

Servicio de actualización de instrumentos normativos del Sistema de Gestión de Seguridad de la Información (SGSI) y del Sistema de Gestión de Continuidad del Negocio (SGCN) de la Plataforma Nacional de Gobierno Digital (PNGD) de la Subsecretaría de Tecnologías y Seguridad Digital (SSTSD) de la Secretaría de Gobierno y Transformación Digital (SGTD) de la Presidencia del Consejo de Ministros (PCM).

ING. ROSA YAMILET ZARATE COILA

Fecha: 13-11-2024

1. Importancia de la Seguridad de la Información
2. Importancia de la Continuidad operativa
3. Sistema Integrado de Gestión
4. Roles y Responsabilidades del Personal
5. Manejo Seguro de la Información y Buenas Prácticas

SENSIBILIZACIÓN





La Plataforma Nacional de Gobierno Digital (PNGD) es una nube privada administrada por el Estado que se crea en el marco de la Ley de Gobierno Digital, aprobada por el Decreto Legislativo N° 1412. Esta ley establece el régimen jurídico para el uso de tecnologías digitales en la Administración Pública.

La PNGD permite a las entidades públicas alojar sus servicios en una infraestructura como servicio, con el objetivo de fortalecer los servicios digitales de la ciudadanía.

Importancia de la Seguridad de la Información



El Peruano / Viernes 8 de setiembre de 2023

NORMAS

**Establecen la implementación y
mantenimiento del Sistema de Gestión
de Seguridad de la Información en las
entidades públicas**

**RESOLUCIÓN DE SECRETARÍA DE GOBIERNO
Y TRANSFORMACIÓN DIGITAL
N° 003-2023-PCM/SGTD**

**ESTABLECE LA IMPLEMENTACIÓN Y
MANTENIMIENTO DEL SISTEMA DE GESTIÓN
DE SEGURIDAD DE LA INFORMACIÓN EN LAS
ENTIDADES PÚBLICAS**

Lima, 6 de setiembre de 2023

VISTO:

CIBERAMENAZAS LIVE-MAP ES

Prot

MAPA ESTADÍSTICAS FUENTES DE INFORMACIÓN ZUMBIDO WIDGET

 **RUSIA** 

1 EL PAÍS MAS ATACADO

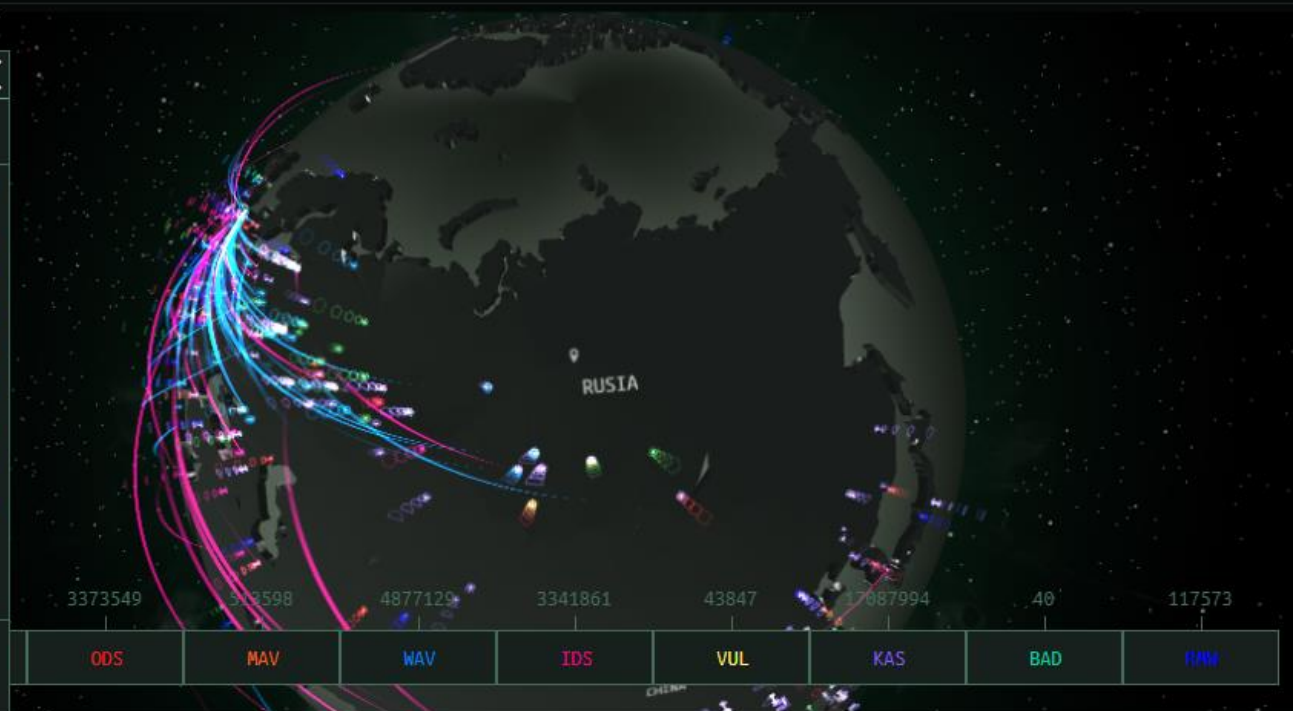
OAS	2230681
ODS	1393513
MAV	24676
WAV	2333577
IDS	524994
VUL	7839
KAS	5227571
BAD	0
RAW	5022

