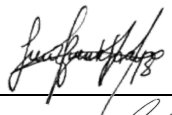
GTI-SGI-POL-01

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA

Elaborado por:	Lucía Isabel Puente Loayza **Jefe de Seguridad de la Información y Riesgos**	Firma: 
Revisado por:	José Luis Yupán Cardenas **Subgerente de Operaciones de Tecnología**	Firma: 
Aprobado por:	Katya Hurtado Siu **Gerente Corporativo de Tecnología y Servicios**	Firma: 

CONTENIDO

1. Objetivo

La política de Seguridad de la Información tiene por objetivo proteger los recursos de información de la Universidad Científica del SUR (CIENTIFICA) y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de minimizar los riesgos de daño y asegurar la confidencialidad, integridad, disponibilidad y respaldo de la información, así como garantizar la continuidad de los sistemas de información.

2. Alcance

Esta política es aplicable a todo el personal y terceros que tengan relación con la Universidad, que tengan acceso, utilicen o traten los activos de información de la institución.

3. Documentos a consultar

3.1. No Aplica

4. Información Complementaria

4.1. La Política de Seguridad de la Información de CIENTIFICA ha sido elaborada tomando como marco de referencia la norma ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos", cuya finalidad principal es asegurar la confidencialidad, integridad y disponibilidad de la información gestionada en la Institución.

5. Lineamientos Generales

5.1. Las Políticas de Seguridad de la Información identifican responsabilidades y establecen los objetivos para una protección apropiada y consistente de los activos de información de CIENTIFICA.

5.2. El Comité de Seguridad de la Información se encargará de los esfuerzos necesarios para la difusión, consolidación y cumplimiento de la presente política. A tal efecto, gestionara la seguridad de la información relacionada con actividades, metas y programas, en concordancia con la normatividad vigente y siguientes lineamientos:

- El establecimiento de mecanismos para preservar la confidencialidad, integridad y disponibilidad de la información de la institución, garantizando su transparencia.
- La continua identificación, manejo y mitigación de los riesgos de seguridad de la información que son relevantes para la institución.
- La respuesta efectiva y adopción de acciones correctivas ante incidentes relacionados con la seguridad de la información y ciberseguridad.
- La comunicación oportuna de las políticas y procedimientos de seguridad definidos,

asegurando que sean comprendidos y se encuentren disponibles para todos los interesados.

- El fortalecimiento de los valores y el compromiso de todo el personal de velar por el cumplimiento de las presentes políticas.

5.3. El Comité de Seguridad de la Información de CIENTIFICA reconoce que la Seguridad de la Información es un objetivo primordial para el desarrollo del negocio, el mismo que debe ser impulsado y apoyado por todos los miembros de la organización.

5.4. Lo dispuesto en la presente política es de uso obligatorio y entrará en vigor a partir de la fecha de su aprobación, permaneciendo vigente hasta la aprobación y/o publicación de otro documento de similar jerarquía que lo sustituya.

5.5. Se debe asegurar que la política es comunicada, entendida e implementada en toda la institución y es de conocimiento del personal y partes interesadas.

5.6. La Política de Seguridad de la Información será revisada por lo menos una vez al año o en caso ocurran cambios significativos en la organización, con el objetivo de garantizar su idoneidad, adecuación y efectividad continua.

5.7. El Comité de Seguridad de la Información posee una metodología de gestión de riesgos aprobada, la misma que sirve para identificar, cuantificar y tratar los riesgos de Seguridad de la Información a fin de poder establecer los controles apropiados para los riesgos identificados y llevarlos a niveles aceptables para la institución.

5.8. Se debe asegurar que los riesgos son monitoreados y que se realiza el seguimiento a los riesgos tratados para medir la efectividad de los controles implementados. La evaluación de riesgos debe realizarse como mínimo una vez al año y cada vez que se identifiquen cambios significativos dentro de la organización.

5.9. Se deben de cumplir todos los requisitos legales definidos para la Institución, así como todo requisito de seguridad de la información aplicable.

5.10. El responsable de Recursos Humanos, en coordinación con el responsable del Comité de Seguridad de la Información, planificará anualmente las actividades de capacitación y concienciación en Seguridad de la Información para el personal.

