



INSTITUTO PERUANO DE ENERGÍA NUCLEAR

Resolución de Presidencia

N° 056-19-IPEN/PRES

Lima, 15/MAR/2019



VISTOS: La Hoja de Trámite N° Expediente I-5421-2018 de Secretaria General; y, el Informe N° 11-2019-PLPR/RACI de la Unidad de Racionalización de la Oficina de Planeamiento y Presupuesto, y;

CONSIDERANDO:

Que, mediante Hoja de Trámite N° Expediente I-5421-2018, Secretaria General remite el Memorandum N° 22-18-GTRI/IPEN, quien valida el proyecto de Directiva para el funcionamiento y operación del Sistema de Seguridad Electrónica del Instituto Peruano de Energía Nuclear - IPEN;

Que, el artículo 1 del Decreto Legislativo N° 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional, prescribe que el objeto, es regular la naturaleza, finalidad, funciones y estructura del Sistema de Defensa Nacional; asimismo, señala que el Sistema de Defensa Nacional garantiza la Seguridad Nacional, para la afirmación de los derechos fundamentales y el Estado constitucional de derecho, en el marco de una gestión pública moderna;

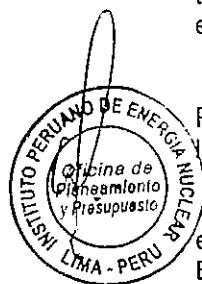
Que, el inciso c) del artículo 25 del Reglamento de Organización y Funciones del IPEN, aprobado mediante Decreto Supremo N° 062-2005-EM, establece que la Unidad de Racionalización está encargada de conducir la racionalización y modernización de los procesos técnicos y administrativos, así como de mantener actualizados los instrumentos de gestión como el ROF, el CAP y el MOF, así como los manuales y directivas de la Institución;

Que, en atención a ello, con Informe N° 11-2019-PLPR/RACI, la Unidad de Racionalización de la Oficina de Planeamiento y Presupuesto ha emitido la opinión técnica sobre la propuesta de la Directiva en mención;

Que, la propuesta de Directiva tiene por objetivo, establecer las disposiciones generales y específicas que permitan regular el funcionamiento y operación del Sistema de Seguridad Electrónica del IPEN;

Que, en atención a ello, resulta necesario emitir el acto administrativo que apruebe la citada Directiva, la cual contribuirá con la gestión administrativa de la Entidad;

De conformidad con los Artículos 9 y 10 del Reglamento de Organización y Funciones del IPEN, aprobado por Decreto Supremo N° 062-2005-EM;



Con los vistos del Director Ejecutivo (a.i.); de la Secretaria General; de la Directora de la Oficina de Asesoría Jurídica; y, del Director de la Oficina de Planeamiento y Presupuesto;

SE RESUELVE:

Artículo Primero.- Aprobar la Directiva para el funcionamiento y operación del Sistema de Seguridad Electrónica del Instituto Peruano de Energía Nuclear - IPEN, que forma parte integrante de la presente Resolución.

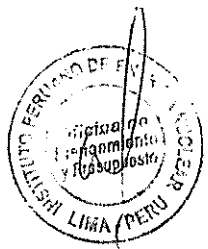
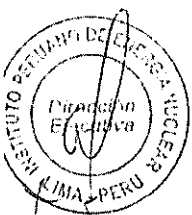
Artículo Segundo.- Los Órganos de la Institución, darán estricto cumplimiento al contenido de la Directiva, bajo responsabilidad.

Artículo Tercero.- Publicar la presente Resolución en la página web institucional.

REGISTRESE Y COMUNIQUESE



SUSANA PETRICK CASAGRANDE
Presidenta
Instituto Peruano de Energía Nuclear



	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 1 de 13

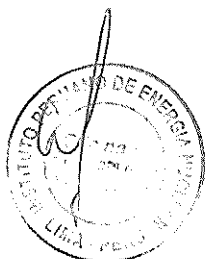
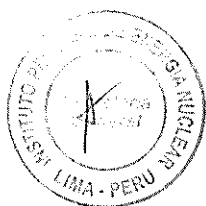
DIRECTIVA PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR

Secretaría General	Oficina de Planeamiento y Presupuesto	Oficina de Asesoría Jurídica	Resolución de Presidencia N° -2019-IPEN/PRES	15/03/2019
Elaborado por 	Revisado por 	Revisado por 	Aprobado por 	Fecha de aprobación

	DIRECTIVA		DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR		Versión N° 01
			Página de 2 de 13

Control de cambio en documentos

Nº	Versión	Ítem	Modificación respecto a la edición anterior	Sustento	Unidad que solicito el cambio	Observaciones



	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 3 de 13

1. FINALIDAD

Permitir la detección de eventos de intrusión, sabotaje u otros actos maliciosos y/o prevenir la ocurrencia de situaciones irregulares provenientes de las amenazas internas o externas (creíbles, potenciales y evidentes), así como riesgos (naturales o antrópicos), que podrían atentar contra la integridad de las personas, la seguridad física de los materiales, las instalaciones nucleares, las instalaciones radiactivas y las instalaciones administrativas del IPEN.