Detección realizada desde las 00:00 GMT

[Más detalles](#)

Compartir información



kaspersky

Basado en los datos de Kaspersky.

© 2024 AO Kaspersky Lab. Todos los derechos reservados.

[Términos de servicio](#) [Política de privacidad](#) [Cookies](#)

Importancia de la Continuidad operativa



Resolución Ministerial

Lima, 30 DIC. 2021

Nº320-2021-PCM

VISTOS:

El Oficio N° 5008-2020-INDECI/5.0 complementado con el Oficio N° 4612-2021-INDECI/12.0, del Instituto Nacional de Defensa Civil – INDECI; así como el Informe N° 0000097-2021-PCM-UF-OTGRD-BAS de la Unidad Funcional de Ordenamiento Territorial y Gestión de Riesgo de Desastres del Despacho Viceministerial de Gobernanza Territorial;

CONSIDERANDO:

Que, el artículo 1 de la Ley N° 29864, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), dispone la creación de dicho Sistema, con la finalidad de identificar y reducir los riesgos asociados a peligros o minimizar sus efectos; así como, evitar la generación de nuevos riesgos, y preparación y atención ante situaciones de desastres mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión del Riesgo de Desastres;

Que, según lo dispuesto en el artículo 9 y el literal g) del artículo 10 de la citada Ley, la Presidencia del Consejo de Ministros es el ente rector del SINAGERD; y, en dicha condición, tiene la atribución de aprobar directivas y lineamientos en los ámbitos relacionados con la Gestión del Riesgo de Desastres;

