POLÍTICA DE SEGURIDAD INFORMÁTICA

UNISANGIL pretende, mediante la Política de Seguridad Informática, garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas de información de la institución, minimizando los riesgos de incidentes de seguridad, protegiendo la privacidad de los usuarios y cumpliendo con las regulaciones y estándares aplicables.

FUNDACIÓN UNIVERSITARIA DE SAN GIL
UNISANGIL
Departamento de Sistemas y TIC

POLÍTICA DE SEGURIDAD INFORMÁTICA UNISANGIL

FIRMADO EN ORIGINAL

JOSÉ MANUEL SERRANO JAIMES
Vicerrector Administrativo y Financiero

FIRMADO EN ORIGINAL

ELIANA MARÍA REMOLINA TORRES
Directora Departamento de Sistemas y TIC

Equipo de trabajo que elaboró este documento:

Sede San Gil:

LUIS FERNANDO MILLAN MORALES, Administrador de Redes y Telecomunicaciones
CARLOS ANDRES GUTIERREZ, Administrador de Servidores
NORBERTO VILLAR SUÁREZ, Asistente de Redes y Telecomunicaciones
CARLOS ACEVEDO CAMARGO, Jefe Taller de Mantenimiento
LUIS DANERY PRADA BUENO, Auxiliar Taller de Mantenimiento
EDWARD CAMILO CIFUENTES MORENO, Administrador de Base de Datos
ELIANA MARIA REMOLINA TORRES, Directora Departamento de Sistemas y TIC
DIEGO ALEXANDER RODRÍGUEZ DURÁN, Coordinador Departamento de Sistemas y TIC- Yopal

Comité Interno de Seguridad informática UNISANGIL

San Gil, 01 de Diciembre del 2025.

TABLA DE CONTENIDO

1. OBJETIVOS

El objetivo central de la Política de Seguridad Informática es presentar de forma coherente y clara a los grupos de interés internos y externos las normas y los procedimientos necesarios para proteger la infraestructura tecnológica y los datos alojados en ella. Para lograrlo, se plantea la planificación, organización, dirección y control de actividades para asegurar la integridad de los recursos informáticos y activos tecnológicos. Esto se llevará a cabo en un marco transparente y definido, con el equipo del Departamento de Sistemas y TIC asumiendo la responsabilidad de gestionar riesgos. También se busca fomentar el compromiso de todo el personal en el proceso de seguridad, acelerando la implementación de controles para fortalecer la protección de activos e información de UNISANGIL en su conjunto.

2. ALCANCE

La Política de Seguridad Informática es aplicable para todos los aspectos administrativos y de control que deben ser cumplidos por el personal administrativo, docente, directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con UNISANGIL, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad del presente documento.

3. TÉRMINOS Y DEFINICIONES

Activo tecnológico: bien o recurso digital o electrónico que una organización utiliza para llevar a cabo sus operaciones y actividades, incluye hardware, software, redes, bases de datos y otros componentes tecnológicos que tienen un valor y contribuyen al funcionamiento eficiente de la organización

Administración de incidentes de seguridad: La administración de incidentes de seguridad se enfoca en evaluar amenazas a la infraestructura de TI. Su objetivo es solucionar rápidamente interrupciones en los servicios, pero también investigar y prevenir causas subyacentes de futuros incidentes, su enfoque se basa en tres pilares fundamentales:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del Departamento de Sistemas y TIC y las medidas de seguridad informática de la institución.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, propiedad que garantiza que la identidad de un sujeto o recurso es la que declara, se aplica a entidades tales como usuarios, procesos y sistemas de información.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados,

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad informática por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una institución, durante el tiempo suficiente como para verse afectada de manera significativa.

Directiva: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evento: Se refiere a un incidente identificado en un sistema, servicio o estado de la red que sugiere una posible violación de la Política de Seguridad Informática, una falla en las salvaguardas, o una situación previamente desconocida que podría ser relevante para la seguridad.

