



**INSTITUTO DE EDUCACIÓN
SUPERIOR PRIVADO
INSUR**

**PLAN DE SEGURIDAD Y
VIGILANCIA
INSTITUCIONAL**

2026 – 2032

Presentación

Las instituciones educativas tienen la responsabilidad y obligación de garantizar la seguridad tanto de los estudiantes como del personal, docente y no docente, y de otros usuarios que frecuentan la institución. Para ello deben mejorar las condiciones, garantizando la seguridad de los miembros de la comunidad educativa, mediante la eliminación de riesgos o reduciendo su probabilidad.

El Plan de Seguridad y Vigilancia Institucional (en adelante, el plan) es un instrumento de planeamiento que permite al Instituto de Educación Superior INSUR (en adelante, IES INSUR) planificar acciones para disminuir las vulnerabilidades e incrementar la capacidad de respuesta ante posibles amenazas, o reducir su probabilidad, brindando el resguardo, seguridad y protección a los miembros de la comunidad educativa, coadyuvando a una adecuada prestación del servicio educativo.

El presente plan establece directrices claras para la vigilancia constante y constituye una herramienta integral para la planificación y ejecución de acciones de seguridad que abarquen los diferentes escenarios a los que se enfrenta una institución.

Plan de Seguridad y Vigilancia Institucional

I. FINALIDAD

El plan de seguridad y vigilancia institucional del IES INSUR tiene por finalidad garantizar la integridad física, psicológica y material de los miembros de la comunidad educativa.

II. ALCANCE

El plan es de cumplimiento obligatorio para todos los miembros de la comunidad educativa del IES INSUR, que interactúan en la sede administrativa, independientemente de su dirección, cargo o nivel jerárquico. Incluye también a estudiantes, docentes y visitantes durante sus visitas ocasionales, garantizando un entorno seguro en la sede en mención.

III. BASE LEGAL

El plan tiene como marco legal las siguientes normas y documentos de gestión del IES:

- Ley N° 28851, “Ley que establece la obligación de elaborar y presentar planes de contingencia”
- Decreto Supremo N° 058-2014-PCM “Reglamento de Inspecciones Técnicas de Seguridad en Edificaciones”
- La Constitución Política del Perú.
- Ley General de Educación N° 28044 y su reglamento.
- Ley N° 29988, “ Ley que establece medidas extraordinarias para el personal docente y administrativo de instituciones educativas públicas y privadas, implicado en delitos de terrorismo, apología del terrorismo, delitos de violación de la libertad sexual y delitos de tráfico ilícito de drogas; crea el Registro de personas condenadas o procesadas por delito de terrorismo, apología del terrorismo, delitos de violación de la libertad sexual y tráfico ilícito de drogas y modifica los artículos 36 y 38 del Código Penal” y su reglamento.
- Ley N° 30512: Ley de Institutos y Escuelas de Educación Superior y de la Carrera Pública de sus Docentes y su reglamento.
- Ley N° 29783, Ley de Seguridad y Salud en el Trabajo y su reglamento.
- Resolución Viceministerial N° 103-2022-MINEDU que aprueba el Documento Normativo de las Condiciones Básicas de Calidad para los Institutos de Educación Superior y las Escuelas de Educación Superior Tecnológica.
- Resolución Viceministerial N° 049-2022-MINEDU, que actualiza los “Lineamientos Académicos Generales para los Institutos de Educación Superior y las Escuelas de Educación Superior Tecnológica”.
- Reglamento Interno INSUR
- PEI INSUR

IV. OBJETIVO

Objetivo Estratégico PEI

Desarrollar acciones de acompañamiento, supervisión y mejora continua en la gestión pedagógica e institucional para garantizar el uso adecuado de los recursos y el funcionamiento de los servicios que brinda el IES.

Objetivo del Plan.

Establecer los mecanismos y protocolos de seguridad específicos para la sede administrativa, orientados a garantizar la protección de la salud física y psicológica de cada miembro de la comunidad educativa, así como la seguridad de los recursos materiales, financieros, patrimoniales y tecnológicos del IES, siendo esta última relevante para la modalidad del servicio educativo.

Objetivos específicos:

- a. Identificar los riesgos físicos, de salud, psicológicos y/o materiales de la comunidad educativa y del público durante su estancia en la sede administrativa.
- b. Elaborar y difundir procesos, procedimientos y/o protocolos para atender tanto las medidas de protección y prevención de incidentes, como su aplicación.
- c. Establecer el mecanismo de identificación en el IES de estudiantes, docentes, trabajadores¹ y público en general.
- d. Generar actividades de capacitación y/o fortalecimiento y/o entrenamiento para los miembros de la comunidad y en especial para el personal de seguridad y vigilancia.
- e. Garantizar la seguridad y vigilancia de la infraestructura física y equipamiento del IES.
- f. Implementar medidas de seguridad informática para proteger los recursos informáticos y los datos del instituto.

V. LINEAMIENTOS PARA LA SEGURIDAD Y VIGILANCIA

Lineamientos para la seguridad y vigilancia de la infraestructura física

El presente plan establece lineamiento para que el personal de seguridad realice sus labores, las ejecute en la sede administrativa del IES, que incluye el ingreso al local hasta el cuidado de los ambientes del IES.

- *Del horario*
El horario del personal de seguridad y vigilancia del IES se brinda durante el servicio educativo que comprende de 8:00 am – 1:00 pm y de 3:00pm - 10:00 pm
- *Del ingreso del personal*
El personal de seguridad y vigilancia asignado en portería solicita el DNI al personal, cuando considere necesario y en especial a personas que no conozca como miembro del personal del IES.