2. OBJETIVO

Establecer las disposiciones generales y específicas que permitan regular el funcionamiento y operación del Sistema de Seguridad Electrónica del Instituto Peruano de Energía Nuclear – IPEN.

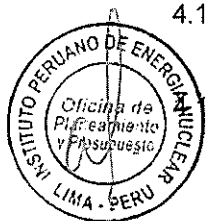
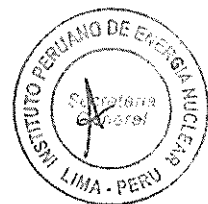
3. ÁMBITO DE APLICACIÓN

Las disposiciones contenidas en la presente directiva son de aplicación en todos los Órganos del Instituto Peruano de Energía Nuclear.

4. BASE LEGAL

- 4.1 Constitución Política del Perú
- 4.2 Decreto Legislativo N° 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional.
- 4.3 Decreto Supremo N° 037-2013-PCM, que aprueba el Reglamento del Decreto Legislativo 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional.
- 4.4 Ley N° 29733, Ley de Protección de datos personales
- 4.5 Ley N° 28716, Ley de Control Interno de las Entidades del Estado.
- 4.6 Decreto Legislativo N° 1218, Decreto Legislativo que regula el uso de cámaras de video vigilancia.
- 4.7 Resolución Legislativa N° 26376, que aprueba la Convención sobre la Protección Física de Materiales Nucleares.
- 4.8 Resolución de Contraloría N° 320-2006-CG, Normas de Control Interno.
- 4.9 Decreto Supremo N° 062 – 2005 - EM que aprueba la Estructura Orgánica y el Reglamento de Organización y Funciones del Instituto Peruano de Energía Nuclear.
- 4.10 Decreto Supremo N° 014-2002-EM, que aprueba el Reglamento de Protección Física de Materiales e Instalaciones Nucleares.
- 4.11 Resolución de Presidencia N° 097-18-IPEN/PRES, que aprueba la Directiva DIR-001-IPEN/PLPR "Directiva para la Elaboración, Aprobación, Difusión, Actualización y Control de los Documentos Normativos del Instituto Peruano de Energía Nuclear".
- 4.12 Resolución de Presidencia N° 131-11-IPEN/PRES, que aprueba la Norma Técnica "Requisitos de Seguridad Física de Fuentes Radiactivas. Norma de Seguridad SF.001.2011.
- 13 Recomendaciones de Seguridad Física Nuclear para la Protección Física de los Materiales e Instalaciones Nucleares, NSS N° 13 (INFCIRC/225/Revisión 5). (Publicación –libro) Colección de Seguridad Física Nuclear del OIEA N° 13.

Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.



	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 4 de 13

5. DISPOSICIONES GENERALES

5.1. Siglas

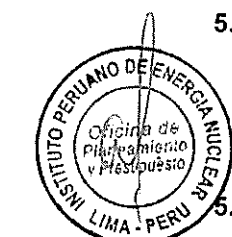
APDP	Autoridad Nacional de Protección de Datos Personales
CGBVP	Cuerpo General de Bomberos Voluntarios del Perú.
COEL	Centro de Operaciones de Emergencia Local
DNSF	Defensa Nacional y Seguridad Física
EPP	Equipo de Protección Personal
IPEN	Instituto Peruano de Energía Nuclear.
LSCD	Laboratorio Secundario de Calibraciones Dosimétricas
PGRR	Planta de Gestión de Residuos Radiactivos
SAMU	Servicio de Atención Médica de Urgencias
SCTR	Seguro Complementario de Trabajo de Riesgo
SIF	Seguridad Integral Física
SINAGERD	Sistema Nacional de Gestión del Riesgo de Desastres
SINASEC	Sistema Nacional de Seguridad Ciudadana
TEIN	Equipo Técnico de Tecnología de la Información
UDEX	Unidad de Desactivación de Explosivos

5.2. Definiciones Operativas

- 5.2.1. Alarma:** Advertencia de una situación anormal, frente a indicios de peligro como la intrusión de personas, inicio de fuego, la presencia de agentes tóxicos, etc.
- 5.2.2. Amenaza:** Fenómeno natural o provocado por la actividad humana que se toma peligrosos para las personas, propiedades, instalaciones, al medio ambiente y al proceso. Es un factor externo de Riesgo.
- 5.2.3. Cámara IP:** Es una cámara de red que emite las imágenes directamente a la red e incorpora su propio miniordenador, que permita comprimir y emitir video sin necesidad de un ordenador.