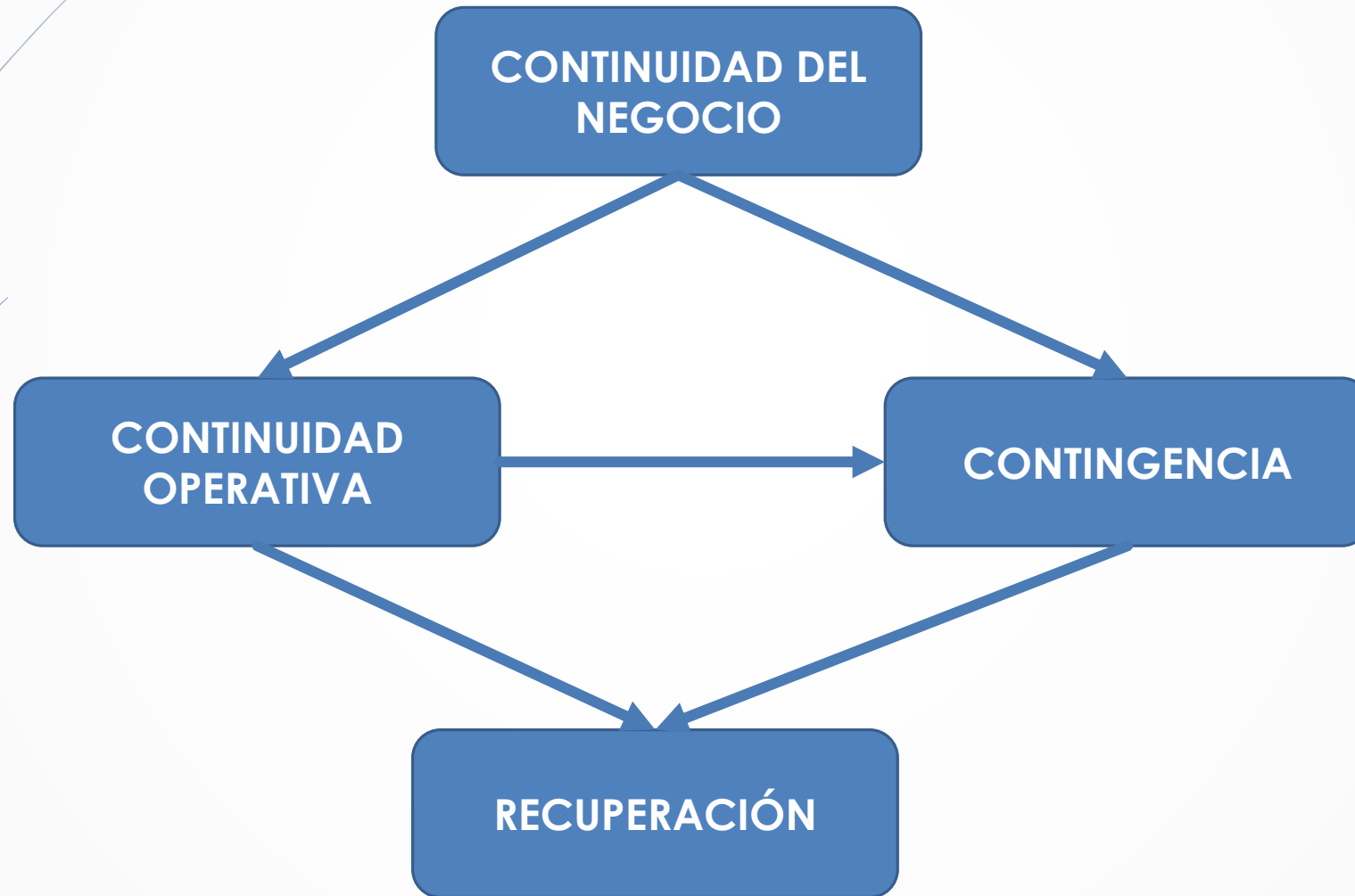
Que, el numeral 5.3 del Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2014-2021, aprobado por Decreto Supremo N° 034-2014-PCM, prevé como objetivo estratégico 5, fortalecer las capacidades institucionales para el desarrollo de la gestión de riesgo de desastres; y, en ese marco, establece como objetivo específico 5.2, desarrollar la gestión de continuidad operativa del Estado que, a su vez, tiene como indicador, un porcentaje de entidades del SINAGERD que cuentan con Planes de Continuidad Operativa implementados y actualizados;

Que, el referido Plan Nacional establece para el objetivo específico 5.2, tres (3) acciones, siendo una de ellas, desarrollar instrumentos técnicos normativos para la gestión de la continuidad operativa, que implica la elaboración, difusión e implementación de instrumentos que permitan la gestión de la continuidad operativa de las entidades de mayor alcance en las acciones de emergencia y contingencias, contemplando como actores de dicha acción a los tres niveles de gobierno;

