UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

SECRETARÍA GENERAL

RESOLUCIÓN NRO. R- 544 -2025-UNSAAC

Cusco, 07 de mayo de 2025

EL RECTOR DE LA UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO:

VISTO, los Oficios Nros. 410-2024-UCC-DSI-UNSAAC y N°. 135-2025-UCC-OTI-UNSAAC, signados con Expediente Nro. 706397, presentado por el **Ing. AGUEDO HUAMANI HUAYHUA**, Jefe de la Unidad de Centro de Cómputo de la Institución, elevando propuesta de "**DIRECTIVA PARA ESTABLECER DISPOSICIONES Y PROCEDIMIENTOS DE SEGURIDAD EN EL USO DE LOS SITEMAS DE INFORMACION EN LA UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO",** para su aprobación, y;

CONSIDERANDO:

Que, mediante Documento de Visto, Jefe de la Unidad de Centro de Cómputo de la Institución, eleva la propuesta de "**DIRECTIVA PARA ESTABLECER DISPOSICIONES Y PROCEDIMIENTOS DE SEGURIDAD EN EL USO DE LOS SITEMAS DE INFORMACION EN LA UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO",** para su aprobación correspondiente; precisando que el documento cuenta con opinión favorable de la Unidad de Modernización, según consta del Oficio N°. 166-2024-UM/OPP/UNSAAC, así como de la Dirección de Asesoría Jurídica de la Institución;

Que, con Dictamen Legal N°. 80-2025-DAJ-UNSAAC, el Director de Asesoría Jurídico, opina que la citada Directiva sea aprobada, previo levantamiento de las observaciones y recomendaciones advertidas en la evaluación y análisis jurídico;

Que, la Jefe de la Unidad de Modernización de la Oficina de Planeamiento y Presupuesto, con Oficio N°. 70-2025-UM/OPP-UNSAAC, comunica el levantamiento de observaciones y recomendaciones formuladas por el Director de Asesoría Jurídica, en tal sentido eleva la propuesta de Directiva, con la visación correspondiente, para su aprobación;

Que, la mencionada Directiva tiene por objeto establecer las disposiciones y procedimientos necesarios para garantizar la seguridad de la información, salvaguardando su confidencialidad, integridad y disponibilidad en todas las unidades de organización de la Universidad Nacional de San Antonio Abad del Cusco. Su contenido comprende: I Objeto, II Finalidad, III Base legal, IV Alcance, V Disposiciones Generales, VI Disposiciones Específicas, VII responsabilidades y Disposiciones Complementarias y Finales;

Que, con Nota de Atención N°. 116-2025-DAJ-UNSAAC el Director de Asesoría Jurídica de la Institución, señala que la Unidad de Modernización y Unidad de Centro de Cómputo han levantado las observaciones formuladas mediante Dictamen Legal N.° 80-2025-DAJ-UNSAAC; por lo tanto, el trámite administrativo de aprobación debe continuar;

Que, el Art. 8° de la Ley Universitaria 30220 concordante con el Art. 7° del Estatuto Universitario, prescribe que la autonomía inherente a las universidades se ejerce de conformidad con lo establecido en la Constitución, la Ley Universitaria y demás normativas aplicables; esta autonomía se manifiesta, entre otros, en el régimen

normativo, que implica la potestad auto-determinativa para elaborar y aprobar todas sus normas internas orientadas a regular las acciones académico-administrativas, así como de control;

Que, la Autoridad Universitaria, ha tomado conocimiento de la petición y de conformidad a los Lineamientos para Elaboración de Directivas en la Universidad Nacional de San Antonio Abad del Cusco, aprobado por Resolución N°. 1563-2018-UNSAAC del 6 de noviembre de 2018, ha dispuesto la emisión de la Resolución correspondiente;

Estando a lo solicitado, Dictamen Legal N.° 80-2025-DAJ-UNSAAC, Nota de Atención N°. 116-2025-DAJ-UNSAAC y en uso de las atribuciones conferidas por la Ley y el Estatuto Universitarios;

RESUELVE:

PRIMERO.- APROBAR la Directiva N°. 01-2025-UCC/OTI-UNSAAC "**DIRECTIVA PARA ESTABLECER DISPOSICIONES Y PROCEDIMIENTOS DE SEGURIDAD EN EL USO DE LOS SITEMAS DE INFORMACION EN LA UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO",** elaborada por la Unidad de Centro de Cómputo y revisada por la Unidad de Modernización de la Oficina de Planeamiento y Presupuesto; el documento comprende: I Objeto, II Finalidad, III Base legal, IV Alcance, V Disposiciones Generales, VI Disposiciones Específicas, VII responsabilidades y Disposiciones Complementarias y Finales, el mismo que en anexo forma parte de la presente Resolución.

SEGUNDO.- ENCARGAR a la Oficina de Planeamiento y Presupuesto y la Unidad de Centro de Cómputo, adopten las acciones correspondientes para el cumplimiento de la presente resolución.