	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 5 de 13

- 5.2.4. Captación:** Recepción y transmisión de imágenes, videos o audios registrados a través de cámaras de video vigilancia.
- 5.2.5. CCTV:** Circuito Cerrado de Televisión. Definición que se da al conjunto de componentes de receptor de la visualización (cámaras), medios de transmisión de la señal de video (cables) y presentación de la visualización (monitor-TV).
- 5.2.6. Datos personales:** Son aquellas imágenes, videos, audios u otros que identifican o hacen identificables a las personas naturales.
- 5.2.7. Estación de Control de Alarmas (CAS):** Estación de monitoreo donde se encuentra el personal de Defensa Nacional y Seguridad Física (DNSF) que opera el sistema de seguridad electrónico y atiende durante las 24 horas de los 365 días del año las llamadas de emergencias y/o situaciones inusuales de las sedes del IPEN.
- 5.2.8. Emergencia:** Estado de daños sobre la vida, el patrimonio y el medio ambiente ocasionado por la ocurrencia de un fenómeno natural o inducido por la acción humana que altera el normal desenvolvimiento de las actividades de la zona afectada.
- 5.2.9. Grabación:** Almacenamiento de imágenes o audios en cualquier medio de soporte, de manera que se pueda reproducir.
- 5.2.10. Incendio:** Reacción química que adquiere dimensiones mayores con efectos destructores y de gran pérdida.
- 5.2.11. Instalación:** Procedimiento de colocación de equipos y conexiones de las cámaras de video vigilancia.
- 5.2.12. Niveles de visualización de Usuario:** Niveles a otorgarse para la visualización, registro y operación del sistema de seguridad electrónica:
- Nivel A: Solamente Visualización.
- Nivel B: Visualización, registro y operación del sistema
- Nivel C: Visualización, registro, operación del sistema y configuración de parámetros.
- 5.2.13. Peligro:** Probabilidad de que un fenómeno físico, potencialmente dañino, de origen natural o inducido por la acción humana, se presente en un lugar específico, con una cierta intensidad y en un periodo de tiempo y frecuencia definidos. Es todo aquello que tiene potencial de causar u ocasionar un daño a las personas, al medio ambiente, a la propiedad o al proceso productivo.
- 5.2.14. Registro:** Acto mediante el cual se administra la información obtenida en las cámaras de video vigilancia.
- 5.2.15. Riesgo:** Es la probabilidad de ocurrencia de sufrir daños las personas, estructura física o las actividades socioeconómicas, a causa de la vulnerabilidad existente y el impacto de un peligro.
- 5.2.16. Servidor Local:** Recurso de computo (ordenador) dedicado atender los requerimientos del Sistema de Seguridad Electrónico en las Sedes (almacenamiento y visualización), conectado a través de la red LAN, para su transmisión al CAS.



	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 6 de 13

5.2.17. Servidor NAS: Dispositivo de almacenamiento principal que se accede a través de protocolo IP, dedicado a compartir la capacidad de almacenamiento de un computador con órdenes o servidores clientes a través de la red (TCP/IP) y para este caso donde se almacena la información visual de los servidores locales.

5.2.18. Sistema de Seguridad Electrónico: Sistema que utiliza el principio del CCTV, para la visualización y grabación local y remota de cámaras con tecnología IP (Red LAN/WAN) y cámaras análogas con tecnología digital, integradas a un solo sistema, para la vigilancia de instalaciones.

5.2.19. Situación de Emergencia: Situación declarada ante la inminencia del Impacto de una amenaza o después de que esta ha ocurrido, donde será necesario activar el Plan de Contingencias.

5.2.20. Tratamiento de Información: Procedimiento que incluye la reproducción, entrega, conservación, reserva y destrucción de imágenes y/o audios.

5.2.21. Utilidad del Sistema de Seguridad Electrónico: Puede ser usado como una herramienta de detección (vigilancia, identificación, prevención y observación), registro y en algunos casos para el aprovechamiento de la información visual para el análisis; a fin de orientar el flujo de atención a una respuesta.

5.2.22. Visualización: Observación de una imagen captada por una cámara de video (IP o Analógica) a través de una pantalla (monitor) transmitida por un medio de comunicación (Red LAN/WAN).

