POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DEL CALLAO (En construcción, análisis y recolección de documentación).

La Universidad Nacional del Callao; reconoce el valor de la información de sus procesos para el logro de sus objetivos estratégicos, por lo que se compromete a garantizar su confidencialidad, integridad y disponibilidad, mediante la gestión de riesgos e incidentes de la seguridad de la información, así como el fortalecimiento de la cultura y la mejora continua en el sistema de gestión de seguridad de la información.

Alcance

La Política de Seguridad de la Información que se presenta basado en el cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Universidad Nacional del Callao, en adelante UNAC. Esta se aplica para toda la comunidad universitaria que contempla a docentes, no docentes, estudiantes y toda otra persona que de alguna manera esté relacionada con la UNAC. Esta política deber ser conocida por el personal de la universidad, funcionarios públicos y demás involucrados con la UNAC que involucre la seguridad de la información.

Términos y definiciones

Seguridad de la Información: La seguridad de la información se entiende como la preservación de las siguientes características tales como la confidencialidad, disponibilidad e integridad.
Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la UNAC.
Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
Tecnología de la Información: Se refiere al hardware y software operados por la UNAC o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la UNAC, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
Evaluación de Riesgos. Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la UNAC
Administración de Riesgos. Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
Procedimiento. Acciones que se realizan, con una serie común de pasos claramente definidos, que permiten realizar correctamente una tarea o alcanzar un objetivo.
Proceso de Información. Conjunto de tareas relacionadas lógicamente que se realizan para lograr un resultado determinado en un Sistema de Información.
Activos de Información. Son los bienes relacionados a un sistema de información en cualquiera de sus etapas. Ello involucra diferentes tipos de activos como los que se mencionan a continuación:
Información: Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, resultados de proyectos de investigación, etc. **Software:** Software de aplicaciones, software de sistemas, herramientas de desarrollo, etc.
Activos físicos: Computadoras, equipamiento de redes y comunicaciones, medios de almacenamiento, mobiliario, lugares de emplazamiento.
Servicios: Servicios informáticos y de comunicaciones.
Propietario de un Activo Físico. Es el responsable patrimonial del bien.

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

1. Garantizar la confidencialidad, integridad y disponibilidad de la información para contribuir al logro de nuestros objetivos estratégicos, mediante la implementación de controles de seguridad de la información.

2. Identificar, analizar y valorar los riesgos de seguridad de la información para establecer estrategias de tratamiento, basadas en un enfoque de gestión de riesgos.

3. Gestionar los incidentes de seguridad de la información para reducir el impacto en los activos de información, a través de un modelo de gestión de incidentes.

4. Fortalecer una cultura de seguridad de la información en la UNAC para protegerla información, mediante programas de concientización y capacitación.

5. Realizar la mejora continua del sistema de gestión de seguridad de la información para su fortalecimiento, mediante la ejecución de acciones correctivas y/o acciones de oportunidades de mejora.

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNAC

Las políticas de seguridad que se plantean van con relación a los siguientes puntos:

Organización de la Seguridad. Orientado a administrar la seguridad de la información
dentro de la UNAC y establecer un marco gerencial para controlar su implementación.

Clasificación y Control de Activos. Destinado a mantener una adecuada protección de los activos de la UNAC.

Seguridad del Personal. Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la UNAC o uso inadecuado de instalaciones.

Seguridad Física y Ambiental. Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la UNAC.

Gestión de las Comunicaciones y las Operaciones. Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

Control de Acceso. Orientado a controlar el acceso lógico a la información.