TERCERO.- DISPONER que la **UNIDAD DE RED DE COMUNICACIONES y la OFICINA DE COMUNICACIÓN E IMAGEN INSTITUCIONAL**, procedan con publicar y difundir la presente resolución en la página web de la institución, según corresponda.

REGISTRESE, COMUNIQUESE Y ARCHIVESE

Universidad Nacional de San Antonio Abad del Cusco – RECTORADO

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

DR. ELEAZAR CRUCINTA UGARTE
RECTOR

Tr. VRAC.-VRIN.-OCI.- OFICINA DE PLANEAMIENTO Y PRESUPUESTO.-UNIDAD DE PLANEAMIENTO Y PRESUPUESTO.-U DE MODERNIZACIÓN.- DIGA.- UNIDAD DE RECURSOS HUMANOS.- FACULTADES (18).- ESCUELAS PROFESIONALES.- DEPARTAMENTOS ACADÉMICOS.- UNIDAD DE CENTRO DE COMPUTO.-ASESORÍA JURÍDICA.-IMAGEN INSTITUCIONAL.-RED DE COMUNICACIONES.-ARCHIVO CENTRAL.-ARCHIVO. ECU/MMVZ/MQL/EMM.

Lo que transcribo a Ud. para su conocimiento y fines consiguientes.

Atentamente,

Universidad Nacional de San Antonio Abad – SECRETARÍA GENERAL – CUSCO

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

BOG. M. VYLLUSKA VILLAGARCÍA ZERECEDA
SECRETARIA GENERAL (e)

DIRECTIVA Nº 01-2025-UCC/OTI-UNSAAC

DIRECTIVA PARA ESTABLECER DISPOSICIONES Y PROCEDIMIENTOS DE SEGURIDAD EN EL USO DE LOS SISTEMAS DE INFORMACIÓN EN LA UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

OBJETO

Establecer las disposiciones y procedimientos necesarios para garantizar la seguridad de la información, salvaguardando su confidencialidad, integridad y disponibilidad en todas las unidades de organización de la Universidad Nacional de San Antonio Abad del Cusco.

II. FINALIDAD

La presente Directiva tiene como finalidad establecer disposiciones y procedimiento de control, así como fortalecer la cultura para seguridad de la información que tienen a su cargo y conocimiento los funcionarios, servidores, colaboradores y estudiantes de la UNSAAC; asegurando el cumplimiento normativo en materia de seguridad y confianza digital y gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información. Proteger la información que permite asegurar la confidencialidad, integridad y disponibilidad de la información institucional ante amenazas internas y externas, minimizando los riesgos de daño a la información digital o física que pueda afectar la continuidad operativa y servicio que brinda la entidad, mediante el cumplimiento de las normativas legales y regulatorias aplicables.

III. BASE LEGAL

- Constitución Política del Perú.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- Decreto Supremo N° 003-2013-JUS, aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
- Decreto Supremo N° 029-2021-PCM, aprueba el Reglamento de la Ley de Gobierno Digital
- Decreto Supremo N° 007-2020, Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto de Urgencia N° 006-2020, crea el Sistema Nacional de Transformación Digital.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.
- Directivas de acceso a la información bajo ISO 27001 Extensión de ISO/IEC 27001 y 27002.
- Norma Técnica Peruana NTP ISO/IEC 27001:2014.

- Resolución N° R-1563-2018-UNSAAC, aprueba Lineamientos para la Elaboración de Directivas en la Universidad Nacional de San Antonio Abad del Cusco.

IV. ALCANCE

Lo establecido en la presente Directiva es de cumplimiento obligatorio, para todo el personal docente, personal administrativo, estudiantes, colaboradores, investigadores y terceros que utilicen o gestionen los sistemas de información en la Universidad Nacional de San Antonio Abad del Cusco.

V. DISPOSICIONES GENERALES

5.1. DEFINICIONES

Acceso: Autorización concedida a un usuario para la utilización de los diversos recursos informáticos disponibles.

Activo de información: Cualquier dato o recuso relacionado con las operaciones educativas, administrativas o investigativas de la universidad.

Amenaza: Cualquier evento o acción que pueda comprometer la seguridad de la información.

Base de datos: Recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático, que puede ser consultado rápidamente de acuerdo con las características selectivas.

Confidencialidad: Asegurar que solo las personas autorizadas accedan a la información clasificada o restringida.

Disponibilidad: Asegurar que los sistemas de información estén operativos y accesibles cuando se necesiten.

Gestión de incidentes de seguridad digital: Proceso formal por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares.

Incidente de seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de los sistemas o datos de la universidad.

Integridad: Propiedad de salvaguardar garantizar que los datos y sistemas no sean alterados de manera no autorizada o accidental.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): Comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riegos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación.