El personal en mención no permitirá el ingreso a la sede administrativa del personal que se encuentre bajo efectos del alcohol o de alguna sustancia psicoactiva.

El personal en mención comunicará previamente a la Dirección Administrativa el ingreso de contratistas y proveedores.

¹ Los trabajadores hacen referencia al personal administrativo.

- *Del ingreso y salida de estudiantes y/o visitantes individuales*

El personal de seguridad y vigilancia solicitará al visitante información del área u oficina donde se dirige, junto con la información del documento de identidad y la hora de ingreso, debiendo ser registradas en el cuaderno de control de ingreso de visitas.

El personal en mención reporta vía telefónica (celular) a la secretaria Académica, para que pueda bajar a portera y conducir al visitante a la sede principal y ser atendido.

Culminada la visita la secretaria Académica deberá conducir al visitante a la puerta principal para que registre en portería su salida del campus.

- *Del ingreso y salida de bienes muebles ajenos a la institución*

El personal de seguridad y vigilancia controlará el ingreso de bienes muebles ajenos a la institución, cuando estos son ingresados por el personal, debiendo ser anotados en el cuaderno de control de ocurrencias las características del bien.

A la salida de los bienes muebles por parte del personal, deberá hacer constar la hora de salida y corroborar que los bienes muebles que están saliendo son los mismos que han ingresado.

- *Objetos y/o documentos perdidos*

Cuando algún miembro del personal que labora en la sede institucional encuentre un objeto o documento, no teniendo conocimiento de su propietario, deberá de entregarlo al personal de seguridad y vigilancia, quien debe reportar la secretaria Académica del Instituto y registrar en el cuaderno de incidencias, para luego hacer el seguimiento y entrega al propietario previo cruce de información.

- *Otros lineamientos para el ingreso a la sede administrativa*

No se permitirá el ingreso de: i) mascotas, iii) armas y municiones u otros elementos para su fabricación, uso y comercialización; iii) otras cosas que pongan en riesgo al personal o bienes institucionales.

Lineamientos de seguridad y vigilancia de la infraestructura tecnológica (entorno virtual y herramientas digitales)

A través de este plan se busca garantizar la integridad, confidencialidad y disponibilidad de la información, así como la protección la privacidad de los usuarios, para ello se considera lo siguiente:

- Se hace un diagnóstico y evaluación de los riesgos para encontrar una posible amenaza y vulnerabilidad en el entorno virtual de aprendizaje y de herramientas digitales
- Se establecen políticas claras relacionadas con la seguridad y privacidad de los entornos virtuales de aprendizaje
- Se asegura que los usuarios informados cumplan con las políticas establecidas
- Se Implementa un sólido sistema de autenticación para garantizar que solo usuarios autorizados tengan acceso a los recursos.
- Se utiliza un cifrado para proteger la información sensible y los datos transmitidos a través de la plataforma
- Se mantiene actualizados todos los sistemas y software utilizados en el entorno virtual para abordar vulnerabilidades conocidas.

- Se establece procedimientos de respaldo regular para garantizar la disponibilidad y la recuperación de datos en caso de pérdida o daño.

Lineamientos de seguridad frente a los riesgos físicos, de salud, psicológicos y/o material.

Se establecen e identifican problemas de seguridad que ponga en riesgo aspectos físicos, de salud, psicológicos del personal en la sede administrativa, y se implementan protocolos de atención frente a los riesgos identificados. De la misma manera con respecto a riesgos materiales.

El personal del IES, vinculado a los servicios de atención al estudiante, estarán al servicio de atención de problemas u ocurrencias de índole de salud y psicológicos.

De ser necesario se hará coordinaciones con otras instituciones de seguridad o salud.

VI. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS

IDENTIFICACIÓN DE RIESGOS

Se identifican y evalúan los tipos de riesgo físicos, psicológicos, salud y materiales que podrían afectar al personal administrativo de la sede y a los estudiantes, docentes y visitantes durante sus visitas ocasionales.

La sede administrativa dispone de instalaciones y equipos para la prevención de incendios, incluyendo extintores, señalizaciones, luces de emergencia y detectores de humo, entre otros.

Con el fin de proporcionar un mayor conocimiento al personal de seguridad y facilitar la identificación rápida de las propiedades a atender, se presenta a continuación los tipos de riesgos que podrían presentarse en las instalaciones del IES.

6.1. Infraestructura física

- Intrusiones no autorizadas: las áreas administrativas pueden ser vulnerables a intrusiones de personas no autorizadas, lo que podría resultar en el robo de equipos, documentos confidenciales o información sensible.
- Acceso no autorizado a sistemas informáticos: si los sistemas no están bien protegidos, existe el riesgo de que individuos malintencionados puedan acceder de forma no autorizada a datos sensibles o comprometer la seguridad de la red de la empresa.
- Suplantación de identidad: los sistemas de identificación y acceso pueden ser vulnerables a la suplantación de identidad, lo que podría permitir a las personas no autorizadas ingresar a áreas restringidas y acceder a información confidencial.
- Vulnerabilidades en sistemas de seguridad electrónica: los sistemas de seguridad electrónica, como cámaras de vigilancia o sistemas de alarma pueden ser vulnerables a hackeos o manipulaciones, lo que comprometería la capacidad de monitorear y proteger las instalaciones del IES.
- Fugas de información confidencial: los empleados pueden ser susceptibles a cometer errores o actuar de manera negligente, lo que podría resultar en la

divulgación no autorizada de información confidencial a personas no autorizadas.