Desarrollo y Mantenimiento de los Sistemas. Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

Administración de la Continuidad de las Actividades de la UNAC. Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Cumplimiento. Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

1. Organización de la Seguridad

1.1. Infraestructura de la Seguridad de la Información.

1.1.1. Comisión de Seguridad de la Información.

La seguridad de la información es una responsabilidad de la UNAC compartida por todas las Autoridades Políticas, secretarios, y Decanos de Facultades, por lo cual se debe conformar la Comisión de Seguridad de la Información, integrada por representantes de las autoridades mencionadas, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. La misma cuenta con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

1.1.2. Conformación de la Comisión de Seguridad de la Información

La Comisión de Seguridad de la Información está conformada de la siguiente manera:

Área	Representante
Secretaría de Planificación y Gestión Institucional	Por definir
Prosecretaría de Informática	Por definir
Unidad de Auditoría Interna	Auditor Interno Titular
Asuntos Jurídicos	Director General
Recursos Humanos	Director General
Seguridad Física	Un representante designado por la Comisión de Prevención para la Seguridad.
Seguridad de la Información	Responsable de la Seguridad de la Información

Sus funciones:

- Revisar y aprobar, la Política y las responsabilidades generales en materia de seguridad de la información.
- Monitorear cambios significativos en la exposición de activos de información frente a las amenazas más importantes.

- Revisar y monitorear de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información.
- Acordar funciones y responsabilidades específicas relativas a seguridad de la información para toda la UNAC.
- Acordar metodologías y procesos específicos relativos a la seguridad de la información.
- Acordar y brindar apoyo y difusión a las iniciativas de seguridad de la información.
- Velar por que la seguridad sea parte del proceso de planificación de la información. Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la pertinencia y la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de la UNAC.
- Desarrollar toda actividad relacionada con la seguridad de la información que le encomienden el Consejo Superior.

El responsable del área Informática coordinará las actividades de la Comisión de Seguridad de la Información.

1.1.3. Asignación de Responsabilidades en Materia de Seguridad de la Información.

El Rector designará a un “responsable de Seguridad Informática”, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la UNAC, lo cual incluye la supervisión de todos los aspectos inherentes a la seguridad de la información, cualquiera sea el medio de almacenamiento, tratados en la presente Política. La comisión de Seguridad de la Información propondrá al Rector para su aprobación la definición y asignación de las responsabilidades que surjan de la presente Política.

1.1.4. Proceso de Autorización para Instalaciones de Procesamiento de Información.

Los nuevos recursos de procesamiento de información serán autorizados por los responsables de las Unidades Organizativas involucradas conjuntamente con el responsable de Seguridad Informática, considerando su propósito y uso, a fin de garantizar que se cumplan todas las políticas y requerimientos de seguridad pertinentes. Cuando corresponda, el Propietario de la información con el asesoramiento del responsable de Seguridad Informática y el responsable del Área Informática verificará el hardware y software para garantizar su

compatibilidad con los componentes de otros sistemas de la UNAC. El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el responsable de Seguridad Informática y deberá ser autorizado por el responsable del Área Informática y el responsable de la Unidad Organizativa al que se destinen los recursos.

1.1.5. Asesoramiento Especializado en Materia de Seguridad de la Información.

El responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en la UNAC a fin de brindar ayuda en la toma de decisiones en materia de seguridad.

1.1.6. Revisión Independiente de la Seguridad de la Información.

La Unidad de Auditoría Interna realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas de la UNAC reflejan adecuadamente sus disposiciones.

1.2. Seguridad Frente al Acceso por Parte de Terceros.

1.2.1. Identificación de Riesgos del Acceso de Terceras Partes.

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la UNAC, el responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información de la UNAC.

2. Clasificación y Control de Activos.

2.1. Inventario de activos.

El Comité de Seguridad identificará los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación. El responsable de cada Unidad Organizativa involucrada deberá elaborar un inventario con dicha información y deberá actualizarlo ante cualquier

modificación de la información registrada y revisarlo con una periodicidad semestral.

