVULGACION

La divulgación de la política institucional de tecnología del Instituto Nacional Penitenciario (INP) de Honduras tiene como objetivo garantizar el uso eficiente y seguro de la tecnología en los centros penitenciarios del país. Esta política está orientada a:

- 1. Optimizar los recursos tecnológicos:** Asegurar que las infraestructuras tecnológicas disponibles sean adecuadas para el cumplimiento de las funciones de seguridad, control y rehabilitación en los centros penitenciarios.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 26 de 29

2. Protección de la información: Implementar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos e información del INP, así como la protección contra ciber amenazas.

3. Capacitación del personal: Promover la formación continua del personal para asegurar que estén actualizados sobre el uso adecuado y seguro de las tecnologías implementadas en las operaciones penitenciarias.

4. Innovación y mejora continua: Fomentar la innovación tecnológica para mejorar la eficiencia operativa y los procesos de rehabilitación de los reclusos, utilizando herramientas y sistemas avanzados que faciliten el trabajo dentro del sistema penitenciario.

5. Cumplimiento normativo: Asegurar que todas las acciones tecnológicas cumplan con las leyes y regulaciones nacionales e internacionales en materia de seguridad, privacidad y protección de datos.

11. ACTUALIZACION

La política institucional de tecnología del Instituto Nacional Penitenciario (INP) de Honduras establece que debe ser revisada anualmente por el Comité de Control Interno Institucional. En caso de que se consideren necesarias modificaciones, se debe seguir un procedimiento estructurado para asegurar la transparencia y el cumplimiento normativo. Los pasos a seguir son los siguientes:

- 1. Revisión Anual:** El Comité de Control Interno Institucional debe revisar la política cada año, asegurándose de que esté actualizada y alineada con las necesidades operativas del INP y las normativas vigentes.
- 2. Modificaciones Necesarias:** Si durante la revisión se determinan cambios necesarios, se deberá documentar la fecha de la sesión del Comité en la que se haya aprobado dicha modificación.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 27 de 29

3. Notificación:

Una vez aprobadas las modificaciones, estas deben ser notificadas a:

- La Unidad de Auditoría Interna.
- Cada una de las unidades que conforman el INP.
- La Oficina Nacional de Desarrollo Integral de Control Interno (ONADICI).

4. Publicación: Las modificaciones también deben ser publicadas en:

- La página web institucional del INP.
- La plataforma de la Oficina Nacional de Desarrollo Integral de Control Interno (ONADICI).

5. Monitoreo de Cambios Normativos: El Comité de Control Interno Institucional tiene la responsabilidad de monitorear cualquier cambio en la normativa de control interno establecida por:

- El Tribunal Superior de Cuentas.
- La Oficina Nacional de Desarrollo Integral de Control Interno (ONADICI).
- El Instituto de Acceso a la Información Pública (IAIP).

6. Modificación Inmediata: Si hay cambios en estas normativas, el Comité deberá realizar las modificaciones correspondientes en la política tecnológica de forma inmediata, asegurando que el INP continúe cumpliendo con los requerimientos legales y de control interno.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 28 de 29

12. GLOSARIO

- **Software:** El software es el conjunto de programas informáticos que permiten a un dispositivo realizar diversas tareas o funciones específicas.
- **Fortinet:** Fortinet proporciona una amplia gama de soluciones de prevención de intrusos que ayudan a proteger las redes informáticas contra ataques cibernéticos, detectando y bloqueando actividades maliciosas antes de que causen daño.
- **Antivirus:** Un antivirus es un programa informático diseñado para detectar, prevenir y eliminar software malicioso, como virus, gusanos, troyanos y spyware, con el objetivo de proteger un sistema informático contra amenazas de seguridad.
- **Licencias de Software:** Las licencias de software son acuerdos legales que especifican los términos y condiciones de uso de un programa informático. Estas licencias pueden incluir restricciones sobre la cantidad de dispositivos en los que se puede instalar el software, el período de tiempo de uso y las capacidades del programa.
- **Soporte Técnico:** El soporte técnico es un servicio proporcionado por empresas o individuos que ayuda a los usuarios a resolver problemas técnicos relacionados con el hardware o software de sus dispositivos informáticos. Esto puede incluir asistencia telefónica, en línea, por correo electrónico o presencial.
- **Vulnerabilidades:** son debilidades o fallos en el software o hardware de un sistema informático que pueden ser explotadas por atacantes para comprometer la seguridad de dicho sistema. Estas vulnerabilidades pueden permitir el acceso no autorizado, la ejecución de código malicioso u otras actividades malintencionadas.

	INSTITUTO NACIONAL PENITENCIARIO	 HONDURAS GOBIERNO DE LA REPÚBLICA
Versión "1.0"	POLÍTICA DE TECNOLOGÍA Fecha: XX de Mes 20XX	I.N.P. 29 de 29

- **Firewalls:** Un firewall es un sistema de seguridad que controla y filtra el tráfico de red basado en reglas predefinidas, con el fin de proteger una red privada o un dispositivo de accesos no autorizados y ataques maliciosos desde Internet.
- **Monitoreo de Red:** El monitoreo de red es el proceso de supervisar y analizar el tráfico de una red informática con el fin de detectar problemas de rendimiento, identificar posibles amenazas de seguridad y garantizar el funcionamiento óptimo de los dispositivos y servicios de red.
- **Arquitectura del Software:** La arquitectura del software se refiere a la estructura y organización de un sistema de software, incluyendo los componentes, módulos, interfaces y relaciones entre ellos. Define cómo se diseñan, implementan y gestionan los diferentes elementos del software para satisfacer los requisitos del sistema y los objetivos del proyecto.