Incidente: Evento único o serie de eventos de seguridad informática inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: La información constituye un importante activo, esencial para las actividades de una institución y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras. Puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Integridad: Implica preservar la precisión y exhaustividad de la información, así como de los métodos de procesamiento. También se refiere a la capacidad de proteger la exactitud y la integridad de los activos tecnológicos.

Inventario de activos: Lista completa de todos los recursos, como bienes físicos, datos, software, documentos, servicios, personas y la reputación de la institución, que tienen valor para la organización y, por lo tanto, deben protegerse de posibles riesgos.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Usuario: En el presente documento se emplea para referirse a directivos, empleados administrativos, docentes, estudiantes, egresados, contratistas, terceros y otros, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de UNISANGIL y a quienes se les otorga un nombre de usuario y una clave de acceso.

Vulnerabilidad: Debilidad en la seguridad informática de una institución que potencialmente permite que una amenaza afecte a un activo.

Ciberseguridad: Conjunto de acciones y medidas orientadas a garantizar la seguridad de la información y la protección de las redes, infraestructuras tecnológicas, sistemas de información y usuarios frente a ciberamenazas. Comprende la prevención, detección, gestión y respuesta frente a incidentes que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de los activos digitales.

Datos Personales: Información vinculada o que pueda asociarse a una persona natural identificada o identificable, de forma directa o indirecta. Incluye datos generales (nombre, identificación, fecha de nacimiento, dirección, contacto) y datos sensibles como información de salud, orientación política, información biométrica o

cualquier dato cuyo tratamiento pueda afectar la intimidad del titular. Aplica a cualquier formato (texto, imagen, sonido, numérico) y a cualquier soporte (físico o digital), conforme a la Ley Estatutaria 1581 de 2012.

Principio de autenticidad: Mandato según el cual debe garantizarse que el origen de la información y las identidades asociadas a ella corresponden verdaderamente a quien aparece como emisor o autor. Se relaciona con el principio de no repudio, que busca impedir que un usuario desconozca la autoría de una acción realizada en el sistema o su vinculación con un dato o transacción.

Principio de confidencialidad: Obliga a asegurar que la información solo sea accesible a usuarios autorizados conforme a sus funciones, y que no sea revelada, transferida o puesta a disposición de terceros sin autorización o fundamento legal.

Principio de disponibilidad: Exige que la información y los sistemas que la soportan estén accesibles y operativos cuando los usuarios autorizados lo requieran, garantizando la continuidad de los procesos institucionales. Se articula con el principio de resiliencia, orientado a asegurar la capacidad de recuperación y restablecimiento de los sistemas tras un incidente que afecte temporalmente su operación.

Principio de integridad: Supone que la información debe mantenerse completa, exacta y protegida frente a alteraciones no autorizadas. Garantiza que los datos no han sido modificados, eliminados o manipulados por personas o procesos no habilitados para ello.

Principio de trazabilidad: Busca que sea posible identificar en todo momento quién accede a la información, qué acciones realiza, en qué momento y en qué condiciones. Incluye el seguimiento de los estados, movimientos y transformaciones de la información durante su ciclo de vida, como mecanismo de control, auditoría y responsabilidad.

4 Política de Seguridad Informática

UNISANGIL se compromete a implementar protocolos y estrategias para proteger la información institucional y ofrecer orientación en seguridad informática. Estas medidas se aplican a todos los usuarios de la institución, de esta manera, se procura establecer un entorno seguro y confiable para la comunidad académica.

4.1 Estructura organizacional de seguridad informática.

- Se establece el Comité Interno de Seguridad informática, definiendo los roles, funciones y responsabilidades correspondientes.
- El Departamento de Sistemas y TIC, debe aplicar los roles, funciones y responsabilidades de operación y administración de los sistemas de información existentes por la institución.
- Los proyectos de UNISANGIL que involucren temas tecnológicos y sistemas de información deben incluir en su planificación y desarrollo el seguimiento de la Política de Seguridad Informática, la evaluación de riesgos y la implementación de controles correspondientes.

4.2 Seguridad Informática para el talento humano.

- Los contratistas y proveedores deberán otorgar consentimiento para el manejo de sus datos personales, conforme al Acuerdo de Confidencialidad de UNISANGIL y a la Política Institucional de Tratamiento de Datos Personales. De igual manera, el personal administrativo y docente deberá firmar dicho acuerdo y participar en los procesos de capacitación sobre seguridad informática.