5.2.23. Vulnerabilidad: Es la susceptibilidad de las personas, estructura física o las actividades socioeconómicas, de sufrir daños por acción de un peligro o amenaza.

5.3. El Sistema de Seguridad Electrónica del IPEN

5.3.1. El Sistema de Seguridad Electrónica cuenta con tres (03) centros de visualización y grabación en las Sedes del IPEN, y están ubicados en:

- Sede Central: Av. Canadá No. 1470 – San Borja
- Centro Nuclear: Av. José Saco Km 13 – Caraballo
- Oficina Técnica de la Autoridad Nacional : Jr. Justo Vigil 456 Magdalena del Mar

5.3.2. Se tendrá el control y visualización de las cámaras instaladas desde la Estación de Central de Alarmas (CAS) de Defensa Nacional y Seguridad Física (DNSF) ubicado en el Centro Nuclear "Oscar Miro Quesada de la Guerra" – RACSO.

5.3.3. El Sistema de Seguridad Electrónica incluye los equipos de radiocomunicación que dispone el IPEN, según la gamma de frecuencia autorizadas por el Ministerio de Transportes y Comunicaciones; asimismo forma parte del sistema el equipamiento de video vigilancia y radiocomunicaciones instaladas en los vehículos de servicio de transporte de personal.

5.3.4. El Sistema de Seguridad Electrónica debe disponer y cumplir con los estándares técnicos señalados en el Anexo N° 1 para la preservación y conservación de la integridad de las imágenes, videos y audios; durante el empleo del sistema se deberá velar por la protección de datos personales.

	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 7 de 13

- 5.3.5. La tecnología empleada en el Sistema de Seguridad Electrónica, permitirá disponer de la información de imágenes, videos o audios con indicios de la comisión de faltas o delitos y que sean requeridas por las autoridades del IPEN, la Policía Nacional o el Ministerio Público, según sea el caso.

6. DISPOSICIONES ESPECIFICAS

6.1 De las cámaras de video vigilancia

- 6.1.1 Las cámaras de video vigilancia deben complementarse con programas de administración de datos con licencia, soporte de energía de contingencia y sistemas de almacenamiento de cuarenta y cinco (45) días calendario como mínimo; que permitan la integración e interacción interna con dispositivos o aplicativos para la interface de Security y Safety.

- 6.1.2 Las cámaras de video vigilancia instaladas en las Sedes del IPEN y los Sub Sistemas de Seguridad Electrónica del Reactor Nuclear RP-10, Reactor Nuclear RP-0, Laboratorio de Irradiación - GAMMACELL, Laboratorio Secundario de Calibraciones Dosimétricas (LSCD) y Planta de Gestión de Residuos Radiactivos (PGRR) deberán integrarse a la Estación Central de Alarmas (CAS), en coordinación con DNSF.

- 6.1.3 Cualquier tipo de intervención o cambio de ubicación de las cámaras de video vigilancia y componentes electrónicos de los subsistemas RP-10, RP-0, Laboratorio de Irradiación - GAMMACELL, LSCD y PGRR, debe ser autorizado por DNSF.

6.2 De la captación y grabación de imágenes, videos o audios

- 6.2.1 Las imágenes, videos o audios registrados deben ser de alta calidad, permitiendo la plena identificación de las personas y serán almacenados por un periodo no menor a cuarenta y cinco (45) días calendario. La reproducción de estas imágenes o audios deben realizarse a través de mecanismos que permitan su visualización en tiempo real e ininterrumpido, se debe priorizar el empleo de fibra óptica.

- 6.2.2 En caso de detectarse indicios de comisión de delitos o faltas que se encuentren en procesos de investigación; las grabaciones podrán ser almacenadas durante un tiempo mayor al establecido, ser empleadas para interponer denuncias, identificar imputados o resolver controversias y podrán ser solicitados a Secretaría General por las autoridades pertinentes, personas naturales, jurídicas o ciudadanía en general contando con las autorizaciones correspondientes.

- 6.2.3 Los plazos de entrega de las grabaciones, bajo responsabilidad de DNSF son:

- **Flagrante delito:** menos de veinticuatro (24) horas.
- **Delitos bajo otras formas de ejecución:** no mayor de cinco (05) días hábiles.
- **Hechos no vinculados a la comisión de un delito o falta:** no mayor de diez (10) días hábiles

- 6.2.4 La alteración del estado original de imágenes, audios y videos o el incumplimiento de los plazos establecidos puede generar responsabilidad administrativa, civil o penal según corresponda.