2.2. Clasificación de la información.

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad. A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

Confidencialidad:

1. Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la UNAC o no. PUBLICO
2. Información que puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves a la UNAC o terceros. CLASIFICADA – USO INTERNO
3. Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la UNAC o a terceros. CLASIFICADA - CONFIDENCIAL
4. Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la UNAC, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves a la UNAC o a terceros. CLASIFICADA- SECRETA

Integridad:

1. Información cuya modificación no autorizada, si no es detectada, no afecta la operatoria de la UNAC.
2. Información cuya modificación no autorizada, si no es detectada, podría ocasionar pérdidas leves para la UNAC o terceros.
3. Información cuya modificación no autorizada, si no es detectada, podría ocasionar pérdidas significativas para la UNAC o terceros.
4. Información cuya modificación no autorizada, si no es detectada, podría ocasionar pérdidas graves a la UNAC o a terceros.

Disponibilidad**:** Se distinguen dos casos

Inaccesibilidad transitoria:

a. Información cuya inaccesibilidad transitoria no afecta la operatoria de la UNAC.
b. Información cuya inaccesibilidad transitoria durante 1 semana podría ocasionar pérdidas significativas para la UNAC o terceros.

c. Información cuya inaccesibilidad transitoria durante 1 día podría ocasionar pérdidas significativas a la UNAC o a terceros.
d. Información cuya inaccesibilidad transitoria durante 1 hora podría ocasionar pérdidas significativas a la UNAC o a terceros.

Inaccesibilidad permanente:

1. Información cuya inaccesibilidad permanente no afecta la operatoria de la UNAC.
2. Información cuya inaccesibilidad permanente podría ocasionar pérdidas leves para la UNAC o terceros.
3. Información cuya inaccesibilidad permanente podría ocasionar pérdidas significativas para la UNAC o terceros.
4. Información cuya inaccesibilidad permanente podría ocasionar pérdidas graves a la UNAC o a terceros.

Al referirse a pérdidas, se contemplan aquellas mensurables (materiales) y no mensurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.). El Propietario de la Información asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

CRITICIDAD BAJA: ninguno de los valores asignados supera el 1.
CRITICIDAD MEDIA: alguno de los valores asignados es 2.
CRITICIDAD ALTA: alguno de los valores asignados es 3.

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad. Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.
- Luego de clasificada la información, el Propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma. En adelante se mencionará como “información clasificada” (o “datos clasificados”) a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

2.3. Rotulado de la Información.

El responsable de Seguridad Informática definirá procedimientos para el rotulado y manejo de información, de acuerdo con el esquema de clasificación definido. Los mismos contemplarán los activos de información tanto en formatos

físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia.
- Almacenamiento.
- Transmisión por correo, fax, correo electrónico.
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

3. Seguridad del Personal.

3.1. Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos.

3.1.1. Incorporación de la Seguridad en los Puestos de Trabajo.

El Comité de Seguridad de la Información incorporará las funciones y responsabilidades en materia de seguridad en la descripción de las responsabilidades de los puestos de trabajo. Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

3.1.2. Control y Política del Personal.

El responsable del Área de Recursos Humanos llevará a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto.

3.1.3. Compromiso de Confidencialidad.

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la UNAC. La copia firmada del Compromiso deberá ser retenida en forma segura por el responsable del Área de Recursos Humanos. Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado. El responsable de Área de Recursos Humanos desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

1. Suscripción inicial del Compromiso por parte de la totalidad del personal.

2. Método de re-subscripción en caso de modificación del texto del Compromiso.

El responsable del Área Legal revisará anualmente el contenido del Compromiso.

3.1.4. Términos y Condiciones de Empleo.

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la UNAC y del horario normal de trabajo. Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo, en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

3.2. Capacitación del Usuario.

3.2.1. Formación y Capacitación en Materia de Seguridad de la Información.

Todos los empleados de la UNAC y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la UNAC recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la UNAC. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo. El responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política. Una capacitación mensual.

3.3. Respuesta a Incidentes y Anomalías en Materia de Seguridad.

3.3.1. Comunicación de Incidentes Relativos a la Seguridad.

Los incidentes relativos a la seguridad serán comunicados a través de canales apropiados y tan pronto como sea posible al responsable de la Unidad Organizativa y al responsable de Seguridad Informática. El responsable de Seguridad Informática y el responsable del Área Informática establecerán un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Esto con la inmediates que se requiera para la atención del incidente.