5.11. Se debe integrar la seguridad de la información en los métodos de gestión de proyectos de la organización para asegurar la identificación y tratamiento de los riesgos de seguridad de la información y ciberseguridad como parte de los proyectos, es decir, los riesgos asociados a la ausencia de Confidencialidad, Integridad y Disponibilidad. Esto se aplica a cualquier proyecto, sin importar su carácter. Para la gestión de riesgos se utilizará la Metodología aprobada dentro de la institución.

6. Lineamientos Específicos

6.1. RESPONSABILIDADES

6.1.1. Comité Evaluador

- Está conformado por:
  - Gerente General
  - Gerente corporativo de Finanzas y Gestión del Talento
  - Gerente corporativo de Tecnología y Servicios
  - Subgerente del área legal
- Deliberar sobre las medidas disciplinarias a ejecutarse ante el incumplimiento de la Política de Seguridad de la Información.

6.1.2. Comité de Seguridad de la Información

- Está conformado por:
  - Gerente corporativo de Tecnología y Servicios
  - Oficial de Seguridad de la Información
  - Subgerente de Operaciones de Tecnología
  - Jefe de Educación Virtual
- Revisar, aprobar, establecer y comunicar el alcance, las políticas, los planes, los objetivos e información documentada relacionada con la Seguridad de la Información.
- Supervisar la implementación y efectividad de la Política de Seguridad de la Información.
- Definir los niveles de riesgo, aprobar el plan de tratamiento de los riesgos, los riesgos residuales y supervisar la eficacia de los controles implementados.
- Supervisar el cumplimiento de los controles organizativos y técnicos aplicados para cumplir con la preservación de la Seguridad de la Información.
- Revisar la eficacia de los controles de seguridad de la información aplicados a intervalos planificados.
- Impulsar la concientización, formación y capacitación en Seguridad de la Información.
- Aprobar los roles y responsabilidades específicas para la Seguridad de la Información en toda la institución.
- Asegurar la integración y alineamiento de los requisitos de la Seguridad de la Información a los procesos de la institución.
- Dirigir y apoyar a las personas para que contribuyan a la aplicación de la Política de Seguridad de la Información.
- Coordinar, debatir y proponer soluciones para la mejora de la Seguridad de la Información, además del cumplimiento de requisitos legales, contractuales y de seguridad de la Información, promoviendo la mejora continua.
- Comunicar las actualizaciones y cambios sobre la Política de Seguridad de la Información a las partes interesadas.

6.1.3. Oficial de Seguridad de la información

- Gestionar y mantener actualizada la Política de Seguridad de la Información.
- Aplicar una metodología de análisis de riesgo, en función a los lineamientos establecidos por el Comité de Seguridad de la Información.
- Proporcionar apoyo al Comité de Seguridad de la Información en todo lo relacionado a la Seguridad de la Información.
- Proponer ante el Comité de Seguridad de la Información las modificaciones a la documentación perteneciente a las políticas y procedimientos de seguridad de la información.
- Programar auditorías enfocadas en la seguridad de la información, para evaluar las prácticas de Seguridad de la Información.
- Supervisar que la información y los todos los sistemas en el ámbito del alcance estén adecuadamente protegidos.
- Velar por el cumplimiento de la Seguridad de la Información.

6.1.4. Responsable del control de accesos

- Gestionar las cuentas de los usuarios con accesos a los diversos sistemas de información de CIENTIFICA.
- Asegurar que sólo las personas autorizadas cuenten con acceso a los recursos de TI, de acuerdo a su perfil definido.
- Asegurar que los sistemas de información tienen los niveles de confidencialidad, integridad y disponibilidad requeridos por la organización.
- Realizar las revisiones de accesos a los recursos de TI, oportunamente y de manera planificada

6.1.5. Personal de CIENTIFICA

- Conocer y cumplir con lo establecido en la Política de Seguridad de la información aprobada y vigente.
- Notificar los incidentes de seguridad de la información conforme a los canales de comunicación establecidos.
- Mantener la confidencialidad sobre toda la información, datos de carácter personal y de terceros a los que se tenga acceso en virtud de su trabajo. Obligación que subsistirá incluso después de finalizar su relación con la organización.
- Acceder únicamente a la información que han sido autorizados para el desarrollo de sus funciones en función de su perfil de puesto o responsabilidades.
- Queda terminantemente prohibido hacer entrega, por cualquier medio y sin autorización, de listados o de bases de datos a personas no autorizadas, ya sea de forma total o parcial.
- Participar en las pruebas del plan de contingencia, ante eventuales caídas de los sistemas de información y aplicaciones informáticas.
- Velar por la seguridad y confidencialidad de la información contenida en sus equipos, especialmente cuando se encuentren fuera de las instalaciones de la institución.