	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 8 de 13

6.3 De la Instalación y mantenimiento del Sistema de Seguridad Electrónica

- 6.3.1** El servicio de instalación y mantenimiento de los componentes del sistema de seguridad electrónica podrá ser tercerizado integral o parcialmente, en estos casos los proveedores deberán contar con las autorizaciones legales pertinentes así como con la verificación de probidad y conformidad que deberá ser efectuada por DNSF.
- 6.3.2** DNSF efectuará el requerimiento para la contratación de servicios de personal y equipamiento especializado para el mantenimiento continuo del Sistema de Seguridad Electrónica según los programas especificados por los fabricantes de las partes y componentes del sistema.
- 6.3.3** La renovación de equipos electrónicos de seguridad debe mantener los estándares técnicos existentes, teniendo en cuenta la tendencia a un cambio continuo de la tecnología vigente en el mercado nacional.

6.4 Del Especialista de DNSF

- 6.4.1.** Es el encargado de la verificación permanente de la disponibilidad y almacenamiento de la información captada por un máximo de cuarenta y cinco (45) días calendario, periodo durante el cual se podrá rescatar información de utilidad en caso de situaciones inusuales o estadísticas. Cuando se requiera información visual del registro de grabación deberá atender las solicitudes presentadas con un máximo de cuarenta y cinco (45) días calendario de antigüedad de la ocurrencia o situación a verificar.
- 6.4.2.** Debe verificar diariamente que las cámaras no sean movidas de su lugar, que el servidor local y sus componentes instalados en el CAS y Sedes del IPEN se encuentren encendidos y operando correctamente; así como evitar que el compartimiento de comunicaciones donde se encuentra ubicado el servidor local sea utilizado para otros fines.
- 6.4.3.** El Especialista DNSF se encuentra sujeto al compromiso de confidencialidad de la información a fin de garantizar la no transmisión o divulgación de imágenes, videos o audios, bajo responsabilidad administrativa, civil y/o penal.
- 6.4.4** En caso de detectarse indicios de comisión de delitos o faltas en horario laboral o fuera de éste, el Especialista de DNSF o quien haga las veces, según el caso seguirá los protocolos de actuación y respuesta con la Policía Nacional del Perú, (PNP) y/o con el Serenazgo local como parte integrante del Sistema Nacional de Seguridad Ciudadana (SINASEC).

6.5 Del Personal operador de la estación de control de alarmas (CAS)

- 6.5.1** El personal del CAS contará con el nivel B de visualización de usuario a través del software implantado en el sistema, protegido con un código de acceso y clave (Password); el cual permitirá visualizar, recuperar los registros (grabaciones) y operar (controlar) las cámaras (IP y análogas) y el Sistema de Seguridad Electrónica y Radiocomunicación, realizando un monitoreo continuo para la captación de imágenes, videos y/o audios.
- 6.5.2** Durante el cumplimiento de sus funciones monitorea, orienta y apoya a los agentes de seguridad física, quienes custodian en forma permanente los accesos a las sedes

	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 9 de 13

institucionales protegiendo la seguridad de las personas y bienes dentro de las instalaciones.

6.5.3. Mediante la vigilancia electrónica controla que la intervención de los agentes de seguridad en áreas con presencia de material radiactivo o nuclear; sea con asesoramiento y/o acompañamiento del Oficial de Protección Radiológica (OPR) de dicha área.

6.5.4 Administra y revisa periódicamente el sistema CCTV y los servidores locales del Centro Nuclear Racso, Sede Central y OTAN para que la información de las cámaras (imágenes) de los hechos relevantes o inusuales queden registrados en la carpeta "Ocurrencias Relevantes" del servidor NAS con un máximo de cuarenta y cinco (45) días calendario y el mínimo de tiempo que se indica de acuerdo a cada Sede:

- Sede CN RACSO : Diez (30) días
- Sede Central : Quince (15) días
- Sede OTAN : Treinta (10) días

Posterior al tiempo mencionado deberá trasladar la información que lo amerite a una cinta magnética de almacenamiento (CD) u otros medios magnéticos, a fin de que sirva para el esclarecimiento de ocurrencias.

6.5.5 El personal del CAS se encuentra sujeto al compromiso de confidencialidad de la información a fin de garantizar la no transmisión o divulgación de imágenes, videos o audios, bajo responsabilidad administrativa, civil y/o penal; efectúa un servicio rotativo cada doce (12) horas a fin de cubrir las veinticuatro (24) horas del día en el CAS, estableciéndose los siguientes turnos:

- Turno diurno 08:00 a 20:00 horas
- Turno Nocturno 20:00 a 08:00 horas

La responsabilidad de la operatividad y entrega cargo del CAS se realiza durante el relevo en el registro de ocurrencias, dejando constancia de ello con la firma y aceptación del operador entrante y del operador saliente.