- UNISANGIL, a través del Departamento de Sistemas y TIC, proporciona a los usuarios un espacio de almacenamiento en el servidor institucional destinado al resguardo de información relevante para el ejercicio de sus funciones. Este espacio garantiza la disponibilidad de la información en caso de daño o sustitución del equipo asignado. Los usuarios deberán copiar la información necesaria en la carpeta designada y abstenerse de almacenar en los equipos información de carácter personal o no institucional.
- El Departamento de Sistemas y TIC instalará únicamente software legalmente adquirido y autorizado.
- El uso de programas sin licencia o no aprobados por dicho Departamento constituye una infracción a las políticas de seguridad y puede generar consecuencias legales y disciplinarias para el usuario.
- UNISANGIL no se hace responsable por los softwares, copias o programas no autorizados instalados o ejecutados en los equipos asignados al personal administrativo, docente o contratista.
- El Departamento de Sistemas y TIC no asumirá responsabilidad por el uso de dispositivos de almacenamiento externo (memorias USB, discos duros, DVD, CD, tabletas, teléfonos móviles u otros), debido a los riesgos que pueden derivarse de su conexión a los equipos institucionales.
- Los recursos tecnológicos y el software asignados al personal administrativo, docente y contratista son de uso exclusivo para el cumplimiento de funciones institucionales y de su entera responsabilidad en cuanto a custodia, conservación y buen uso.
- Los usuarios son responsables de la información que administran en los equipos asignados a su actividad laboral y deben abstenerse de almacenar, copiar o transferir información no institucional o de carácter personal.
- Los usuarios solo tendrán acceso a los datos y recursos expresamente autorizados por UNISANGIL y responderán disciplinaria y legalmente por la divulgación o manipulación no autorizada de la información institucional.

- Los dispositivos electrónicos, como computadoras e impresoras, deben emplearse únicamente para los propósitos aprobados por la Institución. Cualquier evento o incidente que amenace la seguridad informática deberá ser notificado de inmediato a la mesa de ayuda (GLPI) del Departamento de Sistemas y TIC.
- Los jefes de las diferentes dependencias de UNISANGIL, en conjunto con el Comité Interno de Seguridad Informática, deberán propiciar actividades de sensibilización y capacitación sobre las medidas preventivas que los usuarios finales deben observar en el manejo de los recursos informáticos.
- Los usuarios deberán aplicar prácticas esenciales de seguridad informática, tales como evitar la instalación de aplicaciones innecesarias, bloquear dispositivos al ausentarse, proteger documentos confidenciales y emplear contraseñas seguras, de conformidad con las directrices del Departamento de Sistemas y TIC.
- Toda labor desarrollada por personal administrativo, docente o contratista que implique el uso de los recursos tecnológicos institucionales y el tratamiento de información de UNISANGIL deberá realizarse dentro de las instalaciones institucionales, salvo autorización expresa de la Dirección del Departamento de Sistemas y TIC para el desarrollo remoto controlado.

4.3 Equipo de Trabajo Departamento de Sistemas y TIC.

- El personal del Departamento de Sistemas y TIC no debe dar a conocer su clave de usuario a otros sin previa autorización de la Dirección de dicho Departamento.
- El Departamento de Sistemas y TIC realizará respaldo a bases de datos y servidores según se contempla en el procedimiento de administración de respaldo de base de datos y servidores.
- Los administradores de sistemas adscritos al Departamento de Sistemas y TIC deben adherirse a las políticas de cambio de contraseñas y emplear un procedimiento de resguardo seguro de claves. Estas claves solo deben estar accesibles para el Director de este Departamento.