Sistema de información: Conjunto interdependiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, presentación, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

5.2 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

En el contexto de la Universidad Nacional de San Antonio Abad del Cusco, el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) está diseñado para proteger la diversidad de activos, usuarios y procesos únicos de la institución. A continuación, se detalla un alcance:

A. Procesos Académicos y Administrativos

- **Gestión Académica:** Procesos relacionados con la inscripción, calificaciones, expedientes académicos, expedición de títulos y certificados. Este proceso implica manejar datos sensibles y confidenciales de estudiantes y académicos.
- **Administración de Recursos Humanos:** Incluye la gestión de datos del personal docente y administrativo, como contratos, evaluaciones y nominas.
- **Investigación y Desarrollo:** Protección de proyectos de investigación, patentes y datos sensibles, especialmente aquellos que contienen información confidencial o de propiedad intelectual.
- **Finanzas y Contabilidad:** Cobranza de matrículas, contabilidad institucional, gestión de presupuestos y auditorías. Este proceso también puede incluir datos de tarjetas de crédito y cuentas bancarias de estudiantes y empleados.

B. Activos de Información

- **Datos de Estudiantes, Personal Docente y Administrativo:** Incluye datos personales, registros académicos y laborales, y cualquier otro dato sensible almacenado en bases de datos internos o sistemas de administración.
- **Documentos y Expedientes Digitales:** Documentos digitales almacenados en los servidores de la universidad que contienen información administrativa, académica y de investigación.
- **Sistemas de Gestión Académica y Administrativa:** Plataformas como sistemas de administración académica, bases de datos de calificaciones, sistemas de recursos humanos, gestión de nómina y bibliotecas digitales.

C. Usuarios y Roles

- **Estudiantes, Personal Docente y Personal Administrativo:** Todos los grupos de usuarios que acceden a la red universitaria, sistemas de información académica, plataformas de aprendizaje y recursos digitales.
- **Proveedores y Colaboradores Externos:** Usuarios externos, como proveedores de servicios de tecnología y software, así como investigadores externos que puedan tener acceso temporal o parcial a ciertos datos.

D. **Infraestructura Tecnológica y Redes**
- **Red Universitaria y Centros de Datos:** Incluye servidores, centros de datos y sistemas de almacenamiento en campus y centros de respaldo.
- **Plataformas de Aprendizaje y Aplicaciones en la Nube:** Herramientas como entornos de aprendizaje virtual, portales estudiantiles y sistemas de colaboración que se ejecutan en la nube o en servidores locales.
- **Dispositivos de Usuario Final:** Equipos de profesores, servidores administrativos, laboratorios de computación y dispositivos móviles que acceden a la red y a los sistemas de la universidad.

E. **Entornos Físicos y Virtuales**
- **Campus Principal y Campus Satélites:** Incluye las ubicaciones físicas donde se encuentran los centros de datos, oficinas administrativas y bibliotecas.
- **Ambientes Virtuales de Aprendizaje:** Sistemas y plataformas digitales de acceso remoto que ofrecen contenido académico, como plataformas de educación en línea.

F. **Normativas y Requisitos Legales**
- **Protección de Datos Personales:** Cumplimiento de leyes de privacidad de datos como el Reglamento General de Protección de Datos (RGPD) o las normativas locales de protección de datos personales.
- **Derechos de Propiedad Intelectual:** Protección de la propiedad intelectual, derechos de autor de publicaciones y otros materiales de investigación.
- **Regulación de Infraestructura Crítica:** Si la universidad tiene infraestructura crítica o realiza investigaciones sensibles, deben cumplirse regulaciones adicionales en ciberseguridad.

VI. DISPOSICIONES ESPECÍFICAS.

6.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1.1. Clasificación de la Información

Toda la información de la Universidad Nacional de San Antonio Abad del Cusco está clasificada según su nivel de sensibilidad:

- **Información Pública:** Datos disponibles para la comunidad académica y el público en general.
- **Información Interna:** Información accesible solo para el personal autorizado de la universidad y estudiantes, como carga académica, catálogo, planes de estudio y comunicaciones internas.
- **Información Confidencial:** Información crítica que incluye datos personales de estudiantes, información financiera, evaluaciones académicas y documentos de investigación no publicados.

6.1.2. Gestión de Accesos

Los sistemas de información administrados por la Unidad de Centro de Cómputo de la Universidad Nacional de San Antonio Abad del Cusco, otorgan acceso a los mismos a través de diferentes principios como se detallan a continuación:

a) **El Principio de Mínimos Privilegios.** - Es un principio fundamental en la seguridad de la información donde se establece que los usuarios, procesos, aplicaciones y sistemas deben tener únicamente los privilegios necesarios para realizar sus funciones o tareas específicas, y nada más. En entornos en desarrollo, los desarrolladores pueden tener acceso a sistemas de prueba, pero no a los sistemas de producción, a menos que sea absolutamente necesario y bajo supervisión. En Sistemas Automatizados que realiza copias de seguridad de los datos debe tener acceso solo a los datos necesarios para la copia, y no a otros archivos o sistemas que no sean parte de su función.
El Equipo de Desarrollo de la Unidad de Centro de Computo debe de contar con un sistema de control de versiones (Producción y pruebas), servidores con sistemas operativos usados (Producción y pruebas) y gestores de bases de datos (Producción y pruebas). Los equipos de desarrollo solo deben de tener acceso irrestricto a sistemas de pruebas.