6.5.6 Durante el servicio nocturno debe revisar los registros de grabaciones de los servidores locales, manteniendo la información almacenada un máximo de cuarenta y cinco (45) días calendario y trasladar al servidor NAS las informaciones que han sido solicitadas y los hechos importantes o inusuales registrados en la carpeta de ocurrencias relevantes.

6.5.7 En caso de producirse una alarma, situaciones inusuales o de emergencia, el operador de turno en el CAS deberá comunicarse inmediatamente con el Especialista de DNSF y a la fuerza de respuesta constituida en las instalaciones nucleares del IPEN. De ser necesario interactuará externamente con las Centrales de Emergencia de la Policía Nacional del Perú, Centro de Operaciones de Emergencia Local (COEL), SAMU, Cuerpo General de Bomberos Voluntarios del Perú, Ministerio de Salud, Defensa Civil, entre otras entidades integrantes del SINAGERD y responsables de atender emergencias o desastres; según la naturaleza del evento que se genere.

6.6 Del personal CAS ante situaciones de sabotaje o robo

6.6.1. El personal operador del CAS, al visualizar situaciones inusuales como robo o sabotaje en alguna de las Sedes del IPEN tomará nota de la descripción de personas (cantidad, vestimenta, armas), vehículos (número de placa, color de vehículo) y de forma inmediata

	DIRECTIVA		DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR		Versión N° 01
			Página de 10 de 13

se comunicará con la fuerza de respuesta constituida en las instalaciones del IPEN y el especialista DNSF de la sede donde se presente la ocurrencia.

- 6.6.2. Administrará el sistema de seguridad electrónica para que las imágenes de los hechos queden registradas y sirvan para el esclarecimiento del delito a las autoridades especiales, debiendo archivarse en la carpeta de "Ocurrencias Relevantes" del servidor NAS.

6.7 Del personal CAS ante situaciones de atentado

- 6.7.1 El personal de turno en el CAS al momento de visualizar mediante el sistema de video vigilancia, acciones sospechosas por parte de vehículos que no sean del IPEN o personas con paquetes que fueran dejados de manera extraña cerca de las instalaciones del IPEN, deberá verificar la posible existencia de un artefacto explosivo.

- 6.7.2 Dispondrá las recomendaciones de seguridad en coordinación permanente con el Especialista DNSF de la Sede donde se registre la emergencia; a fin de mantener la calma, impedir que alguna persona se acerque al artefacto o paquete sospechoso y evacuar la zona de peligro identificada.

- 6.7.3 Solicitará la intervención de la fuerza de respuesta en la Sede correspondiente; asimismo comunicará a la Unidad de Desactivación de Explosivos (UDEX) de la Policía Nacional para su asistencia inmediata dándole la descripción de los hechos.

- 6.7.4 Administrará el sistema de seguridad electrónica para que las imágenes de los hechos queden registradas y sirvan para el esclarecimiento del delito a las autoridades policiales, debiendo registrarse en la carpeta de "Ocurrencias Relevantes" del servidor NAS e informará a la Alta Dirección de la emergencia.

6.8 Del personal CAS ante situaciones de incendio

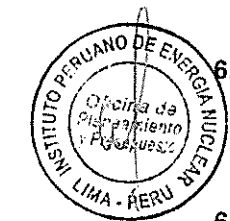
- 6.8.1 De acontecer un amago de incendio el operador de turno del CAS, registrará su ubicación y lo comunicará al personal de brigadas contra incendio y/o agentes SIF de las Sedes IPEN, a fin emplear adecuadamente los equipos de lucha contra incendio tales como extintores, gabinetes, etc.

- 6.8.2 De suscitarse un incendio en cualquiera de las Sedes del IPEN, solicitará de forma inmediata la presencia del personal del Cuerpo General de Bomberos Voluntarios del Perú y Policía Nacional del Perú; a su vez se comunicará con el Especialista DNSF, a fin de salvaguardar vidas humanas y los bienes de la institución.

- 6.8.3 Administrará el sistema de seguridad electrónica para que las imágenes de los hechos queden registradas y sirvan para su esclarecimiento, a las autoridades policiales y Cuerpo General de Bomberos Voluntarios del Perú, debiendo archivarse en la carpeta de "Ocurrencias Relevantes" del servidor NAS e informará a la Alta Dirección sobre los hechos y acciones tomadas durante la emergencia.