6.2. SANCIONES POR INCUMPLIMIENTO

6.2.1. CIENTIFICA se reserva el derecho de tomar medidas disciplinarias ante el personal que incumpla con lo dispuesto en la Política de Seguridad de la Información, conforme a las disposiciones señaladas en los documentos normativos de la organización, sin perjuicio de las acciones civiles y/o penales que pudieran corresponder. Todos los incumplimientos serán elevados al Comité Evaluador.

6.2.2. Asimismo, si se comprueba que un colaborador ha accedido, modificado, eliminado, substraído o perdido información a la que no estuvo autorizado a tratar podrá suponer causa suficiente de apertura de proceso disciplinario, conforme a la tabla que se muestra a continuación:

Clase de Información	Proceso Disciplinario
Confidencial	Si se demuestra que un colaborador ha modificado, eliminado, sustraído o extraviado información confidencial se abrirá proceso y se le retirarán los privilegios de acceso. Investigada la causa, se determinará si corresponde la suspensión temporal o despido considerando lo dispuesto en la normatividad vigente que establece las causas justificadas de despido.
Interna	Si un colaborador hace un mal uso de información interna, de la que carece de privilegios, se le dará un aviso de advertencia y se tendrá en cuenta en su Ficha de Evaluación Profesional.
Pública	No existe un proceso disciplinario con respecto a este tipo de Información.

6.3. CLASIFICACIÓN DE LA INFORMACIÓN

6.3.1. Se debe establecer criterios y niveles adecuados de clasificación y tratamiento de la información asegurando que las personas que requieran acceso a la misma lo hagan bajo el principio de necesidad de saber y en línea con las funciones que desarrollan.

6.3.2. El dueño/propietario de la información deberá evaluar el nivel aplicable considerando los siguientes criterios:

- Posible impacto o consecuencias para la organización en caso de divulgación de la información a personas o grupos no autorizados.
- Limitaciones legales o por regulación que sean aplicables (ejemplo: protección de datos personales, secreto de las telecomunicaciones, secreto bancario, etc.)

6.3.3. En base a ello se ha establecido niveles de clasificación de la información, la misma que puede ser tratada como confidencial, interna o pública, conforme lo establecido a continuación.

Tipo	Descripción
Confidencial	Esta información por su grado de sensibilidad para la organización puede generar pérdidas económicas, problemas legales o daños al derecho de la privacidad y datos personales. Cualquier persona u organización que solicite acceder a este tipo de información, deberá solicitarlo por los canales de comunicación establecidos y la institución determinará si puede ser revelada de conformidad con la normatividad vigente.
Interna	Es la información que genera, utiliza o controla la organización continuamente. Las atribuciones de generación, modificación o eliminación están limitadas de acuerdo con las funciones o roles de cada trabajador. Cada trabajador tiene la responsabilidad de custodiar la información concedida en el medio que fuese, digital o físico.
Pública	Es la documentación que la organización considera que no genera daño alguno y puede ser de conocimiento público.

6.3.4. Se debe considerar que de manera predeterminada se aplicará el nivel de clasificación de información confidencial cuando se trate de:

- Información de datos personales
- Estrategia de la organización o proyectos estratégicos o de innovación
- Datos comerciales o financieros cuya divulgación pudiese afectar los intereses de la Universidad.
- Información tecnológica estratégica
- Datos judiciales e investigaciones internas

6.3.5. El nivel de clasificación de la información podrá ser reevaluado por el dueño/propietario de la información decidiendo si cambia el nivel aplicable.