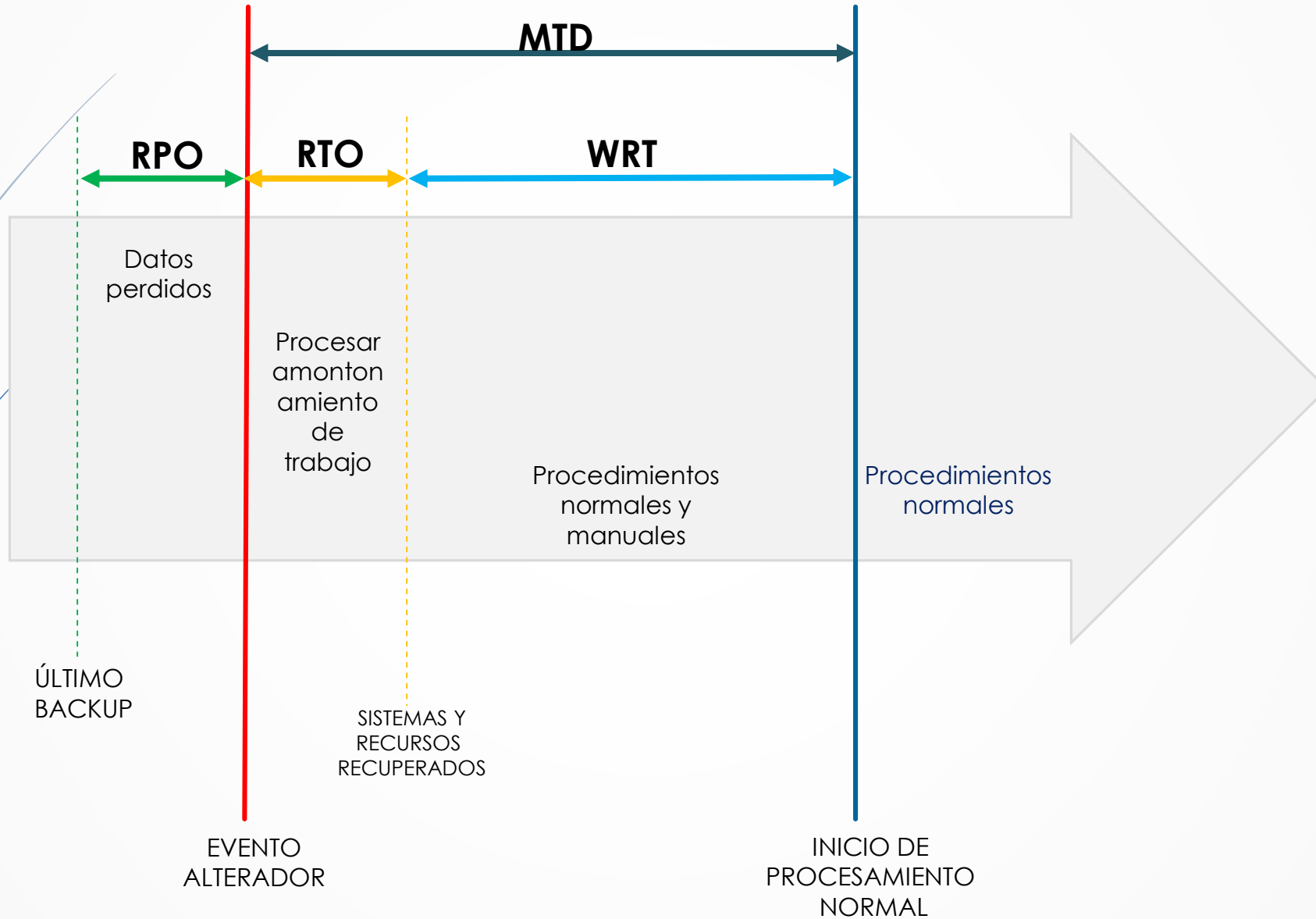
Que, bajo dicho marco normativo, mediante Resolución Ministerial N° 028-2015-PCM se aprueban los "Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno";