b) **Asignan diferentes roles dentro del sistema de gestión académica.-** Dentro de este principio a cada individuo que ingresa al sistema se le asigna a uno de estos roles y adquiere los permisos predefinidos de esta, los roles identificados son:
   - **Docente.-** Se le asignan los siguientes permisos: Ver lista de estudiantes, ver catálogo, ver carga académica, registrar calificaciones, acceder a informes académicos, llamar asistencia, subir sílabos, subir ficha de labor.
   - **Director de escuela.-** Se le asignan los siguientes permisos: Matricula de estudiantes, subir catálogo, subir horarios.
   - **Director de departamento.-** Subir carga académica de docentes, descargar sílabos, subir sílabos.
   - **Estudiante.** - Se le asignan los siguientes permisos: Ver sus propias calificaciones, enviar trabajos, consultar horarios, procesos de matrícula, reportes académicos.
   - **Administrador de sistemas.-** Se le asignan los siguientes permisos: Gestionar cuentas de usuario, configurar servidores, acceder a logs del sistema, realizar copias de seguridad.
   - **Operador.-** Se le asignan los siguientes permisos: Procesar información académica de estudiantes (homologaciones, convalidaciones), emisión académica de reportes en general de acuerdo al Texto Único de Procesos Administrativos (TUPA).

c) Autenticación y Autorización

I. **Autenticación.** - Es el proceso de verificar la identidad de un usuario, sistema o dispositivo. El objetivo es confirmar que la entidad que intenta acceder es quien dice ser. Solo después de una autenticación exitosa, el sistema procede a la autorización.

¿Qué es lo que autentica la Unidad de Centro de Computo?

- Algo que conoces.- Una contraseña, un PIN o respuestas a preguntas de seguridad.
- Algo que tienes.- Un token de seguridad, tarjeta de acceso, dispositivo móvil, o llave física.
- Algo que eres.- Información biométrica, como huellas dactilares, reconocimiento facial, o escaneo de iris.

¿Qué tipos de autentificación usa la Unidad de Centro de Computo?

- Autenticación de un Solo Factor (SFA).- El usuario se autentica usando solo uno de los factores mencionados, generalmente una contraseña.
- Autenticación de Dos Factores (2FA).- Requiere dos factores de autenticación, por ejemplo una contraseña (algo que conoces) y un código enviado a tu teléfono móvil o email institucional (algo que tienes).
- Autenticación Multifactor (MFA).- Va más allá del 2FA, involucrando múltiples factores de autenticación, como una contraseña, una clave física y un escaneo biométrico o huella digital.

Ejemplo: Autenticación por Contraseña.- El usuario ingresa su código o DNI y contraseña para acceder a una cuenta en línea.
Autenticación Biométrica.- Un dispositivo (Facial, dactilar, etc.) solicita una huella dactilar o reconocimiento facial para desbloquearse.
Autenticación con Token.- Un código de un solo uso (OTP) se envía a un dispositivo móvil u correo institucional para verificar la identidad.
En resumen, el usuario ingresa sus credenciales de acceso (usuario y contraseña) o se evalúa a través de un dispositivo de Hardware sus accesos. El sistema verifica su identidad comparando las credenciales con las almacenadas en la base de datos, si coinciden, la autenticación es exitosa.

Mejores Prácticas para contraseñas seguras:
La norma ISO/IEC 27001, junto con la ISO/IEC 27002 (ambas relacionadas con la gestión de seguridad de la información), recomienda buenas prácticas en la creación de contraseñas para asegurar el acceso.

- **Longitud mínima. -** Se recomienda que las contraseñas tengan un mínimo de 8 a 12 caracteres. Sin embargo, para sistemas de mayor seguridad, es preferible aumentar la longitud.

- **Combinación de caracteres.-** Las contraseñas deben incluir una combinación de letras mayúsculas, letras minúsculas, números y caracteres especiales para fortalecer la complejidad.
  - Al menos una letra mayúscula (A-Z).
  - Al menos una letra minúscula (a-z).
  - Al menos un número (0-9).
  - Al menos un carácter especial (por ejemplo: !, @, #, $, %).
- **Requerimientos adicionales.-** Se debe de evitar el uso de: contraseñas comunes, nombres, DNI, fechas de nacimiento, direcciones o palabras de uso común en las contraseñas, números alfanuméricos seguidos (123, 1234, 123456. etc.), seas estos ascendentemente o descendentemente.

II. **Autorización.** - Es el proceso que ocurre después de la autenticación y determina a que recursos o acciones puede acceder el usuario autenticado. Una vez que el sistema ha confirmado la identidad, decide que permisos o privilegios tiene esa persona o sistema en particular.