6.3.6. Para cada nivel de clasificación se definen algunas medidas y lineamientos de seguridad que permitan proteger la información a través de todo su ciclo de vida:

Tipo	Medidas para tratamiento
Confidencial	• Se considera que en caso de divulgación no autorizada existe impacto muy alto con daños graves en el negocio, la reputación, la rentabilidad, las personas y otros valores de la Universidad. • Debe estar etiquetada con la marcación "Información Confidencial", siendo obligatorio el uso de marca de agua y etiqueta en encabezado y al pie de página del documento. • El propietario de la información define el nivel de acceso a un grupo limitado de personas bajo el principio de "necesidad de saber". • El envío de información considerada confidencial debe ser cifrada o protegida con contraseña y limitado únicamente a las personas con necesidad de acceso o conocimiento de esta. Para el caso de terceros, se deberá asegurar que existe un acuerdo de confidencialidad. • La información debe estar almacenada en recursos con acceso restringido, tanto a nivel físico como lógico, asegurando el aislamiento y confidencialidad de los datos. • La información debe ser eliminada por procesos de borrado seguro o físicamente destruido, en caso de información en papel o dispositivos de almacenamiento externo (CD, DVD, USB, etc.)

Interna	• Se considera que en caso de divulgación no autorizada existe impacto medio o bajo en el negocio, la reputación, la rentabilidad, las personas u otros valores de la Universidad. • Debe ser adecuadamente etiquetada con la marcación "Información Interna", incluyendo una marca de agua o etiqueta en encabezado o al pie de página del documento. • El propietario de la información define el nivel de acceso bajo el principio de "necesidad de saber". • La información puede ser enviada internamente sin restricción. Sin embargo, el envío de esta a personas fuera de la organización está limitada sólo a las personas que el propietario autorice bajo el principio de "necesidad de saber". • La información puede ser eliminada por procesos regulares de borrado, no siendo exigible un borrado seguro.
Pública	• Se considera que, en caso de divulgación no autorizada, no existe impacto en el negocio, la reputación, la rentabilidad, las personas u otros valores de la Universidad. • Debe ser adecuadamente etiquetada, siempre que sea posible. • No existe restricción en el acceso a esta información. • No existe restricción para el envío de la información, ya sea de forma interna o externa. • La información puede ser eliminada por procesos regulares de borrado, no siendo exigible un borrado seguro.

6.3.7. Es responsabilidad de todo el personal y terceros, asegurar que la información sea clasificada en base a los niveles establecidos y de aplicar las medidas de seguridad correspondientes para su protección, siendo particularmente definidas las siguientes funciones:

a. Propietario de la Información: Es el responsable del proceso, área o proyecto a la que la información pertenece y tiene bajo su responsabilidad:

- Clasificar la información de acuerdo con su sensibilidad, el grado de impacto al negocio y el nivel de riesgo en caso de utilización inadecuada o acceso no autorizado.
- Definir e identificar los permisos de uso y acceso a la información, de acuerdo con el principio de "necesidad de saber".
- Asegurar que se adoptan las medidas de seguridad, tanto físicas como tecnológicas, para garantizar el nivel de confidencialidad de la información de la que es propietario.
- Gestionar y garantizar que se dé un adecuado uso y tratamiento a la información de la cual es propietario.

b. Usuario de la Información: Es quien requiere acceder a la información para la ejecución de actividades vinculadas a sus funciones y tiene bajo su responsabilidad:

- Tomar las medidas necesarias para preservar la seguridad y la integridad de la información a la que tiene acceso (ya sea en files, archivos, contratos, etc.), de acuerdo con su clasificación.
- Mantener la confidencialidad de la información a la que acceda para el cumplimiento de las tareas encargadas.
- Dar adecuado uso y tratamiento a la información a la que tenga acceso en el desempeño de sus funciones.

6.4. CONTROL DE ACCESOS

6.4.1. Se debe garantizar que sólo el personal y terceros con necesidad justificada de acceso a los recursos de CIENTIFICA, tendrán los permisos para hacerlo. Por defecto, todo acceso está denegado a menos que sea expresamente autorizado.