3.3.2. Comunicación de Debilidades en Materia de Seguridad.

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al responsable del Activo que se trate y al responsable de Seguridad Informática, esto incluye la comunicación y corrección de anomalías del software.

3.3.3. Aprendiendo de los Incidentes.

El Comité de Seguridad de la Información definirá un procedimiento que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías.

3.3.4. Procesos Disciplinarios.

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la UNAC y de la Administración Pública en el Perú.

4. Seguridad Física y Ambiental.

4.1. Perímetro de Seguridad Física.

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes de la UNAC y de las instalaciones de procesamiento de información. La UNAC utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. Para ello se debe tener en cuenta lo siguiente:

1. Definir y documentar claramente el perímetro de seguridad.
2. Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida.
3. Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
4. Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán medios alternativos de control de acceso físico al área o edificio. El acceso a dichas áreas y edificios estará

restringido exclusivamente al personal autorizado. Además, se debe registrar los ingresos y salidas a dichas áreas.

5. Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación.
6. Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

El responsable de cada área o facultad involucrada con asesoría del responsable de Seguridad Física y del Responsable de Seguridad Informática, llevará un registro actualizado de los sitios protegidos, indicando:

1. Identificación del Edificio y Área.
2. Principales elementos a proteger.
3. Medidas de protección física.

4.2. Ubicación y Protección de Activos físicos.

Los activos físicos, que incluyen el equipamiento, los medios de almacenamiento (informatizados o no), y las copias de respaldo serán ubicados y protegidos de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

1. Ubicar dichos activos en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
2. Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
3. Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
4. Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará periódicamente, con un período no superior a los seis meses.

4.3. Suministros de Energía.

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

1. Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
2. Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la UNAC.

3. Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento.

4.4. Seguridad del Cableado.

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

1. Cumplir con los requisitos técnicos vigentes en el Perú.
2. Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.
3. Proteger el cableado de red contra intercepción no autorizada o daño.
4. Evitar las interferencias entre los cables de energía de los cables de comunicaciones.
5. Proteger el tendido del cableado troncal (backbone).

4.5. Mantenimiento de Equipos.

El Propietario de la Información realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

1. Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del responsable del Área Informática. El Propietario de la Información mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo y se lo comunicará al Comité de Seguridad de la Información.
2. Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
3. Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
4. Registrar el retiro de equipamiento de la sede de la UNAC para su mantenimiento.
5. Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

4.6. Seguridad de los Equipos Fuera de las Instalaciones.

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la UNAC, será autorizado por el responsable patrimonial. En el caso

de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la UNAC para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

4.7. Retiro de los Bienes.

El equipamiento, la información y el software no serán retirados de la sede de la UNAC sin autorización formal del responsable patrimonial del bien de que se trate. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la UNAC. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

5. Gestión de Comunicaciones y Operaciones.

5.1. Procedimientos y Responsabilidades Operativas.

5.1.1. Documentación de los Procedimientos Operativos.

Los responsables de los Sistemas de Información documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el responsable de Seguridad Informática. Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

1. Procesamiento y manejo de la información.
2. Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
3. Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
4. Restricciones en el uso de utilitarios del sistema.
5. Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
6. Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
7. Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Los responsables de los Sistemas de Información prepararán adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

1. Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
2. Instalación y mantenimiento de las plataformas de procesamiento.
3. Monitoreo del procesamiento y las comunicaciones.
4. Inicio y finalización de la ejecución de los sistemas.
5. Programación y ejecución de procesos.
6. Gestión de servicios.
7. Resguardo de información.
8. Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
9. Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
10. Uso del correo electrónico.