- Fraude interno: Los empleados pueden estar involucrados en actividades fraudulentas, como el robo de activos de la empresa, o el mal uso de información confidencial para beneficio personal.

6.2. Infraestructura tecnológica

- Violaciones de la privacidad de los datos: Los sistemas de información utilizados para servicios educativos en línea almacenan información personal y confidencial de los estudiantes, como nombres, direcciones de correo electrónico, y en algunos casos, datos financieros. Las violaciones de seguridad podrían resultar en la filtración o robo de esta información, lo que podría llevar a graves consecuencias legales y dañar la confianza del estudiante en la plataforma.
- Ataques de piratería informática: Las plataformas educativas en línea son blancos atractivos para los piratas informáticos que buscan acceder ilegalmente a los datos de los estudiantes o interrumpir el servicio. Los ataques pueden incluir ransomware, phishing, ataques de denegación de servicio (DDoS) u otros métodos de intrusión.
- Acceso no autorizado: La falta de controles de acceso adecuados puede permitir a personas no autorizadas ingresar a la plataforma educativa y acceder a información sensible, como calificaciones, exámenes y registros estudiantiles. Esto podría resultar en el robo de identidad, fraude académico o manipulación de datos.
- Falta de seguridad en las contraseñas: Las contraseñas débiles o compartidas pueden comprometer la seguridad de los sistemas de información, permitiendo a los atacantes acceder fácilmente a cuentas de estudiantes, profesores o la secretaría académica.
- Falta de actualizaciones de seguridad: No mantener actualizados los sistemas y aplicaciones con los últimos parches de seguridad puede dejar a la plataforma educativa vulnerable a las amenazas de seguridad conocidas. Los atacantes a menudo buscan explotar vulnerabilidades conocidas en sistemas desactualizados.

6.3. Eventos naturales

- Sismo: la actividad sísmica en el Perú ocurre en todo el territorio y es debida principalmente al proceso de subducción de la placa de Nazca bajo la placa Sudamericana. El margen continental oeste de Sudamérica es uno de los más activos y de los bordes de placa el mayor en la Tierra. Expertos geólogos peruanos señalan que la costa peruana tiene una acumulación de energía por silencio sísmico mayor a 300 años, y que se esperan sismos de hasta 8.5 grados de magnitud. El Mapa de Acoplamiento Físico publicado por el Instituto Geofísico del Perú en el año 2021, muestra las zonas más vulnerables de la costa peruana para que ocurra alguno de esos sismos, estando Tacna entre dichas zonas identificadas

- Inundación: las primeras manifestaciones adversas por la temporada de lluvias (noviembre a abril) se registran en las viviendas afectando directamente la infraestructura de edificaciones, así como de cualquier otro tipo de construcción. Otro es el deterioro de carreteras y puentes, ocasionando en algunos casos el aislamiento. Las inundaciones pueden ocasionarse por los aludes conocidos como “huaicos”.

6.4. Acción humana

- Asalto o robo: vulneración del patrimonio de la sede administrativa por la ocurrencia de actividades ilícitas, como robos, hurtos, intercambio de equipos. Asimismo, es probable la ocurrencia de actos de falsificación de documentos, venta de drogas y delitos en contra de la vida y salud de las personas.
- Hostigamiento sexual: son formas de violencia a través de una conducta de naturaleza o connotación sexual o sexista no deseado por la persona contra la que se dirige, la cual crea un ambiente intimidatorio, humillantes u hostil; o que se puede afectar su actividad o situación laboral, docente, formativa o de cualquier otra índole.

6.5. Material

- Accidentes de equipos: situaciones derivadas del mal uso de equipamiento, mobiliario o la experiencia en manipular tecnología en la sede administrativa. Estos accidentes pueden involucrar caídas, cortes o heridas, lo cual debe ser atento y derivado según el protocolo de emergencia establecido.
- Explosión: las explosiones pueden ocurrir en la sede administrativa debido a fallos en los equipos electrónicos o sistemas de aire acondicionado, acumulación de gases inflamables o mal manejo de materiales peligrosos. Este riesgo debe ser mitigado con mantenimiento preventivo y control de acceso a áreas restringidas.
- Incendio: riesgo de incendio en la sede administrativa debido a fallos eléctricos o manejo inadecuado de materiales inflamables. Las medidas de prevención y atención incluyen instalaciones de extintores y detectores de humo, además de capacitación al personal sobre el uso de los mismo.

6.6. Psicológico

- Estados psicológicos: los estados emocionales adversos, como el estrés, la ansiedad o la depresión pueden afectar el desempeño del personal administrativo. En el ambiente laboral puede darse la sobrecarga laboral, dificultades personales o el uso de sustancias nocivas. Es esencial abordar estos riesgos mediante el programa de bienestar laboral, apoyo psicológico y monitoreo del trabajo para prevenir impactos negativos en el desarrollo del personal administrativo.

6.7. Salud

- Enfermedades virales: frente a pandemia o enfermedades virales declaradas por los organismos gubernamentales de salud, el IES tomará las recomendaciones que se den frente a ello para el personal administrativo infectado.

EVALUACION DE RIESGOS

Se presenta una matriz con cinco (05) niveles de evaluación para el impacto, todas siguiendo una escala de bajo a alto, la cual permite hacer la evaluación de riesgo. Además, puede servir como herramienta complementaria para evaluar los posibles daños y perturbaciones provocadas por los riesgos.