Tipos Comunes de Autorización en la Unidad de Centro de Computo

- **Control de Acceso Basado en Roles (RBAC):** Los permisos se otorgan según el rol del usuario en la organización, como administrador, gerente, empleado, etc.
- **Control de Acceso Basado en Atributos (ABAC):** Los permisos se asignan en función de atributos como el puesto de trabajo, la ubicación geográfica, o la hora del día.
- **Listas de Control de Acceso (ACL)**: Define explícitamente quien tiene acceso a qué recursos y qué acciones pueden realizar (leer, escribir, modificar, etc.).

Ejemplos: Un empleado autenticado puede tener acceso a ciertos documentos de la institución, pero no a todos. Un administrador de sistema podría tener más acceso que un operador. Un servidor autenticado en una aplicación puede consultar un monto, ver datos informativos, pero no modificar los permisos de otro usuario sin la debida autorización. Una vez autenticado, el sistema consulta qué permisos tiene ese usuario. Si el servidor es un profesor, puede ver y modificar las calificaciones de sus estudiantes. Sin embargo, no tiene acceso a modificar la información de nómina, que es responsabilidad de la Unidad de Recursos Humanos o modificar la carga académica que es responsabilidad de un Director de Departamento Académico

Mejores Prácticas:

- **Contraseñas fuertes y MFA:** La autenticación debe estar respaldada por contraseñas seguras y multifactor para reducir el riesgo de suplantación de identidad.
- **Principio de mínimos privilegios:** Solo se debe otorgar acceso a los recursos estrictamente necesarios para realizar las funciones del trabajo.

- **Revisión periódica:** Los permisos de autorización deben revisarse regularmente para asegurarse de que sean apropiados y coherentes con las responsabilidades actuales del usuario.
- **Auditoría de accesos:** Implementar un sistema de auditoría para registrar todas las actividades de autenticación y autorización, para detectar posibles abusos o accesos indebidos.
- **Cambio de contraseña periódico:** Para usuarios administrativos o personal docente con acceso a información sensible, se recomienda cambiar la contraseña cada 60 a 90 días y, para estudiantes o usuarios generales, el cambio podría ser cada 180 días, aunque depende de la criticidad de los datos a los que acceden.

d) **La Segregación de Funciones.-** Es un principio de seguridad que busca dividir las responsabilidades y los privilegios dentro de una institución para reducir el riesgo de fraude, errores o abusos de poder. Su objetivo principal es evitar que una sola persona controle de forma completa o excesiva un proceso o un conjunto de actividades críticas dentro de una organización. Las actividades que podrían generar un riesgo si se realizan sin supervisión o control cruzado se dividen entre varias personas o sistemas.

Prevención de fraude y errores: El propósito de la segregación de funciones es evitar que una sola persona o entidad tenga la oportunidad de cometer un fraude o un error sin que haya otros controles para detectarlo o prevenirlo.

Supervisión mutua: Cuando las tareas están distribuidas, los empleados supervisan y verifican el trabajo de otros, lo que crea un ambiente de control continuo y fomenta la detección temprana de problemas.

Responsabilidad compartida: Al dividir las responsabilidades entre varios individuos o sistemas, se asegura que ninguna persona tenga acceso a todos los recursos o controles, lo que refuerza la rendición de cuentas y hace más difícil que una persona individual pueda ejecutar acciones fraudulentas.

Ejemplo: Un desarrollador que escribe el código no debe ser el mismo que lo revisa y lo aprueba para su implementación. Las pruebas de seguridad y calidad deben ser realizadas por un equipo distinto al que desarrollo el software para garantizar la objetividad. La Segregación de Funciones es un pilar esencial en la gestión de riesgos dentro de una organización, asegurando que ninguna persona tenga control absoluto sobre todas las partes de un proceso crítico. Al dividir las responsabilidades y establecer controles y auditorías efectivas, se pueden mitigar los riesgos de fraude, errores y abusos, asegurando la integridad y la seguridad de los procesos organizacionales.

e) **La Revisión y Auditoría de Accesos.-** Son mecanismos fundamentales dentro de la gestión de seguridad de la información, cuyo objetivo es asegurar que el acceso a los recursos críticos de una institución sea apropiado, controlado y se mantenga bajo supervisión continua.

Pasos para una Revisión de Accesos Efectiva:

I **Identificación de usuarios y roles:** Obtener una lista de todos los usuarios con acceso a sistemas críticos y sus respectivos roles y privilegios.
II **Revisión de la necesidad de acceso:** Determinar si los accesos actuales son coherentes con las responsabilidades del usuario.
III **Revocación de accesos innecesarios:** Retirar permisos que ya no sean necesarios o que no estén alineados con el rol del usuario.
IV **Evaluación de nuevos roles:** Revisar si los usuarios que han cambiado de rol dentro de la organización tienen accesos acordes con sus nuevas responsabilidades.
V **Documentación y seguimiento:** Registrar los resultados de la revisión de accesos y establecer un plan de acción para resolver cualquier anomalía detectada.