5.1.2. Control de Cambios en las Operaciones.

El responsable del Área Informática definirá procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad. El responsable de Seguridad Informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación. El responsable del Sistema de Información retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado. Los procedimientos de control de cambios contemplarán los siguientes puntos:

1. Evaluación del posible impacto de dichos cambios.
2. Aprobación formal de los cambios propuestos.
3. Planificación del proceso de cambio.
4. Prueba del nuevo escenario.
5. Comunicación de detalles de cambios a todas las personas pertinentes.
6. Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

5.1.3. Procedimientos de Manejo de Incidentes.

El responsable de Seguridad Informática establecerá funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

1. Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo:
    a. Fallas operativas.
    b. Código malicioso.
    c. Intrusiones.
    d. Fraude informático.

e. Error humano.
f. Catástrofes naturales.

2. Comunicar los incidentes a través del responsable del área o facultad de Incidentes Relativos a la Seguridad.
3. Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):

a. Definición de las primeras medidas a implementar.
b. Análisis e identificación de la causa del incidente.
c. Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
d. Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
e. Notificación de la acción a la autoridad y/u Organismos pertinentes.

4. Registrar pistas de auditoría y evidencia similar para:
   a. Análisis de problemas internos.
   b. Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial
   c. Negociación de compensaciones por parte de los proveedores de software y de servicios.
5. Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
   a. Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
   b. Documentación de todas las acciones de emergencia emprendidas en forma detallada.
   c. Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
   d. Constatación de la integridad de los controles y sistemas de la UNAC en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del responsable del Área Legal en el tratamiento de incidentes de seguridad ocurridos.

5.2. Planificación y Aprobación de Sistemas.

5.2.1. Planificación de la Capacidad.

El responsable del Área Informática junto con los responsables de los Sistemas de Información efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin

de garantizar un procesamiento y almacenamiento adecuados. Para ello tomarán en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información de la UNAC para el período estipulado de vida útil de cada componente.

5.2.2. Aprobación del Sistema.

El responsable del Área Informática y el responsable de Seguridad Informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

1. Verificar el impacto en el desempeño y los requerimientos de capacidad de las computado- ras.
2. Garantizar la recuperación ante errores.
3. Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
4. Garantizar la implementación de un conjunto acordado de controles de seguridad.
5. Confeccionar disposiciones relativas a la continuidad de las actividades de la UNAC.
6. Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
7. Considerar el efecto que tiene el nuevo sistema en la seguridad global de la UNAC.
8. Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

5.3. Protección Contra Software Malicioso.

5.3.1. Controles Contra Software Malicioso.

El responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El responsable del Área Informática, o el personal designado por éste, implementará dichos controles. El responsable de Seguridad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios. Estos controles deberán considerar las siguientes acciones:

1. Prohibir el uso de software no autorizado por la UNAC
2. Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.

3. Instalar y actualizar periódicamente software de detección y reparación de virus, examina- do computadoras y medios informáticos, como medida precautoria y rutinaria.
4. Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (pro- bar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
5. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la UNAC, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
6. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
7. Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
8. Concientizar al personal acerca del problema de los virus y de cómo proceder frente a los mismos.

5.4. Mantenimiento.

5.4.1. Resguardo de la Información.

El Propietario de Información con la ayuda del responsable del Área Informática y el responsable de Seguridad Informática determinará los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información. El responsable del Área Informática dispondrá la realización de dichas copias, así como la prueba periódica de su restauración.

1. Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
2. Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indica- do por el proveedor, y asegurando la destrucción de los medios desechados.
3. Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal.
4. Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
5. Probar periódicamente los medios de resguardo.

6. Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.
7.

5.5. Administración de la Red.

5.5.1. Controles de Redes.

El responsable de Seguridad Informática y el responsable del Área Informática definirán controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la UNAC, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

1. Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido.
2. Establecer controles especiales para salvaguardar la confidencialidad e integridad del pro- cesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los ser- vicios de red y computadoras conectadas.
3. Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

6. Control de Accesos.

6.1. Requerimientos para el Control de Acceso.

6.1.1. Política de Control de Accesos.

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

1. Identificar los requerimientos de seguridad de cada una de las aplicaciones.
2. Identificar toda la información relacionada con las aplicaciones.
3. Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes. (
4. Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
5. Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
6. Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.
7.