6.9 Del personal CAS ante situaciones de sismo

- 6.9.1 De acontecer un sismo el operador de turno del CAS coordinará con los Jefes de brigada y personal de agentes SIF las recomendaciones de seguridad para la normalización de las actividades.



	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 11 de 13

6.9.2 De ser necesaria la evacuación de heridos, personas atrapadas y/o fallecidos, solicitará el apoyo de la Policía Nacional del Perú, Cuerpo General de Bomberos Voluntarios del Perú e INDECI.

6.9.3 Administrará el sistema de video vigilancia y verificará las imágenes con los responsables de las diferentes Sedes del IPEN, a fin de registrar las consecuencias de los hechos y archivarlas en la carpeta de "Ocurridos Relevantes" del servidor NAS, de tal manera que sirvan para la actualización de los planes de respuesta y levantamiento de información real para Alta Dirección.

7 RESPONSABILIDADES

7.1 El especialista de DNSF es responsable de la administración, funcionamiento, operatividad, supervisión y control del Sistema de Seguridad Electrónica; asimismo, es responsable del manejo y gestión del programa de mantenimiento de los equipos de seguridad física, gestionando la asignación presupuestal para dicho fin.

7.2 Los Directores de los Órganos del IPEN aseguran la implementación y cumplimiento de la presente Directiva en las Unidades a su cargo, bajo responsabilidad.

8 DISPOSICIONES FINALES Y COMPLEMENTARIAS

8.1 El Sistema de Seguridad Electrónica del IPEN, será implementado de manera integrada como un componente del sistema de seguridad física nuclear, para la protección física de las instalaciones nucleares, radioactivas y administrativas, en cumplimiento de la normativa nacional e internacional.

8.2 La Alta Dirección del IPEN y el Especialista de DNSF podrán tener acceso en tiempo real al sistema de visualización remota, para una oportuna información y toma de decisiones.

8.3 Los Directores y Jefes de los Órganos del IPEN, que por razones de emergencia lo soliciten, podrán tener acceso solo al sistema de visualización en las Salas de monitoreo de DNSF.

8.4 Secretaria General en coordinación con DNSF, asegurará anualmente la provisión de recursos presupuestales para el mantenimiento del sistema de Seguridad Electrónica, las licencias de los programas de administración de datos, así como el pago de canon de uso del espectro radioeléctrico.

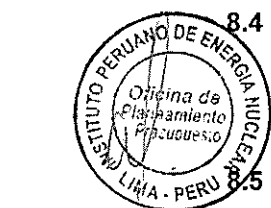
8.5 Para acceder a la información y reproducción de imágenes, videos o audios, se solicitará a Secretaría General.

8.6 No se deben captar imágenes, videos o audios de viviendas cercanas, baños, espacios de aseo, vestidores, zonas de descanso, entre otros espacios protegidos por el derecho a la intimidad y determinados por la Autoridad Nacional de Protección de Datos Personales (APDP). En caso fueran captadas dichas imágenes, se dará inicio a las sanciones administrativas, civiles o penales según corresponda.