Asimismo, la Auditoría de accesos es el proceso de revisión exhaustiva y sistemática de los registros de acceso y las actividades realizadas por usuarios, sistemas o aplicaciones. Su objetivo es detectar comportamientos anómalos o no autorizados, identificar posibles violaciones de políticas de seguridad, y garantizar que los controles de acceso estén funcionando correctamente.

Objetivos de la Auditoría de Accesos:

I Detectar accesos no autorizados o violaciones de políticas de seguridad.
II Garantizar que los usuarios y sistemas accedan únicamente a los recursos que están autorizados a utilizar.
III Identificar actividades anómalas que puedan indicar posibles intentos de ataque o mal uso de privilegios.
IV Proporcionar evidencia objetiva para informes de cumplimiento regulatorio o en caso de auditorías externas.

Elementos Clave de una Auditoría de Accesos: .

I Recolección de Registros de Acceso: Captura de todos los eventos relacionados con accesos a sistemas y recursos, incluidos accesos exitosos, fallidos y la naturaleza de las acciones realizadas (lectura, escritura, modificación).
II Análisis de Logs: Evaluar los registros para identificar patrones anómalos, intentos de acceso repetidos, o accesos a recursos no esperados.
III Investigación de Incidentes: En caso de detectar accesos sospechosos o violaciones de políticas, iniciar un proceso de investigación para determinar la causa y la gravedad del incidente.
IV Cumplimiento Normativo: Asegurar que la organización cumpla con los requisitos de auditoría establecidos por normativas como SOX, ISO 27001, HIPAA, entre otras.

V Reportes y Acciones Correctivas: Generar reportes detallados de los hallazgos de la auditoría, y en caso de encontrar problemas, implementar acciones correctivas para solucionar las vulnerabilidades detectadas.

Tipos de Auditoria de Accesos:

I Auditoria Interna: Realizada por el propio equipo de seguridad de la organización, enfocada en revisar los accesos y la adherencia a las políticas de seguridad internas.

II Auditoria Externa: Llevada a cabo por una entidad externa o auditoría independiente, generalmente como parte de los requisitos de cumplimiento regulatorio o certificación.

Ejemplos de Auditoría y Revisión de Accesos: Auditoría de Acceso en una Universidad Pública:

I Se revisa quién tiene acceso a sistemas críticos, como los sistemas de gestión académica y bases de datos de estudiantes.

II Se detectan accesos no autorizados por parte de usuarios que han dejado la institución y se revocan dichos accesos.

III La auditoría revela un número elevado de intentos de acceso fallidos a los registros académicos, lo que podría indicar intentos de ataque.

Objetivo de la Revocación de Accesos: El principal objetivo de la revocación de accesos es mitigar el riesgo de accesos no autorizados o indebidos a los recursos de la organización. Esto puede suceder cuando:

I Un empleado cambia de rol o departamento y ya no necesita acceso a ciertos sistemas.

II Un empleado, consultor o contratista finaliza su relación con la organización.

III Un sistema o aplicación ya no está autorizado para interactuar con determinados recursos

Situaciones en las que es Necesaria la Revocación de Accesos:

I Salida de un empleado o contratista: Cuando un empleado o contratista deja la organización, ya sea por renuncia, despido o finalización del contrato, es necesario revocar de inmediato todos los accesos a sistemas, bases de datos y recursos. Esto incluye:
- Cuentas de usuario en aplicaciones internas y externas.
- Accesos a sistemas operativos y redes corporativas.
- Accesos físicos a instalaciones, como oficinas o centros de datos.

II Cambio de rol o departamento: Los empleados que cambian de puesto dentro de la organización pueden no necesitar los mismos accesos que tenían en su función anterior. Los permisos innecesarios deben ser revocados para evitar riesgos, mientras que se otorgan nuevos accesos alineados a su nueva función.

III Finalización de proyectos o contratos temporales: En proyectos temporales o colaboraciones, al finalizar la tarea, es crucial revocar los accesos otorgados a contratistas o colaboradores externos, asegurando que no tengan acceso continuado a los recursos de la organización.

IV Accesos innecesarios detectados en revisiones: Durante las revisiones periódicas de accesos, se puede detectar que ciertos usuarios o sistemas tienen privilegios que ya no son necesarios, lo que indica que deben ser revocados.

V Incidentes de seguridad o comportamiento sospechoso: Si se detecta un comportamiento sospechoso o un posible incidente de seguridad relacionado con un usuario o sistema, los accesos deben revocarse inmediatamente hasta que se realice una investigación.

Pasos para una Revocación de Accesos Efectiva:

I Identificación del usuario o sistema: Determinar qué usuarios, cuentas de servicio o sistemas ya no necesitan acceso. Esto puede hacerse a través de una revisión periódica de accesos o en respuesta a un evento, como la salida de un empleado.