6.1.2. Reglas de Control de Acceso.

Las reglas de control de acceso especificadas deberán:

1. Indicar expresamente si las reglas son obligatorias u optativas.
2. Establecer reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente” y no sobre la premisa inversa de “Todo está permitido a menos que se prohíba expresamente”.
3. Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario. Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
4. Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

6.2. Administración de Accesos de Usuarios.

Con el objetivo de impedir el acceso no autorizado a la información El responsable del Sistema de Información implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

6.2.1. Registro de Usuarios.

El responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

1. Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
2. Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
3. Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la UNAC, por ejemplo, que no compromete la separación de tareas.
4. Entregar a los usuarios un detalle escrito de sus derechos de acceso.
5. Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
6. Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
7. Mantener un registro formal de todas las personas registradas para utilizar el servicio.
8. Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la

autorización, se desvincularon de la UNAC o sufrieron la pérdida/robo de sus credenciales de acceso.

9. Efectuar revisiones periódicas con el objeto de:
   Cancelar identificadores y cuentas de usuario redundantes.
   Inhabilitar cuentas inactivas por más de 30 días.
   Eliminar cuentas inactivas por más de 60 días.
10. En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
11. Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
12. Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

El Propietario de la Información será el responsable del registro de usuarios.

6.2.2. Administración de Privilegios.

El Propietario de la Información limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

1. Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
2. Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo, el requerimiento mínimo para su rol funcional.
3. Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
4. Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.
5. Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el responsable de Seguridad Informática.

6.2.3. Administración de Contraseñas de Usuario.

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

1. Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad.
2. Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
3. Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.

4. Almacenar las contraseñas sólo en sistemas informáticos protegidos.
5. Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la bio- métrica (por ejemplo, verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el responsable de Seguridad Informática conjuntamente con el responsable del Área Informática y el Propietario de la Información lo determine necesario (o lo justifique).
6. El responsable de Seguridad Informática establecerá los procedimientos de manejo de contraseñas apropiados para cada sistema.

Los Propietarios de la Información son los responsables del proceso de asignación de contra- señas.

6.2.4. Administración de Contraseñas Críticas.

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc.. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Propietario de la Información y Responsable de Seguridad Informática definirán procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

1. Se definirán las causas que justificarán el uso de contraseñas críticas, así como el nivel de autorización requerido.

2. Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
3. Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
4. La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
5. Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.
6. Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el responsable de Seguridad Informática.

6.2.5. Revisión de Derechos de Acceso de Usuarios.

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares de 6 meses, a fin de revisar los derechos de acceso de los usuarios.

6.3. Responsabilidades del Usuario.

6.3.1. Uso de Contraseñas.

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Los usuarios deben cumplir las siguientes directivas:

1. Mantener las contraseñas en secreto.
2. Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
3. Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
    a. Sean fáciles de recordar.
    b. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.
    c. No consistan en caracteres idénticos consecutivos.
4. Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

5. Cambiar las contraseñas provisorias en el primer inicio de sesión.
    a. Notificar de acuerdo Incidentes Relativos a la Seguridad", cualquier incidente de seguridad relacionado con sus contraseñas, pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

6.3.2. Equipos Desatendidos en Áreas de Usuarios.

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

6.4. Control de Acceso a la Red.

6.4.1. Política de Utilización de los Servicios de Red.

Las conexiones no seguras a los servicios de red pueden afectar a toda la UNAC, por lo tanto, el responsable del Área Informática controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de los mismos.

El responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la UNAC.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

1. Identificar las redes y servicios de red a los cuales se permite el acceso.
2. Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
3. Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

6.4.2. Acceso a Internet.

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Comité de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el área o facultad a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

El Comité de Seguridad de la Información evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares.

6.4.3. Control de Conexión a la Red.

Sobre la base de lo definido en el punto “Requerimientos”, se implementarán controles para evitar el uso indebido de la red. Dichos controles se podrán implementar en los “gateways” que separen los diferentes dominios de la red.
Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

1. Correo electrónico.
2. Transferencia de archivos.
3. Acceso interactivo.
4. Acceso a la red fuera del horario laboral.