	IMPACTO ¿Qué tan severos serían los resultados si ocurriera el riesgo?					
		Insignificante 1	Menor 2	Significativo 3	Mayor 4	Severo 5
PROBABILIDAD ¿Cuál es la probabilidad de que ocurra el riesgo?	Casi seguro 5	Medio 5	Alto 10	Muy alto 15	Extremo 20	Extremo 25
	Probable 4	Medio 4	Medio 8	Alto 12	Muy alto 16	Extremo 20
	Moderado 3	Bajo 3	Medio 6	Medio 9	Alto 12	Muy alto 15
	Poco probable 2	Muy bajo 2	Bajo 4	Medio 6	Medio 8	Alto 10
	Raro 1	Muy bajo 1	Muy bajo 2	Bajo 3	Medio 4	Medio 5

En relación a lo anterior se presente la evaluación de impacto de los riesgos presentados:

a. Los riesgos de muy bajo impacto son:

- falta de actualizaciones de seguridad
- sismos
- inundaciones

b. Los riesgos de bajo impacto son:

- intrusiones no autorizadas
- acceso no autorizado a sistemas informativos
- suplantación de identidad

- vulnerabilidad en sistema de seguridad electrónica
- accidente de equipos
- estados psicológicos
- salud

c. Los riesgos de medio impacto son:

- fugas de información confidencial
- violación a la privacidad de datos
- ataques de piratería informática
- acceso no autoriza
- explosión
- incendio
- índole ilícitos

d. Los riesgos de alto impacto son:

- hostigamiento sexual

VII. DESCRIPCIÓN DE PROCESOS, PROCEDIMIENTOS Y PROTOCOLOS

7.1. Interacción con el público y la comunidad educativa

El IES INSUR cuenta en su estructura orgánica con un responsable del servicio de seguridad y vigilancia, para velar el cumplimiento de los procesos, protocolos y procedimientos de atención.

7.1.1. Seguridad en la interacción presencial

En el caso de la interacción presencial, la sede administrativa contará con personal capacitado para atención al público, así como las instalaciones necesarias para cumplir con esta labor de orientación y de guía para quienes deseen tomar nuestros servicios y/o solo requieran. La existencia del personal es parte de la estructura orgánica del IES, y, por tanto, para todo el periodo de licencia institucional.

Protocolo para visitantes:

- Los visitantes deberán identificarse al momento de su ingreso mediante algún documento válido en el país de emisión, y que esté vigente. El documento

quedará en posesión del Servicio de Seguridad y Vigilancia en tanto dure la visita.

- Deberán dirigirse exclusivamente al área solicitada, teniendo acceso a los servicios higiénicos disponibles en zonas comunes. En caso de necesitar visitar un área no solicitada al ingresar, deberá hacerlo acompañado del personal de seguridad de la institución.
- En caso el visitante porte mochila, maletín o algún accesorio similar, éste deberá ser revisado al ingreso y a la salida de la sede. En caso el visitante porte algún equipo tecnológico, o algún otro bien de alto valor, deberá reportarlo al momento de ingresar.
- El Servicio de Seguridad y Vigilancia se comunicará con el área solicitada, brindando la información del visitante.
- El personal de la institución atenderá la visita en orden de llegada, debiendo considerar un máximo de 05 minutos para agotar las necesidades del visitante. En caso se requiera de más tiempo (excepcionalmente), se deberá comunicar al personal de seguridad.
- El personal del área solicitada dejará registrada la visita: nombre completo, documento de identificación, procedencia, motivo de la visita, nombre de quién atendió la visita, descripción breve de la atención brindada, observaciones.

Protocolo para estudiantes que acudan a la sede administrativa

- Los estudiantes oficiales de la institución estarán en una base de datos, por lo que al hacer ingreso a la sede administrativa serán identificados de manera inmediata.
- En caso el estudiante porte mochila, maletín o algún accesorio similar, éste deberá ser revisado al ingreso y a la salida de la sede administrativa. En caso el estudiante porte algún equipo tecnológico, o algún otro bien de alto valor, deberá reportarlo al momento de ingresar.
- El estudiante tendrá acceso al área solicitada, y dispondrá hasta un máximo de 10 minutos para agotar el motivo de la visita. En caso se requiera de más tiempo para su atención, el personal de la sede deberá comunicarlo a la garita de seguridad.
- El estudiante deberá evitar compañía ajena a la sede administrativa.
- El estudiante deberá abandonar la sede institucional una vez que haya culminado el propósito de su visita.

En el caso de la interacción a distancia, la institución cuenta con una página web oficial, además de contar con presencia en las principales redes sociales para facilitar el acceso a la información de parte de los interesados. En el caso de la comunicación institucional virtual, la institución cuenta con personal capacitado para la interacción a distancia, brindando la información que la comunidad requiera.

Sólo se hará uso de las redes sociales oficiales de la institución y/o alguna de las

plataformas habilitadas para dichos fines

La comunicación con el personal de la institución deberá ser exclusivamente para los temas relacionados a intereses comunes de la comunidad educativa (asuntos académicos, administrativos, situaciones excepcionales que la institución deba conocer).

7.1.2. Seguridad en el servicio educativo a distancia

- i. Procesos vinculados a la seguridad del servicio educativo a distancia
 - Seguridad de la plataforma educativa
 - Protección de la privacidad y los datos personales
 - Prevención de ciberataques y fraudes
- ii. Procedimientos vinculados a la seguridad del servicio educativo a distancia.