Componentes clave y su interacción



TIEMPOS DE RECUPERACIÓN



**NORMA TÉCNICA
PERUANA**

**NTP-ISO/IEC 27001
2022**

Dirección de Normalización - INACAL
Calle Las Camelias 817, San Isidro (Lima 15046)

Lima, Perú

**Seguridad de la información, ciberseguridad y protección
de la privacidad. Sistemas de gestión de seguridad de la
información. Requisitos**

Information security, cybersecurity and privacy protection. Information security management systems. Requirements

(BQV. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements)

**2022-12-29
3ª Edición**

R.D. N° 022-2022-INACAL/DN. Publicada el 2023-01-12
I.C.S.: 03.100.70; 35.030

Precio basado en 31 páginas

ESTA NORMA ES RECOMENDABLE

Descriptor: Tecnología de la información, seguridad de la información, ciberseguridad, sistemas de gestión, requisitos

© ISO/IEC 2022 - © INACAL 2022

**NORMA TÉCNICA
PERUANA**

**NTP-ISO 22301
2020**

Dirección de Normalización - INACAL
Calle Las Camelias 817, San Isidro (Lima 27)

Lima, Perú

**Seguridad y resiliencia. Sistemas de gestión de continuidad
del negocio. Requisitos**

Security and resilience. Business continuity management systems. Requirements

(BQV. ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements)

**2020-04-02
1ª Edición**

R.D. N° 004-2020-INACAL/DN. Publicada el 2020-04-07
I.C.S.: 03.100.01; 03.100.70

Precio basado en 40 páginas

ESTA NORMA ES RECOMENDABLE

Descriptor: Seguridad, resiliencia, organización, gestión de la empresa, sistemas de gestión

© ISO 2019 - © INACAL 2020

SISTEMA INTEGRADO DE GESTIÓN

ANEXO SL

Cláusula 1:	Objeto y campo de aplicación
Cláusula 2:	Referencias normativas
Cláusula 3:	Términos y definiciones
Cláusula 4:	Contexto de la organización
Cláusula 5:	Liderazgo
Cláusula 6:	Planificación
Cláusula 7:	Soporte
Cláusula 8:	Operación
Cláusula 9:	Evaluación del desempeño
Cláusula 10:	Mejora