6.4.2. Todos los accesos a los recursos de información de CIENTIFICA deben basarse en la necesidad y perfil de puesto del usuario, y se debe tomar en cuenta los siguientes aspectos:

- Acceso basado en Roles.
- Los requerimientos de seguridad de cada una de las aplicaciones considerando siempre el principio de menor privilegio.
- Identificación de toda la información relacionada a las aplicaciones y los riesgos a las que se encuentren expuestas.
- Legislación pertinente y cualquier tipo de obligación contractual en cuanto a la limitación de acceso a los datos o servicios.
- Uso de perfiles de usuarios estandarizados definidos según perfil de puesto.
- Segregación de funciones y roles.
- Requisitos para la autorización formal de las solicitudes de acceso.
- Revisión periódica de los controles de acceso.
- Revocación de los derechos de acceso.
- Administración de derechos de acceso

6.4.3. La modificación o revocación de accesos a los recursos de información se darán de forma inmediata al cese del personal. En caso de cambio de posición se deben retirar los accesos previamente asignados.

6.4.4. Se debe asegurar que todos los usuarios tengan una cuenta de usuario individual nombrada para acceder a los servicios de red y recursos de información de CIENTIFICA, con el fin de tener trazabilidad de las acciones de cada cuenta de usuario.

6.4.5. Toda solicitud de acceso deberá registrarse a través de la herramienta de gestión de servicios de TI y deberá contar con aprobación del jefe de área y de la jefatura de Seguridad de la Información.

6.4.6. Al personal de CIENTIFICA se les creará su usuario con contraseña temporal de inicio de sesión para el acceso a las distintas aplicaciones internas, considerando su perfil de puesto.

6.4.7. El personal de CIENTIFICA debe obligatoriamente configurar su método de autenticación multifactor (MFA) preferido para la autenticación en su cuenta institucional.

6.4.8. El personal de CIENTIFICA debe obligatoriamente cambiar las contraseñas temporales de inicio de sesión entregadas, por una contraseña compleja considerando los siguientes criterios:

- Longitud mínima de 8 caracteres.
- Debe contar al menos con 1 letra mayúscula, minúscula, números y al menos un carácter especial (*.,%@$#!)
- Por seguridad, no deben incluir el uso de palabras y nombres comunes en la composición de la contraseña, como: Cientifica, UCSUR, UCS, Password, Admin y

nombres propios, en mayúsculas o minúsculas y secuencias numéricas relacionadas con meses, años u otros, como: 12345678, Cientifica*2025, UCS!12345, Maria@2025, Enero%2025, o cualquier composición similar.

6.4.9. Las contraseñas son de uso personal e intransferible. Ningún trabajador de CIENTIFICA deberá solicitar las contraseñas de otros trabajadores ni compartir sus credenciales.

6.4.10. Las contraseñas de acceso a los sistemas y aplicaciones deben cambiarse con una periodicidad 90 días y deben ser distintas.

6.4.11. Las contraseñas no deben almacenarse en texto plano en los sistemas, bases de datos o aplicaciones de CIENTIFICA, deben aplicarse mecanismos de cifrado para prevenir incidentes de seguridad asociados a la pérdida de confidencialidad de estas.

6.4.12. No se debe utilizar la función de recordar contraseñas en ninguna de las aplicaciones proporcionadas o requeridas por la institución.

6.4.13. No deben usar las contraseñas de la organización para sistemas externos como correos personales y plataformas web de servicios de streaming u otros (Netflix, Spotify, Apple Music, etc.) no vinculados con CIENTIFICA.

6.4.14. Se debe bloquear la cuenta institucional cuando se identifiquen 4 intentos fallidos reiterados o conexiones desde ubicaciones geográficas sospechosas.

6.4.15. El personal de CIENTIFICA debe tomar las precauciones para proteger su contraseña. En caso de no recordar la contraseña o se produzca el bloqueo de sesión deben comunicarlo según los canales establecidos para poder restablecerla conforme al procedimiento formal.

6.4.16. En caso los trabajadores tengan alguna sospecha de conocimiento de su contraseña por otro usuario, deben cambiarla inmediatamente y comunicarlo.

6.4.17. Las contraseñas no deben estar escritas en texto plano en medios de fácil extravío o divulgación, como cuadernos, notas, archivos no protegidos en espacios compartidos o locales en equipos informáticos.

6.4.18. Las aplicaciones, sistemas, plataformas o servicios de red habilitados para CIENTIFICA ya sean por desarrollo propio o adquiridos a terceros, deberán tener configuradas estas directrices, así como módulos para la gestión de acceso, configuración de roles y reportería/auditoría. Siempre que sea posible deberán utilizar integración con nuestro dominio institucional (SSO).