Seguridad de la Plataforma Educativa:

- Selección de Plataforma Confiable: Seleccionar una plataforma educativa segura y confiable que cumpla con los estándares de protección de datos y privacidad.
- Actualización y Mantenimiento: Realizar actualizaciones periódicas de la plataforma para corregir posibles vulnerabilidades y garantizar su funcionamiento óptimo.
- Autenticación Segura: Implementar medidas de autenticación segura, como contraseñas robustas y autenticación de dos factores, para proteger el acceso de los estudiantes y el personal.
- Respaldo de Datos: Establecer procedimientos de respaldo regular de los datos para prevenir la pérdida de información y garantizar la continuidad del servicio en caso de incidentes.

Protección de la Privacidad y los Datos Personales:

- Política de Privacidad Transparente: Elaborar y comunicar claramente una política de privacidad que detalle cómo se recopilan, almacenan y utilizan los datos personales de los estudiantes y el personal.
- Consentimiento Informado: Obtener el consentimiento informado de los estudiantes y el personal para el procesamiento de sus datos personales de acuerdo con la normativa de protección de datos aplicable.
- Encriptación de Datos: Utilizar técnicas de encriptación para proteger la confidencialidad de la información transmitida a través de la plataforma educativa, como datos de identificación personal y registros académicos

Prevención de ciberataques y fraudes:

- Firewalls y Antivirus: Implementar firewalls y software antivirus actualizados para detectar y prevenir intrusiones maliciosas en la plataforma educativa.
- Detección de Intrusiones: Establecer sistemas de detección de intrusiones que monitoreen continuamente la actividad en la plataforma y alerten sobre posibles amenazas de seguridad.
- Capacitación en Seguridad Cibernética: Brindar capacitación regular

al personal y a los estudiantes sobre buenas prácticas de seguridad cibernética, como el reconocimiento de correos electrónicos de phishing y la protección de contraseñas.

- iii. Protocolos de atención a incidentes de seguridad
 - Protocolo de Respuesta a Incidentes: Desarrollar un protocolo claro y eficiente para responder a incidentes de seguridad, que incluya la notificación rápida a las partes afectadas y la coordinación con las autoridades pertinentes.
 - Registro y Reporte de Incidentes: Mantener un registro detallado de los incidentes de seguridad ocurridos en la plataforma educativa, incluyendo la naturaleza del incidente, las acciones tomadas y las lecciones aprendidas.
 - Evaluación Post-Incidente: Realizar una evaluación post- incidente para identificar las causas subyacentes del incidente y tomar medidas correctivas para evitar su recurrencia.

7. 2. Control de bienes

Para un correcto control de bienes, se elabora un inventario de bienes utilizados tanto por los docentes para desarrollar sus clases virtuales como los administrativos para la prestación y soporte de las clases virtuales.

Protocolo para el traslado externo de bienes

- El personal encargado del traslado de algún bien hacia los exteriores de la sede deberá llenar un formato de traslado de bienes que será autorizado por el Coordinador Administrativo.
- El formato deberá contener información básica: lugar de destino, responsable del traslado, motivo del traslado, tiempo para el retorno, fecha y hora de salida y de retorno, además de un bloque de observaciones para cualquier eventualidad excepcional que pueda ocurrir.
- Posterior al retorno, el personal responsable deberá poner en operatividad el equipo o bien trasladarlo en presencia del personal de seguridad, verificando que esté todo en orden.
- En caso de haberse dado alguna eventualidad, deberá informarse a la Coordinación Administrativa y proceder de acuerdo a lo que este despacho disponga.

Protocolo para el traslado interno de bienes

- En el caso de darse la necesidad de trasladar algún bien inventariado dentro de la sede, este cambio deberá documentarse y ser comunicado a la secretaria Académica para la actualización correspondiente del inventario vigente.
- El traslado deberá quedar registrado en un formato con información básica: lugar de destino, responsable del traslado, motivo del traslado, tiempo para el retorno, fecha y hora de salida y de retorno, además de un bloque de observaciones para cualquier eventualidad excepcional que pueda ocurrir.

7.3. Control de acceso y espacios

La sede administrativa contará con un sistema de circuito cerrado, monitoreado por el Área de redes y Conectividad. Asimismo, el Servicio de Seguridad y Vigilancia hará un control y registro de visitantes a la sede administrativa (véase la sección 7.1).

La sede administrativa cuenta con espacios denominados “Sala de Reuniones”, los cuales son destinados para que los docentes impartan las clases sincrónicas. Éstas se encuentran equipadas con equipos y mobiliario y conexión a internet para el desarrollo de las clases sincrónicas. Los docentes a través de los usuarios asignados por la institución, deben acceder a los entornos virtuales y plataformas dispuestas por la institución para el proceso de enseñanza- aprendizaje.

Por otro lado, cada estudiante a través de los entornos virtuales para el aprendizaje dispuestos por la institución, y con sus correos institucionales, accede a las clases sincrónicas y recursos dispuestos para tal fin. Para ello el estudiante debe:

- Acceder con su usuario y contraseña
- Ingresar a la sesión de clase de su unidad didáctica
- Utilizar el micrófono, hacer click en permitir.
- Utilizar la cámara, hacer click en permitir.
- Para no interrumpir el normal desarrollo de las clases sincrónicas el micrófono debe permanecer apagado. Sólo cuando el docente solicite su participación debe encenderlo.
- Cuando el estudiante desea realizar alguna consulta o intervenir en la clase debe mostrar la reacción “mano levantada” y esperar el pase del docente.