9 ANEXOS

9.1 Anexo N° 01: "Estándares técnicos para cámaras de video vigilancia"

9.2 Anexo N° 02: "Proceso de Funcionamiento y Operación del Sistema de Seguridad Electrónica del IPEN"

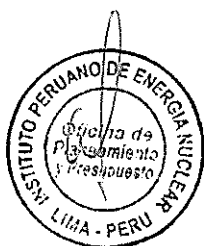


	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 12 de 13

ANEXO N° 01

ESTANDARES TÉCNICOS PARA CÁMARAS DE VIDEO VIGILANCIA

CÁMARA TIPO I: CÁMARA IP DOMO PTZ PARA EXTERIORES	CÁMARA TIPO II : CÁMARA IP FJA TIPO CAJA PARA EXTERIORES	CÁMARA PTZ. DE LARGO ALCANCE	CÁMARA PARA APLICACIONES ESPECIALES
Aplicación: Vigilancia de principales parques, plazas, intersecciones de principales avenidas	Aplicación: Vigilancia de pasajes, accesos peatonales y vehiculares en principales escenarios, monumentos históricos y edificaciones considerados patrimonio cultural.	Aplicación: Vigilancia de principales avenidas, plazas y centros de concentración de flujo masivo de personas y vehículos.	Aplicación: Cámaras de 5 megapixel, 20 megapixel o superior de uso especial, para zonas de muy alta densidad y necesidad de identificación visual.
Requisitos técnicos mínimos:	Requisitos técnicos mínimos:	Requisitos técnicos mínimos:	Requisitos técnicos mínimos:
Alcance de zoom: Óptico 30 X o superior, digital 10X	Resolución. 2 MP o 30 fps	Alcance de zoom motorizado: Óptico 100X o superior, zoom digital 12X	Sensor CMOS progresivo
Resolución: 2MP a 30fps	Resoluciones 1080p: 1920 x 1080 píxeles, 720p: 1280 x 720 píxeles, D1: 720 x 486 píxeles	Resolución 30 fps	Píxeles activos: (H x V) 20 MP (5120 x 3840)
Resoluciones 1080p: 1920x1080 píxeles, 720p: 1280x720 píxeles, D1: 720x486 píxeles	Multi stream de video ilimitadas conexiones multicast, mínimo dos conexiones unicast	Resoluciones 700TVL ó 1600 x 1200	Resolución horizontal > 3000 LTV
Multistream de video; limitadas conexiones multicast, mínimo 2 conexiones unicast	Compresión de video: H.264 (ISO 14496-10)	Lente 17- 2000 mm (22"-0 18" VAF0) sin accesorios externos adicionales	Sensibilidad mínima sólo de día: 0.01 lux (color). 50 iRE, F1.0 obturador 1/30 s
Compresión de video: AAC-LC (ISO 14496-3)	Compresión de audio: AAC-LC (ISO 14496-3)	Sensor CMOS	Rango dinámico 66 dB
Rango dinámico WDR	Rango dinámico WDR	Iluminador: Alcance efectivo :1000 mts	Control de ganancia: Automático/manual
Día/noche; automático y contar un mecanismo para remover el filtro IR	Día/noche; automático y contar un mecanismo para remover el filtro IR	Día/noche; automático	Modo de balance de blancos: Automático/manual, día y noche, sólo de día
Modo de balance de blancos automático	Modo de balance de blancos automático	Modo de balance de blancos automático	Resolución de video 5120 x 3840 píxeles (5k) + 1280 x 960 píxeles (960p)
Control de iris automático	Control de iris automático	Compensación de luz de fondo automático	Opciones de lentes: Variedad de longitudes focales, suministrado con filtro UV e IR
Compensación de luz de fondo automático	Compensación de luz de fondo: automático	Humedad de funcionamiento: <90% sin condensación	Control de exposición automático/manual
Tasa de transmisión (Bit Rate) configurable por el usuario	Tasa de transmisión (Bit Rate): Configurable por el usuario	Calentador/Ventilador incorporado	Compresión de video: Descripción de formato JPEG2000 de Ultra 5k y compresión H.264 HD.
Entradas y salidas binarias: Mínimo 1 entrada y 1 salida	Entradas y salidas binarias: Mínimo 1 entrada y 1 salida	Limpiaparabrisas incorporado	Potencia de procesamiento de video: 120 megapíxeles/segundo
Audio full dúplex	Audio full dúplex	Presets: 80	Velocidad de bits de video: Hasta 100 Mbps
Interfaz de red estándares: IEEE 802.3 y ETF: 10/100 Base-T Ethernet	Interfaz de red: Estándares IEEE 802.3 y IETF: 10/100 base-T Ethernet	Rango de movimiento horizontal: 360° continuo	Codificador múltiple de video: JPEG 2000, Resolución individual H.264
Presets: 250	Análisis de video: soportar contraflujo, congestión, parqueo en zonas prohibidas, detección de movimiento y análisis inteligente	Rango de movimiento vertical 75° a 75°	Estándar-integración: Arquitectura abierta ONVIF.
Rango de movimiento horizontal: 360°	Rango de Protección: IP 66	Velocidad de movimiento horizontal vertical 0.01 a 30°/s y 15°/s	
Rango de movimiento vertical 90°	Rango de temperatura: 20°C - 50°C	Rango de protección: IP66	
Velocidad movimientos: Horizontal y vertical 360°/s	Estándar-integración: Arquitectura abierta: ONVIF	Rango de temperatura: -40°C a 65°C	
Velocidad de preset 200°/s		Conectividad: Puede ser nativa IP o una cámara analoga conectada a un codificador	
Rango de protección: IP66 (IEC 62262)			
Rango de temperatura: 20°C a 50°C			
Estándar-integración: Arquitectura abierta ONVIF			



	DIRECTIVA	DIR-003-IPEN/SEGE
	PARA EL FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL INSTITUTO PERUANO DE ENERGÍA NUCLEAR	Versión N° 01
		Página de 13 de 13

ANEXO N° 02

PROCESO DE FUNCIONAMIENTO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA DEL IPEN