6.4.4. Control de Ruteo de Red.

En las redes compartidas se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación

positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otra autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

6.4.5. Seguridad de los Servicios de Red.

El responsable de Seguridad Informática junto con el Responsable del Área Informática definirán las pautas para garantizar la seguridad de los servicios de red de la UNAC, tanto públicos como privados.
Para ello se tendrán en cuenta las siguientes directivas:

1. Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
2. Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.

3. Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
4. Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Responsable de Seguridad Informática.

7. Desarrollo y Mantenimiento de Sistemas.

7.1. Requerimientos de Seguridad de los Sistemas.

7.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad.

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

1. Definir un procedimiento para que, durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de con- troles manuales complementarios.
2. Los controles de seguridad en el desarrollo y mantenimiento se realizarán a través de pruebas periódicas y al momento del desarrollo por parte del equipo encargado de verificar que se cumplan con los requisitos de desarrollo y mantenimiento relacionado a las políticas de seguridad de la información.

8. Administración de la Continuidad de las Actividades de la UNAC.

8.1. Proceso de la Administración de la Continuidad de la UNAC.

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la UNAC.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la UNAC frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

1. Identificar y priorizar los procesos críticos de las actividades de la UNAC.
2. Asegurar que todos los integrantes de la UNAC comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la UNAC.
3. Elaborar y documentar una estrategia de continuidad de las actividades de la UNAC consecuente con los objetivos y prioridades acordados.
4. Proponer planes de continuidad de las actividades de la UNAC de conformidad con la estrategia de continuidad acordada.
5. Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
6. Coordinar actualizaciones periódicas de los planes y procesos implementados.
7. Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la UNAC.
8. Proponer las modificaciones a los planes de contingencia.

9. Cumplimiento.

9.1. Cumplimiento de Requisitos Legales.

9.1.1. Identificación de la Legislación Aplicable.

El responsable del Área Legal definirá y documentará claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

9.1.2. Derechos de Propiedad Intelectual.

El responsable del Área Legal propiciará el dictado de normas que garanticen el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
Los empleados únicamente podrán utilizar material autorizado por la UNAC.

La UNAC solo podrá autorizar el uso de material producido por ella misma, o material autorizado o suministrado a la misma por su titular, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Derecho de Propiedad Intelectual del Software. El software es considerado una obra intelectual que goza de la protección esto está definido en el Decreto Legislativo N° 822. Esta Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El responsable de Seguridad Informática, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

1. Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
2. Divulgar las políticas de adquisición de software y las disposiciones del decreto legislativo mencionado.
3. Mantener un adecuado registro de activos.
4. Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
5. Implementar controles para evitar el exceso del número máximo permitido de usuarios.
6. Verificar que sólo se instalen productos con licencia y software autorizado.
7. Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
8. Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
9. Utilizar herramientas de auditoría adecuadas.
10. Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

9.1.3. Protección de Datos y Privacidad de la Información Personal.

Todos los miembros de la comunidad universitaria deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan acceso con motivo del ejercicio de sus funciones.

El responsable del Área Legal redactará un "Compromiso de Confidencialidad", el cual deberá ser suscrito por todos los que tengan acceso a información clasificada como Confidencial o Secreta. La copia firmada del compromiso será retenida en forma segura por la UNAC, mediante este instrumento el subscriptor se comprometerá a utilizar la información solamente para el uso específico al que está destinada y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del responsable del Activo de que se trate. El "Compromiso de Confidencialidad" deberá especificar que determinadas actividades pueden ser objeto de control y monitoreo

9.1.4. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información.

Los recursos de procesamiento de información de la UNAC se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino para el cual fueron provistos debe ser considerada como uso indebido. La Universidad puede monitorear el uso de estos recursos, a fin de verificar el cumplimiento de las disposiciones vigentes, y llegado el caso sancionar la violación de la normativa aplicable.