- Para el cambio o retiro de equipos del personal administrativo y docente, se sigue el protocolo definido por el Departamento de Sistemas y TIC para el borrado seguro de la información.
- El personal del Departamento de Sistemas y TIC no debe conceder privilegios especiales a los usuarios en las estaciones de trabajo sin la debida autorización de la Dirección del Departamento y sin el registro correspondiente en el sistema de la mesa de ayuda (GLPI).
- La instalación y/o configuración de todo servidor conectado a la red será responsabilidad del Departamento de Sistemas y TIC.
- Los profesionales del Departamento de Sistemas y TIC no tienen la autorización para alterar o eliminar registros (logs) de sus propias actividades ni de usuarios y sistemas de información. También, para ello el Departamento de Sistemas y TIC implementará medidas de seguridad para prevenir cambios no autorizados en los registros.
- El software adquirido, debe ser únicamente instalado en los equipos y servidores de la institución.
- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
- Todos los protocolos y servicios que no se requieran en los servidores; no se deben permitir a menos que sea solicitado y aprobado oficialmente por la Dirección del Departamento de Sistemas y TIC.
- El Departamento de Sistemas y TIC, no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de propiedad de UNISANGIL, En el caso de los equipos adquiridos mediante leasing, se les realizará mantenimiento preventivo y correctivo en software.
- El Departamento de Sistemas y TIC tendrá protocolos de seguridad con el propósito de restringir el acceso a sitios web que contravengan la ley o las políticas de UNISANGIL.
- Se realizará un control por parte de la Dirección del Departamento de Sistemas y TIC y desde el área de Auditoría Interna, que permita realizar revisiones periódicas y documentadas de los derechos de acceso de los usuarios en los sistemas de información utilizados en la institución.
- Con la debida autorización de las directivas institucionales, el equipo del Departamento de Sistemas y TIC de UNISANGIL, respaldado por la asesoría de un externo en Hacking Ético, llevará a cabo exhaustivas pruebas de vulnerabilidad en los sistemas de información y comunicaciones de la institución.
- El Departamento de Sistemas y TIC aplicará el cifrado de disco duro como parte de su procedimiento interno, el cual se somete a una revisión y actualización anual.
- El Departamento de Sistemas y TIC debe establecer un programa de seguimiento integral para la gestión de recursos tecnológicos, incluyendo proyecciones de crecimiento y expansión para garantizar la disponibilidad de servicios.

4.4 Uso de los activos tecnológicos.

- Los activos tecnológicos pertenecen a UNISANGIL y deberán emplearse exclusivamente para fines laborales, académicos o institucionales. Su utilización con propósitos personales, comerciales o distintos al objeto institucional se encuentra prohibida y constituye una infracción a las políticas de seguridad informática.
- Los usuarios son responsables del uso, custodia y conservación de los equipos, software y demás recursos tecnológicos asignados, debiendo garantizar su integridad y correcto funcionamiento.
- El Departamento de Sistemas y TIC realizará monitoreo y seguimiento técnico de los equipos y del software instalado en cada dependencia, conforme al cronograma de mantenimiento preventivo y correctivo. Dicho monitoreo podrá incluir revisiones o auditorías preventivas en los términos del numeral 4.11 de la presente Política.

- Todos los requerimientos de aplicativos, sistemas, licencias, cuentas o equipos informáticos deberán solicitarse mediante la mesa de ayuda (GLPI), con la justificación correspondiente. Ningún usuario está autorizado para instalar, modificar o sustituir software o hardware sin la aprobación previa del Departamento de Sistemas y TIC.
- Antes de la salida o préstamo de equipos tecnológicos institucionales, el Departamento de Sistemas y TIC aplicará el protocolo de protección, respaldo y seguridad, dejando registro de trazabilidad y verificación del estado físico y lógico de los activos.
- Todo cambio, actualización o modificación a la infraestructura informática deberá estar controlado, documentado y autorizado, conforme a los procedimientos establecidos en el proceso de Gestión de Infraestructura Tecnológica.
- El uso inadecuado de los activos tecnológicos o la alteración de su configuración sin autorización constituirá falta disciplinaria grave, sancionable conforme a los reglamentos internos y a los contratos aplicables.