TEGUCIGALPA, F.M. 19 DE NOVIEMBRE DE 2024

REGISTRO : MEMORÁNDUM No.660-INF-INP-2024
ASUNTO : REMISIÓN

A L : SEÑORA
COORDINADORA DE DESARROLLO INSTITUCIONAL
MÁSTER
NORMA ZULEMA MARTINEZ RAMOS
SU OFICINA

1. Por este medio me dirijo a usted con el fin de dar respuesta al Memorándum COCOIN-INP-No.110-2024 con relación a la Política de Tecnología del Departamento de Infotecnología, se hace la entrega formal del documento adjunto. Adicionalmente, este documento ha sido enviado al correo electrónico erika.jacqueline@inp.gob.hn para su archivo y referencia.
2. Sin otro particular, me suscribo a usted con mis muestras de subordinación y respeto.



INGENIERO

MOISES A. RODRIGUEZ DEGRANDEZ
Coordinador del Departamento de
Infotecnología

CC: ARCH. INFOTECNOLOGIA
K*



ACTA DE APROBACIÓN

POLITICAS INSTITUCIONALES

En el Municipio del Distrito Central, Departamento de Francisco Morazán, a los cuatro días del mes de diciembre del año dos mil veinticuatro (04/12/2024), siendo las 14:00, en las oficinas del Instituto Nacional Penitenciario (INP), reunidos el **Coronel de Infantería D.E.M. RAMIRO FERNANDO MUÑOZ BONILLA**, en su calidad de Comisionado Presidente de la Comisión Interventora; el **Coronel de Ingeniería D.E.M. ADÁN ANTONIO RAMÍREZ SALINAS** en su calidad de Comisionado Adjunto; y el **Coronel de Infantería D.E.M. JOSÉ BALMORES DEL CID QUINTERO** también Comisionado Adjunto, reunidos en el edificio administrativo del Instituto Nacional Penitenciario (INP), específicamente en la Sala de Juntas ubicada en el tercer (03) piso, con el propósito principal de evaluar diversas políticas institucionales, que debido a sus diferentes ejes de acción constituyen elementos fundamentales para la adecuada operativización del Sistema Penitenciario Nacional (SIPENA). Las políticas evaluadas son las siguientes:

- **POLÍTICA DE PROBIDAD Y ÉTICA PÚBLICA:** Tiene como propósito fundamental promover un Sistema Penitenciario transparente, eficiente y comprometido con los principios éticos y legales que aseguren la integridad en su funcionamiento.
- **POLÍTICA DE CONTROL INTERNO:** Busca establecer y fortalecer los mecanismos de supervisión, seguimiento y evaluación de los procesos internos, promoviendo una administración efectiva del Sistema Penitenciario y alineada con las normativas nacionales e internacionales.
- **POLÍTICA DE TALENTO HUMANO:** Tiene como objetivo principal establecer lineamientos claros para la gestión, desarrollo y bienestar del personal que integra el sistema penitenciario. Esta política busca garantizar que los recursos humanos sean gestionados de manera eficiente y profesional, contribuyendo al cumplimiento de la misión institucional y fortaleciendo la seguridad y rehabilitación en el sistema penitenciario.
- **POLÍTICA DE PLANIFICACION Y RENDICION DE CUENTAS:** Busca establecer un marco normativo y operativo que garantice una gestión transparente, eficiente y orientada a resultados en el sistema penitenciario. A través de esta política, el INP busca responder de manera efectiva a las demandas sociales y cumplir con las obligaciones legales e institucionales relacionadas con la administración de recursos, la planificación estratégica y la rendición de cuentas.
- **POLÍTICA DE EFICIENCIA ADMINISTRATIVA:** Busca mejorar la gestión de recursos humanos, materiales y financieros dentro de la institución, asegurando que se utilicen de manera eficiente, efectiva y transparente.

- **POLÍTICA DE TRANSPARENCIA:** Tiene como objetivo principal garantizar la rendición de cuentas, el acceso a la información pública, y la gestión ética en el sistema penitenciario. A través de esta política, el INP busca promover la confianza de la ciudadanía, prevenir la corrupción y fortalecer la institucionalidad.
- **POLÍTICA DE TECNOLOGÍA:** Busca establecer un marco estratégico para el uso, gestión y desarrollo de tecnologías que fortalezcan la operatividad, seguridad y transparencia del sistema penitenciario. Sus objetivos están orientados a optimizar procesos, mejorar la comunicación, garantizar la seguridad y promover la modernización institucional.
- **POLÍTICA DE CALIDAD DE LOS SERVICIOS:** Busca garantizar la prestación eficiente, transparente y humanitaria de los servicios en los centros penitenciarios del país, promoviendo estándares que aseguren la dignidad humana, la rehabilitación y la reintegración social de las personas privadas de libertad.