6.4.19. El área de Recursos Humanos debe notificar a la Gerencia de Tecnología y Servicios el cese del personal de CIENTIFICA o los cambios de puesto o área del personal en la institución.

6.4.20. Las cuentas de usuario del personal de CIENTIFICA que cese sus labores en la institución deberán ser desactivadas en un plazo no mayor a 24 horas desde la notificación del cese y todos sus permisos de acceso a sistemas, aplicaciones u otros servicios de Tecnología revocados, sin excepción. Podrán emplearse mecanismos automatizados o manuales para dicho fin.

6.4.21. La cuenta permanecerá deshabilitada por un máximo de 30 días posterior al cese. Durante este periodo el buzón podrá seguir recibiendo correos por lo que se activará una notificación automática indicando la indisponibilidad de la cuenta y brindando el correo del jefe directo del empleado para cualquier comunicación.

6.4.22. El bloqueo y revocación de accesos será aplicable a:

- Acceso al inicio de sesión en los dispositivos otorgados al empleado
- Acceso a la red corporativa
- Acceso a correo electrónico y otras dependencias (OneDrive, MS Teams, Sharepoint, etc.)
- Acceso a internet o Wi-Fi
- Acceso a sistemas y aplicaciones corporativas

6.4.23. Al finalizar el plazo establecido la cuenta será eliminada, incluyendo archivos almacenados, correos electrónicos o reuniones grabadas. Sólo podrá postergarse la eliminación, por un plazo no mayor a 7 días útiles, a solicitud formal del jefe inmediato superior del empleado, siempre que este pedido se realice dentro de los 30 días de desactivación de la cuenta, a través de la herramienta de gestión de servicios de TI (Canal "Te Ayudamos").

6.4.24. Una cuenta eliminada no podrá ser recuperada, salvo se cumpla con los siguientes criterios:

- La solicitud se realice dentro de los 30 días luego de la eliminación.
- La recuperación se justifique por: reincorporación del personal, investigación o procesos legales en curso o error administrativo.

6.4.25. En el caso de terceros cuyas actividades finalicen previo a la fecha de expiración de su contrato o del plazo establecido para sus labores, el responsable de la gestión del tercero deberá solicitar la revocación inmediata de sus accesos.

6.4.26. En casos de cambio de puesto se deberán retirar los permisos que ya no sean necesarios para el desempeño de las funciones del personal de CIENTIFICA.

6.4.27. La Gerencia de Tecnología y Servicios tiene la potestad de desactivar a cualquier usuario que haga mal uso de los permisos concedidos o que se relacione a algún incidente de seguridad o genere un riesgo a la seguridad de la información de CIENTIFICA.

6.5. POLÍTICAS DE PANTALLA Y ESCRITORIO LIMPIO

6.5.1. El personal de CIENTIFICA debe mantener el escritorio de trabajo ordenado y libre de documentación. En caso tengan documentación impresa o en medios de almacenamiento clasificada como confidencial, impresa y/o en dispositivos de almacenamiento extraíble deberán asegurarlos bajo llave en gabinetes u otro mobiliario asignado para resguardo, cuando no estén siendo utilizados o no se encuentre presencialmente en su puesto de trabajo.

6.5.2. El personal de CIENTIFICA que por la naturaleza de sus funciones requieran imprimir documentos con información clasificada como confidencial deben acercarse a la impresora para imprimirlos con su usuario personal asignado y retirarla inmediatamente de la impresora.

6.5.3. Todas las estaciones de trabajo y equipos portátiles de CIENTIFICA deben estar configuradas para bloquear automáticamente el equipo una vez transcurrido los 10 minutos de inactividad.

6.5.4. El personal de CIENTIFICA debe bloquear la estación de trabajo o equipo asignado cada vez que se retire de su puesto de trabajo o se deje el equipo desatendido. Ejemplo: con las teclas Windows + L, Alt+Ctrl+Del o Alt+Ctrl+Supr en Windows.

6.5.5. Los archivos de mayor importancia no deberán ser guardados localmente en el equipo asignado, sino que se deberán almacenar en el servidor de archivos o repositorios destinados para dicho fin.

6.5.6. El acceso remoto desatendido no está permitido, el usuario quien concede la autorización debe permitir y supervisar el acceso a su equipo mientras se brinde servicios de soporte, ya sea por personal de CIENTIFICA o externos.