4.5 Uso de mensajería instantánea, correo electrónico y redes sociales.

- No está permitido enviar mensajes que contengan amenazas de código malicioso o que puedan perjudicar la integridad, reputación o seguridad de personas, instituciones o la propia UNISANGIL.
- La información que se publique o difunda por medios electrónicos o redes sociales a nombre personal por parte de funcionarios, contratistas o colaboradores de UNISANGIL, se considera fuera del alcance de esta Política, por lo que cualquier daño o perjuicio derivado será de responsabilidad exclusiva del autor.
- Cualquier información institucional que se genere y destine a ser compartida en redes sociales deberá contar con la autorización de los jefes de área o responsables de comunicación, garantizando el uso de lenguaje institucional, adecuado y respetuoso.
- Está prohibido utilizar el nombre, logotipo o imagen institucional en redes sociales o espacios digitales para actividades personales, comerciales o contrarias a la filosofía de UNISANGIL, así como responder comentarios o publicaciones en nombre de la institución sin autorización.
- El correo electrónico institucional es el medio oficial de comunicación interna y externa de UNISANGIL. Su uso está restringido a fines laborales, académicos o administrativos y deberá efectuarse conforme a las disposiciones contenidas en el Manual de Uso del Correo Electrónico Institucional.
- Todo mensaje, archivo o documento transmitido, almacenado o recibido mediante cuentas institucionales se considera información de carácter institucional y propiedad de UNISANGIL.

4.6 Seguridad de red, equipos y centro de datos

- El Departamento de Sistemas y TIC debe implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento.
- Si se requiere un nuevo punto de voz y/o datos por movimientos de usuarios o cualquier otra circunstancia, se debe realizar la solicitud al Departamento de Sistemas y TIC, a través del GLPI, quien determinará los requisitos técnicos de la red conservando siempre el concepto de Monomarca y las normas técnicas para tal fin.
- Los dispositivos personales no pertenecientes a UNISANGIL solo pueden acceder a servicios limitados para invitados o visitantes. Es necesario conectar estos dispositivos a los puntos de acceso permitidos y designados por el Departamento de Sistemas y TIC.
- Ningún usuario tiene la autorización para manipular física ni lógicamente los equipos activos de red, ni tampoco conectar dispositivos de red no autorizados. La responsabilidad de configurar y mantener estos

equipos recae en el Departamento de Sistemas y TIC, específicamente en el área de redes y telecomunicaciones.

- El acceso al centro de datos está restringido al personal autorizado únicamente. Es necesario llevar un registro de las personas que visitan el centro de datos, utilizando una planilla de registro que debe ser diligenciado al comienzo y al finalizar la visita.
- La conexión remota a la red de área local de la Institución debe realizarse a través de una conexión VPN segura suministrada por el Administrador de Redes y Telecomunicaciones, la cual debe ser aprobada, registrada y auditada.
- UNISANGIL está obligada a establecer sistemas de alimentación eléctrica redundante y a mantener acuerdos de soporte y mantenimiento planificado para los equipos críticos, generando informes detallados sobre las tareas de mantenimiento preventivo y correctivo realizadas.
- El Departamento de Sistemas y TIC es responsable de la gestión, el mantenimiento y la salvaguardia de la infraestructura tecnológica del centro de datos. Esta infraestructura se fundamenta en la norma ANSI/TIA-942 y se apoya en los pilares esenciales de telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico. Además, se respalda con un firewall o dispositivo de seguridad perimetral para asegurar la protección de la red institucional.
- Los equipos que necesiten salir de UNISANGIL para reparación deben contar con autorización y asegurarse de que no contienen información crítica según la clasificación de datos.
- El Departamento Sistemas y TIC por medio del directorio activo mantendrá los escritorios de los equipos de cómputo libres de información, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- El Departamento de Sistemas y TIC cuenta con un procedimiento de gestión de cuentas de usuario destinado a definir los niveles de acceso de los usuarios a los servicios y sistemas de información de la institución.