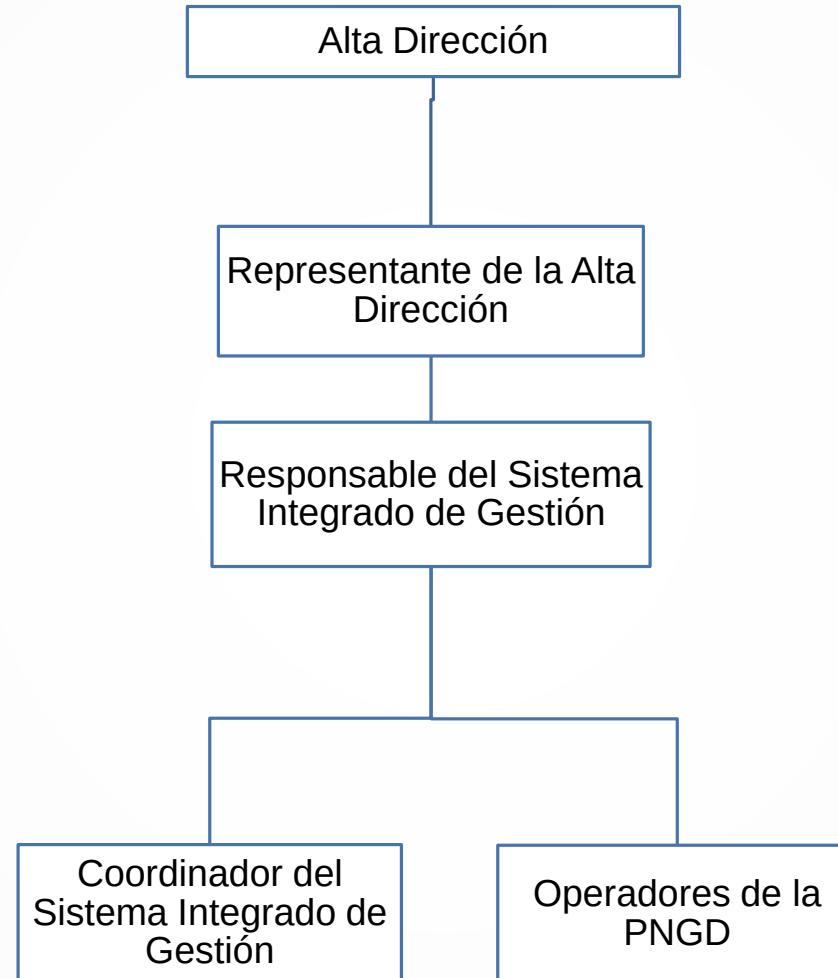
Integración del SGSI y SGCN

Diferencial del SGSI y SGCN

RELACION SGSI - SGCN



Roles y Responsabilidades del Personal



Responsabilidades del personal en materia de incumplimiento

Medidas Disciplinarias

El incumplimiento de estas disposiciones dará lugar a la aplicación de medidas disciplinarias y administrativas establecidas en la normativa interna de la PCM, sin perjuicio de las responsabilidades civiles o penales que correspondan.

Los lineamientos de uso aceptable comprenden:

- Queda prohibido el uso de activos para fines personales, comerciales o distintos a las funciones asignadas.
- Está prohibida la instalación de software no autorizado, así como el acceso o almacenamiento de información no vinculada a las funciones institucionales.
- Los usuarios deberán utilizar los activos de acuerdo con los perfiles de acceso asignados, evitando el uso compartido de credenciales, contraseñas o equipos.
- Todo acceso, modificación o transferencia de información debe realizarse únicamente a través de medios autorizados y seguros.
- Se establece la obligación de reportar de inmediato cualquier incidente de seguridad, pérdida, daño o mal uso de un activo.
- La PNGD se reserva el derecho de monitorear, auditar y registrar el uso de sus activos para verificar el cumplimiento de esta política.

Medidas Disciplinarias

El incumplimiento de estas disposiciones dará lugar a la aplicación de medidas disciplinarias y administrativas establecidas en la normativa interna de la PCM, sin perjuicio de las responsabilidades civiles o penales que correspondan.

Los lineamientos de uso aceptable comprenden:

- Queda prohibido el uso de activos para fines personales, comerciales o distintos a las funciones asignadas.
- Está prohibida la instalación de software no autorizado, así como el acceso o almacenamiento de información no vinculada a las funciones institucionales.
- Los usuarios deberán utilizar los activos de acuerdo con los perfiles de acceso asignados, evitando el uso compartido de credenciales, contraseñas o equipos.
- Todo acceso, modificación o transferencia de información debe realizarse únicamente a través de medios autorizados y seguros.
- Se establece la obligación de reportar de inmediato cualquier incidente de seguridad, pérdida, daño o mal uso de un activo.
- La PNGD se reserva el derecho de monitorear, auditar y registrar el uso de sus activos para verificar el cumplimiento de esta política.



Manejo Seguro de la Información y Buenas Prácticas

- 
1. Uso de Contraseñas Seguras
 2. Autenticación de Múltiples Factores (MFA)
 3. Actualización de Software y Parches
 4. Control de Acceso
 5. Concienciación y Capacitación del Personal
 6. Respaldo de Datos
 7. Protección Contra Malware
 8. Política de Limpieza de Escritorio y Pantalla
 9. Monitoreo y Registro de Actividades
 10. Gestión de Dispositivos Móviles
 11. Política de Eliminación Segura de Información