8.4. Actuaciones en situaciones especiales (actividad ilícita, hostil, entre otras)

8.4.1. Acoso en entornos educativos y laborales

El acoso se entiende como cualquier comportamiento intencionado y reiterado de hostigamiento, maltrato verbal, físico, psicológico o virtual (cyberbullying), que tenga como objetivo discriminar, excluir o afectar la integridad de otra persona. Estas conductas vulneran en el derecho de la comunidad del IES a un entorno respetuoso y libre de violencia.

Acciones generales para la atención y prevención

- Fomentar el respeto mutuo y la convivencia pacífica a través de materiales educativos y campañas virtuales dirigidas a toda la comunidad educativa.
- Permitir que todas las partes involucradas en un incidente presente

Tipos de agresiones contempladas

- Verbal: insultos o expresiones hostiles
- Física: cualquier tipo de agresión directa en los espacios de la sede administrativa
- Exclusión social: actos intencionados que marginen a una persona en actividades grupales
- Cyberbullying: comportamientos agresivos mediante medios digitales, como mensajes ofensivos, difusión de información falsa o no consentida, y hostigamiento en plataformas virtuales.

Procedimientos frente al acoso

Para estudiantes

Los casos deberán ser reportados a la Dirección de Servicios al Estudiante mediante correo electrónico, detallando los hechos, de acuerdo al procedimiento establecido en el RI.

La dirección en mención analizará la situación, recopilará pruebas, y gestionará el diálogo y resolución entre las partes implicadas.

Para trabajadores:

Los incidentes serán reportados al Jefe Administrativo y el responsable psicopedagógico, quienes evaluarán el caso y elevará un informe a la Dirección General, para la resolución del mismo.

Medidas preventivas:

- Distribuir boletines virtuales dirigidos a estudiantes y personal docente y administrativo sobre temas de prevención de violencia, convivencia digital y cyberbullying.
- Incluir contenidos educativos sobre respeto y prevención del acoso en los reglamentos del IES.

8.4.2. Hostigamiento Sexual

El hostigamiento sexual se define como cualquier acción, verbal o física, de naturaleza sexual o sexista que no sea deseada ni consentida por la persona receptora. Este tipo de conducta realizada por una o más personas que aprovechan su posición de autoridad de cualquier tipo de ventaja, vulnera la dignidad y los derechos fundamentales de la víctima.

Asimismo, se considera hostigamiento sexual a aquellas conductas reiteradas, de carácter sexual o sexista, que generan un entorno intimidante, humillante u hostil, independientemente de la relación jerárquica/funcional entre las personas involucradas. Estas acciones pueden presentarse en diversos contextos y afectar de manera significativa la convivencia y el bienestar de la comunidad.

Procedimientos frente al acoso

Para estudiantes

Los casos deberán ser reportados al CIFHS mediante correo electrónico, detallando los hechos, de acuerdo al procedimiento establecido en el RI.

El comité en mención analizará la situación, recopilará pruebas, y gestionará el diálogo y resolución entre las partes implicadas.

Para trabajadores:

Los incidentes serán reportados al CIFHS, quien evaluarán el caso y elevará un informe a la Dirección General, para la resolución del mismo.

8.5. GESTION DE INCIDENTES

Entiéndase “incidentes” como cualquier situación que no configure falta o delito pero que afecta la normalidad en el desempeño de las labores institucionales. Generalmente, los incidentes se producen por malos entendidos, un mal manejo de información, por alguna mala conducta, o a causa de algún accidente sin consecuencias mayores.

En cualquiera de los casos, de darse algún incidente entre dos o más personas dentro de la sede administrativa, o de manera virtual, deberá aparecer un actor no involucrado que haga las de intermediario. Esto significará que cualquier miembro de la comunidad educativa podrá atender el incidente y ayudar a darle solución al tema, dado que, siendo un testigo ocular no involucrado, podrá aportar en la gestión de los incidentes.

El incidente debe ser reportado al personal de seguridad y vigilancia y a la Dirección General en caso se produzca alguna afectación en la integridad física de alguno de los involucrados y/o se haya ocasionado daños en el patrimonio de la institución.

A continuación, se presenta la gestión de los incidentes antes, durante y después de sus ocurrencias:

GESTIÓN EN CASO DE SISMO

ANTES DEL EVENTO	DURANTE EL EVENTO	DESPUES DEL EVENTO
- Realizar simulacros para saber cómo actuar en caso de sismos. - Se debe cuidar la señalización e identificación de las zonas seguras internas y externas, las vías y rutas de evacuación directas y seguras. - Las puertas deben abrirse fácilmente. Es preferible que las puertas tengan doble batimiento evitando que se traben. - Los corredores, pasadizos y vías de evacuación deben mantenerse libres de obstáculos. - Tener a la mano un directorio telefónico de emergencia, botiquín de primeros auxilios y radio portátil. - Conocer la ubicación y saber desactivar las llaves generales de luz y agua. - Contar con un equipo de primeros auxilios (Botiquín, camillas y otros). - Organizar, capacitar y tener formadas las brigadas de primeros auxilios y de evacuación. - Tener preparadas un mínimo de 03 mochilas de emergencias.	- Mantener la calma y trasladarse hacia zonas seguras evitando actitudes que contribuyan al pánico. - En caso de no poder salir hacia las zonas externas de seguridad, ubíquese en las zonas de seguridad internas. - Activar las brigadas de primeros auxilios y de evacuación. - Aléjese de ventanas con vidrios, de los muros, estantes y postes de luz. - Desactivar las llaves generales de luz y agua. - Utilizarán linternas a pilas para alumbrarse; nunca fósforos, velas o encendedores.	- Seguir actuando con serenidad y mantenerse alerta a posibles réplicas. - El responsable de seguridad y vigilancia dirigirá las operaciones de atención médica, control de incendios y efectuará la cuantificación de daños, para saber el número de afectados. - Utilizar radio a pilas y escuchar boletines de emergencia e informes y recomendaciones. - Las brigadas de primeros auxilios y de evacuación atenderán a los heridos y luego serán evacuados al Centro de Salud más cercano. En caso de muertes, estos deberán ser certificados por un Fiscal. - En caso de incendio se debe llamar al Cuerpo de Bomberos. - Comunicar a las autoridades del Centro de Operaciones de Emergencias Regional - COER, a fin de que evalúen los daños, dando información de las pérdidas sin exageraciones. - Se paraliza toda la actividad y el cierre temporal de las instalaciones de acuerdo a los daños sufridos por la infraestructura.