4.7 Adquisición de recursos tecnológicos.

- Cualquier sistema de información adquirido o desarrollado por UNISANGIL debe incluir manuales actualizados. Estos manuales deben comprender una sección técnica que detalle la estructura interna y los componentes del sistema, junto con otra sección que describa a los usuarios y los procedimientos necesarios. Además, es fundamental que cumplan con medidas y políticas de seguridad establecidas.
- Los sistemas de información deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como el usuario, fecha y hora en que se realizó.
- Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los softwares de cómputo, para garantizar su confiabilidad.
- El Departamento de Sistemas y TIC deberá realizar pruebas de funcionamiento y de seguridad en los sistemas, en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación en producción.
- El Departamento de Sistemas y TIC, será la única dependencia autorizada para realizar copia de seguridad del software original.
- Para obtener o actualizar software, se debe presentar una solicitud al Departamento de Sistemas y TIC con justificación. El Departamento evaluará y aprobará las propuestas presentadas.
- El software que se adquiera a través de los proyectos o programas académicos debe quedar a nombre de UNISANGIL
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local.
- Los equipos se deben adquirir de línea corporativa incluyendo garantía 3-3-3.

- Para equipos críticos y de alto de costo como servidores, equipos de comunicaciones, equipos activos de red, y otros, se requiere un programa de mantenimiento preventivo y correctivo. Esto también debe incluir el suministro de repuestos una vez que la garantía haya expirado.
- El Departamento de Sistemas y TIC llevará a cabo una evaluación técnica de los recursos que se pretenden adquirir, invitando a diversos proveedores a participar. Posteriormente, se seguirá el procedimiento de compras aprobado por UNISANGIL.

4.8 Uso de dispositivos móviles

- Los dispositivos móviles de propiedad de UNISANGIL (teléfonos móviles, teléfonos inteligentes, tabletas, portátiles y demás equipos portátiles) son herramientas institucionales destinadas exclusivamente para facilitar el trabajo y las comunicaciones oficiales de los usuarios autorizados.
- El uso de los dispositivos móviles deberá limitarse a fines académicos, administrativos o laborales relacionados con las funciones institucionales. Se prohíbe su utilización con fines personales, comerciales o ajenos al objeto institucional.
- Toda la información generada, almacenada o transmitida a través de los dispositivos móviles institucionales constituye información de carácter institucional y propiedad exclusiva de UNISANGIL.
- Los dispositivos móviles deberán integrarse a las directivas locales del sistema operativo y controles de seguridad definidos por el Departamento de Sistemas y TIC, incluyendo políticas de actualización, contraseñas seguras y bloqueo automático.
- Los usuarios solo podrán instalar aplicaciones autorizadas por el Departamento de Sistemas y TIC y deberán emplear la tarjeta SIM institucional asignada. Queda prohibido el uso de cuentas personales o aplicaciones que comprometan la seguridad de la información institucional.
- En caso de requerir la instalación de aplicaciones adicionales, la solicitud deberá presentarse a través de la mesa de ayuda (GLPI), acompañada de la justificación funcional correspondiente y la validación de seguridad.
- Los dispositivos móviles deberán contar con mecanismos de bloqueo, encriptación y respaldo de información según las directrices de seguridad definidas por el Departamento de Sistemas y TIC.
- El Departamento de Sistemas y TIC podrá realizar verificaciones y controles técnicos preventivos sobre los dispositivos institucionales con el fin de garantizar la integridad y seguridad de la información.
- La pérdida, daño, uso indebido o manipulación no autorizada de los dispositivos móviles institucionales deberá reportarse de inmediato a la mesa de ayuda (GLPI) y constituirá falta grave conforme al Reglamento Interno de Trabajo, al régimen contractual o disciplinario correspondiente.
- Se prohíbe expresamente el uso del correo institucional para fines personales, comerciales, proselitistas, cadenas, reenvíos no autorizados o almacenamiento de información no relacionada con las funciones institucionales.
- UNISANGIL, a través del Departamento de Sistemas y TIC, podrá realizar verificaciones y controles técnicos preventivos sobre las cuentas de correo electrónico y servicios de mensajería institucional, con el fin de proteger la seguridad de la información y prevenir incidentes de fuga o pérdida de datos.
- Los usuarios deberán mantener la confidencialidad de sus credenciales y reportar de inmediato cualquier intento de acceso no autorizado o incidente de seguridad a la mesa de ayuda (GLPI) del Departamento de Sistemas y TIC.
- El incumplimiento de las disposiciones sobre uso del correo electrónico o redes sociales constituye falta disciplinaria grave, conforme a lo previsto en los reglamentos internos, contratos y normas legales aplicables.