Bajo este mismo orden de ideas, es necesario recalcar que, para el cumplimiento de las funciones inherentes a la Comisión Interventora, en virtud de los Decretos Ejecutivos PCM-028-2023 y PCM-018-2024, resulta indispensable asegurar el cumplimiento de los productos establecidos. Para ello, es fundamental contar con actividades planificadas tanto a corto como a largo plazo, mediante una estructura administrativa que proporcione un único instrumento técnico - administrativo. Este instrumento debe delimitar de manera clara la documentación de los procedimientos y procesos garantizando uniformidad en su contenido y presentación, lo que permitirá optimizar y asegurar el cumplimiento de las atribuciones del Sistema Penitenciario Nacional, así como el adecuado funcionamiento de las unidades administrativas, técnicas y operativas, a través de manuales estandarizados.

Asimismo, la Comisión Interventora, con el fin de lograr el normal funcionamiento del Sistema Penitenciario Nacional, procedió a la juramentación del Comité de Control Interno del Instituto Nacional Penitenciario (INP), en fecha veintinueve (29) de agosto de 2023, acto que consta en el acta correspondiente. En dicha ceremonia los miembros del COCOIN-INP manifestaron su compromiso con la implementación de los mecanismos de dirección y control, para asegurar la transparencia y la lucha contra la corrupción en las actividades del Instituto Nacional Penitenciario (INP). Este acto favorece la rendición de cuentas sobre la gestión realizada y el logro de las metas, determinando la necesidad de elaborar e implementar métodos que permitan una adecuada implementación del Control Interno Institucional de las operaciones del Instituto Nacional Penitenciario, conforme a su valor público, con el objetivo de fortalecer la organización y contribuir al logro de los objetivos institucionales.

En este sentido, tras revisar y analizar las ocho (08) políticas internas detalladas anteriormente, se concluye que están alineadas con la Circular STLCC-ONADICI No. 003-01-2023, que establece con carácter urgente la conformación de un Sistema Nacional de Control Interno y el cumplimiento obligatorio de las actividades y productos de control

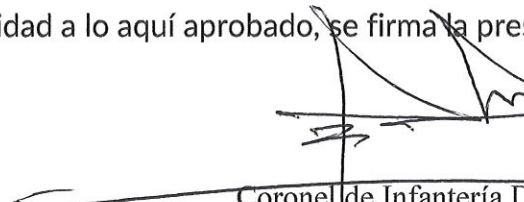
interno planteados en el Plan Anual para la Implementación del Marco Rector del Control Interno Institucional de los Recursos Públicos (MARCI). Además, cada una de las políticas se vincula con las Guías metodológicas para la Elaboración de Manuales de Procedimientos para el Sector Público”.

Bajo esta prerrogativa, y de acuerdo con lo estipulado en el Decreto No.64-2012, en su Artículo 7, se crea el Instituto Nacional Penitenciario Nacional (INP) como un órgano desconcentrado, cuya responsabilidad es la organización, administración y funcionamiento del Sistema Penitenciario Nacional y los servicios inherentes. Según el Artículo 8, inciso 7), el INP tiene entre sus atribuciones la de elaborar y aprobar los reglamentos necesarios para la operativización del Sistema.

En consideración a lo anteriormente expuesto, se proceden a aprobar las siguientes políticas institucionales:

1. Política de Probidad y Ética Pública
2. Política de Control Interno
3. Política de Talento Humano
4. Política de Planificación y Rendición de Cuentas
5. Política de Eficiencia Administrativa y Financiera
6. Política de Transparencia
7. Política de Tecnología
8. Política de Calidad de los Servicios

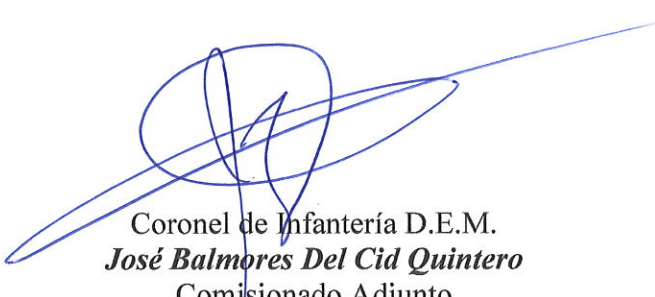
Para dar legalidad a lo aquí aprobado, se firma la presente por:



Coronel de Infantería D.E.M.
Ramiro Fernando Muñoz Bonilla
Presidente Comisión Interventora del Sistema Penitenciario Nacional
Comandante de la PMOP / Operación Fe y Esperanza



Coronel de Ingeniería D.E.M.
Adán Antonio Ramírez Salinas
Comisionado Adjunto
Comisión Interventora del Sistema Penitenciario Nacional


Coronel de Infantería D.E.M.
José Balmores Del Cid Quintero
Comisionado Adjunto
Comisión Interventora del Sistema Penitenciario Nacional