II Inventario de accesos: Realizar un inventario detallado de los accesos que tiene el usuario o sistema. Esto incluye no solo las aplicaciones principales, sino también sistemas secundarios, redes, bases de datos y accesos físicos.

III Revocación inmediata: Ejecutar la revocación de accesos de manera oportuna y eficiente, eliminando los privilegios de todas las cuentas asociadas. Esto incluye:
Desactivar o eliminar cuentas del usuario.
Revocar accesos a redes VPN, sistemas de almacenamiento en la nube, y servidores internos.
Retirar el acceso a credenciales compartidas, como claves SSH o certificados.
Deshabilitar dispositivos de autenticación multifactor (MFA), como tokens o apps de autenticación.
Confirmación de revocación: Verificar que todos los accesos han sido correctamente revocados. En muchos casos, esto puede incluir la revisión de logs de acceso y la comprobación de que el usuario ya no tiene la capacidad de acceder a los sistemas.

IV Documentación: Registrar el proceso de revocación de accesos para auditorias futuras. Esto incluye la fecha y hora de revocación, los sistemas afectados y la confirmación de la eliminación de todos los privilegios.

V Monitoreo Posterior: Después de la revocación de accesos, se debe monitorear la actividad de los sistemas para detectar posibles intentos de acceso por parte de cuentas eliminadas o usuarios desautorizados.

La Revocación de accesos es un proceso fundamental en la gestión de seguridad de la información que consiste en retirar o eliminar los privilegios de acceso a sistemas, datos o recursos cuando estos ya no son necesarios o apropiados.

6.1.3. Protección de la Privacidad de los Estudiantes

- Los datos personales de los estudiantes, tales como nombres, identificaciones, direcciones y calificaciones, se considerarán confidenciales y serán tratados conforme a las normativas de privacidad vigentes, como la Ley de Protección de Datos Personales.
- Se limitará el acceso a los registros académicos y personales a personal autorizado que requiera dicha información para la realización de funciones legítimas.

6.1.4. Seguridad en la Investigación

- Toda la información relacionada con investigaciones en curso será clasificada como confidencial hasta que los resultados sean publicados oficialmente.
- Los investigadores deben implementar medidas de protección para los datos recogidos durante la investigación, como cifrado de archivos, autenticación de acceso y sistemas de respaldo.

6.1.5. Protección Contra Amenazas Internas y Externas

- Se implementarán herramientas de detección y prevención de intrusiones para identificar y mitigar posibles ataques cibernéticos.
- El software antivirus y antimalware deben estar instalados y actualizados en todos los sistemas de la universidad.
- Se garantizará la aplicación de parches de seguridad para vulnerabilidades conocidas de manera oportuna en todos los sistemas críticos.

6.1.6. Uso Aceptable de los Recursos Tecnológicos

- Los recursos tecnológicos de la universidad solo podrán ser utilizados para fines académicos, investigativos y administrativos. El uso personal no autorizado o que contravenga a esta Directiva será considerado una violación de seguridad.
- Queda prohibida la instalación de software no autorizado o aplicaciones que no hayan sido validadas por el departamento de TI.

6.1.7. Copias de Seguridad y Recuperación de Datos

- Se realizarán copias de seguridad periódicas de todos los sistemas y bases de datos esenciales para garantizar la recuperación en caso de pérdida o corrupción de datos.
- Las copias de seguridad deben ser almacenadas en ubicaciones seguras, con controles de acceso adecuados y se realizarán pruebas periódicas de restauración de datos.

6.1.8. Seguridad Física

- Se restringirá el acceso físico a las salas de servidores, centros de datos y oficinas administrativas mediante el uso de sistemas de control de acceso (tarjetas de identificación, registros de entrada, etc.).
- Todo hardware crítico debe ser ubicado en áreas seguras, protegidas contra desastres naturales, robos o accesos no autorizados.

6.2. GESTIÓN DE INCIDENTES DE SEGURIDAD

6.2.1. Notificación y Gestión de Incidentes

- Todos los usuarios (estudiantes, personal docente y administrativos) deben reportar incidentes de seguridad de inmediato al departamento de TI, utilizando los canales designados (correo electrónico, línea directa, portal de incidentes).
- El departamento de TI llevará un registro de todos los incidentes reportados y evaluará su gravedad para determinar la respuesta adecuada.
- El departamento de TI deberá contar con procesos claros para la identificación, respuesta y análisis de incidentes, asegurando que los incidentes se gestionen adecuadamente en el contexto del riesgo institucional

6.2.2. Respuesta y Recuperación

- En caso de un incidente de seguridad, el departamento de TI tomará medidas inmediatas para contener la amenaza, investigar las causas y restaurar los sistemas comprometidos.
- Los incidentes graves, como violaciones de datos, deben ser reportados al Comité de Seguridad y a las autoridades regulatorias correspondientes, según lo exige la normativa.