--	--	--

GESTIÓN EN CASO DE INUNDACIÓN

ANTES DEL EVENTO	DURANTE EL EVENTO	DESPUES DEL EVENTO
• Implementar infraestructura de protección externa en la sede administrativa. • Asegurar equipos y documentos en lugares adecuados. • Tener a mano el kit para emergencias. • Tener la señalización adecuada para guiar la correcta evacuación de la sede.	• Mantener la calma y trasladarse rápidamente a lugares secos y protegidos. • No caminar en espacios mojados como pasadizos, escaleras. • Desenchufar cualquier equipo tecnológico.	• No tocar ni pisar cables eléctricos. • No tomar alimentos ni comida que haya sido mojada por el agua de la inundación. • El Comité de seguridad y salud en el trabajo de desagüe y limpieza de las áreas inundadas. • Evaluar los daños generados.

GESTIÓN EN CASO INCENDIO

ANTES DEL EVENTO	DURANTE EL EVENTO	DESPUES DEL EVENTO
• Se debe identificar las zonas de riesgo y se debe de capacitar en el uso de equipos contra incendios y sobre las medidas mínimas de seguridad ante incendios. • Se debe señalar el local de acuerdo a las normas de seguridad vigentes. Asimismo, la Dirección Administrativa debe velar por la adquisición, ubicación, señalización y operatividad permanente de los extintores. • El responsable de seguridad y vigilancia es el encargado de la organización de seguridad ante la ocurrencia de desastres, lo cual propiciará la autoayuda organizada, conocedores del caos que se presente luego de un incendio. • Los corredores, pasadizos y vías de	• De ocurrir un incendio, se debe evacuar hacia las zonas externas de seguridad en forma rápida y ordenada, alejándose al menos un radio de 50 metros del local a la redonda, guiados por la Brigada de Evacuación. Asimismo, se contactará en forma inmediata al cuerpo general de bomberos. • Se priorizará la integridad de las personas. Por ningún motivo se intentará rescatar documentos y/o equipos si la vida de las personas está en riesgo. • El responsable de seguridad y vigilancia debe accionar los extintores a fin de controlar los incendios presentes. Su acción es de control hasta recibir la ayuda especializada. Si se puede y es seguro se	• El responsable de seguridad y vigilancia deberá dirigir las operaciones de búsqueda, atención médica, control de incendios y otras necesarias a quienes lo requieran dentro o fuera de las instalaciones. Asimismo, dar cuenta inmediatamente de lo sucedido a la autoridad más cercana. • La brigada de primeros auxilios se activa en forma inmediata atendiendo con los recursos de emergencia y botiquines a quienes resultaron heridos, hasta recibir la ayuda especializada y evacuar a los heridos a un centro de salud. • La brigada de evacuación ejecuta un censo inmediato de la totalidad de empleados y clientes,

evacuación deben mantenerse libres de obstáculos. • Cualquier situación de riesgo de incendio debe ser informada al responsable de seguridad y vigilancia y al Director Administrativo. • Verificar la operatividad del hidrante (grifo) contra incendios más cercano del local, se implementará progresivamente con el equipo mínimo necesario para hacer frente a la emergencia. • La institución deberá contar con una alarma que se activará de forma mecánica al presentarse un incendio	cortará la energía eléctrica y se retirará el material combustible que esté próximo, sin que afecte la integridad de las personas.	a fin de determinar quiénes faltan para iniciar su búsqueda si es que se considera seguro, usando los implementos necesarios, caso contrario deberá abstenerse de ejecutarlo informando inmediatamente a la autoridad más cercana. • En caso de haber fallecidos no deben ser movidos de la ubicación en que se encuentran, hasta que las autoridades decidan y actúen conforme a ley. • La brigada de evacuación deberá de ejecutar una evaluación de daños preliminar, a fin de proporcionar a las autoridades y bomberos la asistencia e información necesaria.
--	---	--

GESTIÓN EN CASO DE ROBO O HURTO

ANTES DEL EVENTO	DURANTE EL EVENTO	DESPUES DEL EVENTO
• Instalar el sistema de circuito cerrado y sala de control. • Implementar el equipo de seguridad de la institución. • Implementar los protocolos de control de personas, y control de bienes. • Disponer de un directorio actualizado de las instituciones de apoyo	• La intervención en flagrancia deberá ser ejecutada únicamente por el personal de seguridad, poniendo de conocimiento a la Policía Nacional del Perú de manera inmediata. • En caso de detectarse el caso por una persona que no sea del equipo de seguridad, deberá comunicarse de forma inmediata sin exponerse. • Se detiene el flujo de entrada y salida de personas en la sede administrativa.	• Reunión de evaluación de daños. • Priorización de la salud e integridad de las personas. • Determinación de responsabilidades. • Inicio de procedimientos legales que correspondan.