4.9 Entrega de información institucional.

- En el evento de retiro o traslado del personal administrativo o docente, previa notificación del Departamento de Talento Humano, el Departamento de Sistemas y TIC realizará análisis exhaustivo de los activos de tecnológicos, diligenciando el acta correspondiente.
- La información se almacena y administra en la plataforma interna designada por UNISANGIL para el resguardo de información.
- Se debe seguir el procedimiento de borrado seguro para equipos finales, a fin de garantizar la copia de la información para la institución y la eliminación de la información almacenada en el disco local.

4.10 Gestión de la Continuidad de Seguridad de la Información

- El Departamento de Sistemas y TIC, elaborará el plan de recuperación ante desastres para los sistemas de información y comunicaciones de UNISANGIL, el cual debe incluir mínimo procedimientos, condiciones de seguridad, recuperación y retorno a la normalidad.
- El Departamento de Sistemas y TIC, debe analizar y establecer los requerimientos mínimos de redundancia para los sistemas de información críticos de UNISANGIL, junto con la plataforma tecnológica que los soporta, de igual forma deberá investigar, evaluar y probar las soluciones de tecnología que supla la necesidad de la institución.

4.11 Propiedad, custodia y auditoría de la información institucional (Aplicación transversal)

- Este numeral tiene carácter transversal y aplica a toda la comunidad universitaria de UNISANGIL, incluidos directivos, personal administrativo, docente, contratistas, estudiantes, egresados, aliados institucionales y cualquier tercero que, por razón de sus funciones o vínculos, acceda, genere o administre información institucional o haga uso de los recursos tecnológicos de la Institución.
- UNISANGIL reconoce la información generada, recibida o almacenada en sus sistemas, equipos, servidores, plataformas, redes, mensajería y correos institucionales como un activo estratégico y patrimonio informacional de carácter institucional, sujeto a los principios de confidencialidad, integridad, disponibilidad y legalidad.
- Toda información creada, tratada o transmitida mediante los recursos tecnológicos de UNISANGIL constituye propiedad institucional, sin perjuicio de los derechos morales de autor que correspondan al usuario. El uso de los medios tecnológicos y de comunicación institucional deberá limitarse exclusivamente a fines académicos, administrativos o laborales propios de la Institución, quedando prohibido su empleo con fines personales, políticos, comerciales o ajenos a su objeto misional.
- UNISANGIL, a través del Departamento de Sistemas y TIC, podrá realizar verificaciones, auditorías y controles preventivos sobre los equipos, sistemas, correos electrónicos, redes y demás recursos institucionales, con el propósito de garantizar la seguridad, confidencialidad y continuidad de la información. Estas acciones no se consideran vulneración de la privacidad del usuario, sino ejercicio legítimo de las funciones de protección y salvaguarda de los activos informáticos institucionales.
- Al finalizar cualquier relación laboral o contractual, el Departamento de Sistemas y TIC procederá a la reasignación o actualización de la cuenta institucional asociada al cargo o función, garantizando el respaldo y la trazabilidad de la información de valor institucional. Cuando la persona sea también estudiante o egresado, su cuenta académica personal permanecerá activa por tratarse de un perfil distinto.

- Los usuarios deberán velar por el adecuado manejo, confidencialidad y custodia de la información institucional a la que tengan acceso, absteniéndose de divulgarla, eliminarla, copiarla o transferirla sin autorización. El incumplimiento de estas disposiciones constituye falta grave y podrá dar lugar a sanciones disciplinarias o contractuales, sin perjuicio de las acciones civiles, penales o administrativas a que haya lugar.

5. PROCESO DISCIPLINARIO

Las investigaciones disciplinarias que se realicen al personal administrativo o docente están bajo la jurisdicción del proceso de talento humano, y se enfocan en actos que contravienen las normativas de seguridad informática estipuladas por UNISANGIL. Estas normativas se encuentran respaldadas por acuerdos de confidencialidad firmados individualmente por todos los empleados de la institución.