6.3. CUMPLIMIENTO Y AUDITORÍA

6.3.1. Auditorías Internas y Externas

- Se realizarán auditorias periódicas para evaluar el cumplimiento de la presente Directiva y detectar vulnerabilidades o incumplimientos Las auditorías internas se llevarán a cabo cada seis meses, y las auditorías externas anualmente.
- Evaluación continua de riesgos, la revisión de controles internos y la alineación de objetivos de TI con la estrategia institucional
- Se realizarán auditorias que estén orientadas a garantizar la eficacia, eficiencia, confiabilidad y seguridad de los sistemas de TI.

6.3.2. Sanciones por Incumplimiento

- Cualquier violación de esta Directiva por parte de estudiantes, docentes o personal administrativo procederá en sanciones que pueden incluir la suspensión de acceso a los sistemas de la universidad, medidas disciplinarias o acciones legales, según la gravedad del caso.

6.4. CAPACITACIÓN Y CONCIENTIZACIÓN

- La universidad en coordinación con la Oficina de Tecnologías de la Información, proporcionará capacitación periódica en seguridad de la información para todo el personal y estudiantes, asegurando que comprendan sus responsabilidades y las políticas establecidas.
- Se promoverán campañas de concientización sobre la importancia de la seguridad de la información y las mejores prácticas a seguir.

VII. RESPONSABILIDADES

Son responsabilidades de:

7.1. Comité de Seguridad de la Información

Este Comité, compuesto por representantes de los departamentos de TI, administración, investigación y académico, es responsable de supervisar la implementación, monitoreo y revisión de la Directiva. Debe asegurar que las políticas sean efectivamente comunicadas y aplicadas en toda la institución. El Comité es responsable de:

- **Establecimiento de la Estrategia de Seguridad:** Definir y aprobar la estrategia general de seguridad de la información de la institución, asegurando que se alinee con los objetivos estratégicos de la universidad y con el marco normativo aplicable.
- **Definición y Supervisión de Políticas de Seguridad:** Crear y actualizar políticas de seguridad de la información, en áreas como gestión de accesos, confidencialidad, integridad de datos y protección contra amenazas. Esto incluye monitorear que las políticas sean implementadas adecuadamente.
- **Evaluación y Gestión de Riesgos:** Identificar, analizar y priorizar los riesgos de seguridad, revisando periódicamente el estado de los controles de mitigación y el cumplimiento de los procedimientos para gestionar el riesgo.
- **Supervisión del cumplimiento normativa:** Asegurarse de que la institución cumpla con las normativas legales y regulatorias relevantes, como la ISO 27001, GDPR, leyes nacionales de protección de datos, entre otras. El Comité debe revisar la efectividad del programa de cumplimiento y ajustar medidas, si es necesario.
- **Implementación y control de medidas de seguridad:** Supervisar la implementación de controles técnicos y organizativos, tales como firewalls, encriptación de datos y políticas de contraseñas, asegurando que se ajusten a las políticas de seguridad y respondan adecuadamente a los riesgos identificados.

- **Evaluación de incidentes y respuesta**: Establecer y monitorear un plan de respuesta ante incidentes, evaluando incidentes pasados, asegurándose de que las lecciones aprendidas se integren en la estrategia y promoviendo una cultura de mejora continua en la respuesta a incidentes.
- **Capacitación y concientización en seguridad:** Desarrollar y supervisar programas de capacitación para todos los servidores de la UNSAAC (administrativos y docentes) y estudiantes, promoviendo una cultura de seguridad y asegurando que la comunidad universitaria este al tanto de los riesgos y las prácticas de seguridad.
- **Revisión y mejora continua:** Realizar evaluaciones periódicas de los procesos de seguridad con base en auditoria, nuevos riesgos identificados y cambio en la normativa.

7.2. Departamento de Tecnología de la Información (TI)

La Oficina de Tecnologías de la Información es responsable de implementar las medidas técnicas y operativas necesarias para proteger los activos de información de la universidad. También debe llevar a cabo auditorias de seguridad, gestionar incidentes y realizar el mantenimiento continuo de los sistemas de seguridad.

7.3. Docentes, estudiantes y personal administrativo

Todos los usuarios de los sistemas de información de la universidad son responsables de cumplir con las normas de seguridad establecidas. Deben proteger sus credenciales de acceso, evitar compartir información confidencial sin autorización y reportar incidentes de seguridad.

DISPOSICIONES COMPLEMENTARIAS Y FINALES

PRIMERA.- Los casos no previstos en la presente Directiva, son resueltos por la Unidad de Centro de Cómputo, Oficina de Tecnologías de la Información, Autoridad Universitaria, según corresponda.

SEGUNDA.- La presente Directiva entra en vigencia al día siguiente de su aprobación por Resolución de la Autoridad Universitaria y de su publicación en el Portal de Transparencia Institucional.

Cusco, marzo del 2025.

Aprobado por Resolución R. N° 544-2025 -UNSAAC