8.6. COORDINACIONES DE APOYO

En el IES INSUR las coordinaciones de apoyo se dan de acuerdo a las necesidades y

Página **20** de **25**

de tipo de apoyo que se requiere para gestionar emergencias de acuerdo a la situación que se presente. A continuación, se menciona las entidades con quienes se coordinará:

Coordinación de atención de emergencia

Ante cualquier accidente que afecten la salud de los estudiantes, docentes y personal administrativo.

Coordinación de apoyo psicológico

El responsable del Servicio Psicopedagógico es el encargado de brindar apoyo al personal. No obstante, para un apoyo especializado, se requiere que la persona que lo necesita acuda al especialista en el centro de salud más cercano.

Coordinación de apoyo externo

- Compañía de bomberos: ante problemas de incendios.
- Policía Nacional de la región: ante situaciones delictivas que se produzcan, o conflictos entre miembros, o denuncias de agresión física.
- Con el ministerio público frente a situaciones de hostigamiento, entre otros.

Entidad	Teléfono / Celular
Hospital Miguel A. Mariscal Llerena	(066) 309180
Compañía de Bomberos Ayacucho N°63	(066) 315827
Ministerio Público de Huamanga	939290023
Comisaría Sectorial de Huamanga	066) 49-0277

9. EQUIPO RESPONSABLE

Los responsables del plan de seguridad y vigilancia institucional son los siguientes:

- Director Administrativo
- Director de Servicios al Estudiante
- Responsable de soporte técnico
- Responsable de seguridad y vigilancia

10. ACTIVIDADES, CRONOGRAMA DE ACTIVIDADES Y PRESUPUESTO

OBJETIVOS ESPECÍFICOS	ACTIVIDADES	TAREAS	RESPONSABLE	PERIODO 2026-2032												INDICADORES	META	PRESUPUESTO
				E	F	M	A	M	J	J	A	S	O	N	D			
Identificar los riesgos físicos, de salud, psicológicos y/o materiales de la comunidad educativa y del público durante su estancia en la sede administrativa	Desarrollar medidas de diagnóstico de riesgos físicos, de salud y psíquicos.	Realizar informes de diagnósticos de riesgos	Director Administrativo	X										X	X	N° informes anuales de diagnóstico y evaluación de riesgos	1	NRP*
Elaborar y difundir procesos, procedimientos y/o protocolos para atender tanto las medidas de protección y prevención de incidentes como su aplicación.	Difusión de documentos institucionales que dictan el desarrollo de actividades para resguardar la seguridad y vigilancia de la comunidad.	Remitir mediante correo y plataforma virtual a toda la comunidad educativa el Plan de seguridad y vigilancia institucional.	Responsable de soporte técnico Responsable de Seguridad y vigilancia			X	X		X	X						N° de actividades de difusión semestrales	4	S/. 150.00
Establecer mecanismos de identificación en el IES de estudiantes, docentes, trabajadores y público en general.	Elaborar mecanismos de identificación del personal o público en general que ingresan y egresan del IES.	Distribuir carnet del instituto Registrar la solicitud de carnet de medio pasaje a los estudiantes	Director Administrativo				X			X						% de carnetización de la comunidad educativa	100%	S/. 300.00
Garantizar la seguridad y vigilancia de la infraestructura física y equipamiento del IES.	Llevar un registro de las visitas diarias a la instalación	Registrar todo ingreso al instituto	Responsable de Seguridad y vigilancia	X	X	X	X	X	X	X	X	X	X	X	X	Registro de visitas en el IES	Actas de registro de visitas	NRP*

Generar actividades de capacitación y/o fortalecimiento y/o entrenamiento para los miembros de la comunidad y en especial para el personal de seguridad y vigilancia.	Ejecutar actividades de prevención de riesgos. prevención de incendios y simulación de simulacros en materia de seguridad.	Capacitación al personal administrativo en prevención de riesgos. Realizar la capacitación en prevención de incendios. Realizar los simulacros en materia de seguridad	Responsable de Seguridad y vigilancia					X							X		% personal administrativo y estudiantil capacitado	95%	S/.200.00
	Ejecutar actividades de prevención y promoción de salud física y psicológica del personal	Realiza talleres en convivencia armoniosa, abuso, hostigamiento y cyberbullying	Director de Servicios al Estudiante					X							X		% personal administrativo y estudiantil capacitado	95%	S/.200.00
	Capacitación del personal de seguridad y vigilancia	Capacitar en materia de seguridad	Director Administrativo					X									% personal de seguridad y vigilancia	100%	S/.300.00
Implementar medidas de seguridad informática para proteger los recursos informáticos y los datos del instituto.	Supervisar la seguridad de los sistemas que utiliza el IES y las nubes de almacenamiento.	Actualizar los dispositivos de seguridad del EVA y el sistema de registro de información académica. Revisar la correlación de usuarios de los sistemas con la identidades de los miembros de la comunidad educativa.	Responsable de soporte técnico	X					X					X			N° actualizaciones de seguridad en programas	4	NRP*
TOTAL																			S/1,150

*NRP: no requiere presupuesto

11. PRESUPUESTO

	PRESUPUESTO MULTIANUAL						
	2026	2027	2028	2029	2030	2031	2032
Presupuesto	S/. 1,150	S/. 1,150	S/. 1,300	S/. 1,300	S/. 1,300	S/. 1,400	S/. 1,400