Los demás usuarios, como estudiantes, egresados, contratistas, terceros y otros, deben sujetarse a los procesos disciplinarios establecidos por las leyes, estatutos y regulaciones promulgadas por el gobierno nacional, así como a lo establecido por los reglamentos de UNISANGIL.

6. CUMPLIMIENTO

Los diferentes aspectos contemplados en este documento son de obligatorio cumplimiento para todos los usuarios de UNISANGIL. En caso de que se violen la Política de Seguridad informática, ya sea de forma intencional o por negligencia, UNISANGIL tomará las acciones disciplinarias y legales correspondientes.

La Política de Seguridad Informática debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

7. CONTROLES

La Política de Seguridad Informática esta soportada en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este documento. Los usuarios pueden consultar los procedimientos a través del aplicativo de ACADEMUSOFT, módulo de gestión documental, proceso de Gestión de infraestructura tecnológica.

7.1. Requisitos básicos de seguridad de la información

Para la gestión diaria de la seguridad de la información, la institución aplicará los siguientes requisitos básicos, cuyo desarrollo se implementará mediante políticas, estándares y procedimientos específicos:

- Incorporación de requisitos de seguridad desde el diseño y por defecto.
- Prevención, detección, respuesta y preservación ante incidentes de seguridad.
- Vigilancia continua y reevaluación periódica de los controles.
- Separación y diferenciación de responsabilidades.

- Organización e implementación del proceso integral de seguridad.
- Análisis y gestión de riesgos asociados a los activos de información.
- Gestión del personal en materia de seguridad de la información.
- Autorización, control y monitoreo de accesos.
- Protección física y ambiental de las instalaciones.
- Adquisición de productos y contratación de servicios con criterios de seguridad.
- Principio de mínimo privilegio.
- Mantenimiento de la integridad y actualización del Sistema de Información.
- Protección de la información almacenada y en tránsito.
- Prevención frente a riesgos derivados de sistemas interconectados.
- Registro de actividades, auditoría técnica y detección de código malicioso.
- Gestión integral de incidentes de seguridad.
- Garantía de continuidad operativa y recuperación ante desastres.
- Mejora continua del proceso de seguridad.
- Seguridad en la cadena de suministro y proveedores.
- Confiabilidad, seguridad y resiliencia de los sistemas y servicios.

Cada uno de estos requisitos será desarrollado mediante los procedimientos y políticas internas aprobadas institucionalmente.

La documentación generada en materia de seguridad de la información será gestionada, estructurada y conservada conforme a los procedimientos documentales institucionales, atendiendo la normativa vigente y los estándares nacionales e internacionales aplicables. Los requisitos básicos y sus desarrollos se proyectan sobre toda la comunidad institucional y son obligatorios para todos los usuarios que interactúan con los activos de información de UNISANGIL.

8. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad (Statement of Applicability - SOA) referenciado en la cláusula 4.2.1j del estándar ISO 27001 es un documento que lista los objetivos y controles que se van a implementar en la entidad, así como las justificaciones de aquellos controles que no van a ser implementados.

Para el caso específico de UNISANGIL, se toma como referente el cumplimiento de la norma ISO 27001, para cada uno de los controles establecidos relacionados con la gestión de la seguridad informática que este estándar específico, y una vez se complete este análisis ya se puede realizar la declaración de aplicabilidad.

9. MARCO NORMATIVO

ISO 27001 norma internacional de Seguridad de la Información

Constitución Política de Colombia 1991.
Código Penal Colombiano - Decreto 599 de 2000
Ley 906 de 2004, Código de Procedimiento Penal.
Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
Ley 594 de 2000 - Ley General de Archivos.
Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas
Data y se regula el manejo de la información contenida en base de datos personales.
Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
Ley 1581 de 2012, "Protección de Datos personales".
Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 2000 y ley 1437 de 2011
Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012
Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”

10. RESPONSABLE DEL DOCUMENTO

Departamento de Sistemas y TIC - UNISANGIL