6.6. USO ACEPTABLE DE ACTIVOS

6.6.1. Los equipos y sistemas de CIENTIFICA, incluidos entre otros, equipos informáticos, dispositivos móviles, software, sistemas operativos, aplicaciones, servidores, equipos de red, impresoras, cuentas institucionales que facilitan acceso al correo electrónico, plataformas de colaboración (Teams, Sharepoint, etc.), navegación por internet, conexión VPN, SFTP u otros servicios de red se utilizarán únicamente para los fines y propósitos para los que fueron asignados y puestos a disposición del personal de CIENTIFICA.

6.6.2. El personal de CIENTIFICA es completamente responsable de todas las actividades realizadas con sus cuentas de red, correo electrónico y sistemas de información asociados a la organización. Los empleados no deben tener expectativa de privacidad con respecto al uso de los equipos o sistemas asignados por CIENTIFICA para el desarrollo de sus actividades laborales, siendo este sujeto a fiscalización para asegurar el cumplimiento de esta política y ante la investigación de eventos o incidentes.

6.6.3. El uso de la red, computadoras e impresoras es exclusivo para fines laborales.

6.6.4. El uso de Internet y correo electrónico por parte del personal de CIENTIFICA queda restringido a fines estrictamente laborales.

6.6.5. El personal de CIENTIFICA que por la naturaleza de sus funciones requiere hacer uso de herramientas para conferencias o seminarios web debe limitarse únicamente a transmitir contenido que sea acorde a su reunión y no sea considerada confidencial.

6.6.6. El personal de CIENTIFICA tiene el deber de reportar de inmediato el robo, pérdida o divulgación no autorizada de equipos o información de propiedad de la organización.

6.6.7. La conexión a la red institucional de aulas, laboratorios y red administrativa está limitada únicamente a dispositivos de CIENTIFICA, no permitiéndose la conexión de equipos personales.

6.6.8. Los alumnos, docentes, invitados y proveedores podrán conectarse a redes de navegación WiFi destinadas para uso de equipos personales o externos a la organización. Cualquier excepción a este lineamiento deberá ser aprobado por el Oficial de Seguridad de la Información y siempre que exista justificación válida.

6.6.9. Queda terminantemente prohibido utilizar el internet para descargar archivos de ocio, entrar a redes sociales, blog, radio y televisión en línea, videos en línea, juegos, chat, contenido pornográfico, descarga de software, evasión de proxy, software ilegal y piratería

informática.

6.6.10. Está prohibido enviar mensajes de correo electrónico que contengan datos de carácter personal o de terceros sin mecanismos de protección adecuada que faciliten la vulneración del nivel de confidencialidad de los mismos.

6.6.11. No se utilizará el correo electrónico para enviar o recibir mensajes con contenidos inapropiados, discriminatorios, difamatorios o dañinos que puedan atentar contra los derechos y libertades de las personas.

6.6.12. No se debe adjuntar en los correos electrónicos archivos que superen la capacidad de 25MB. El usuario es responsable de gestionar y usar adecuadamente el espacio designado para su buzón de correo electrónico y otros recursos asignados por la institución.

6.6.13. No se debe de abrir correos electrónicos, ni acceder a links, ni descargar documentos adjuntos cuyo emisor sea desconocido. Toda sospecha debe ser alertada al equipo de Seguridad de la Información.

6.6.14. El personal de CIENTIFICA debe tener especial cuidado en la publicación de fotografías de la institución (tomadas al interior de la institución), esto debido a que pueden contener información confidencial o interna como cronogramas de proyectos, oportunidades de negocio, entre otras.

6.6.15. Únicamente se podrán instalar, en las estaciones de trabajo y computadoras portátiles proporcionadas por CIENTIFICA, las aplicaciones permitidas por la organización, por lo que queda prohibido el uso de software no autorizado.

6.6.16. La Gerencia de Tecnología es la única responsable de la instalación de software en los equipos de CIENTIFICA y debe aplicar controles para evitar que los usuarios puedan instalar software válido o no autorizado en sus equipos.

6.6.17. Por seguridad y mantenimiento de la red, todos los servicios de tecnologías de la información se encuentran sujetos a monitoreo y análisis de tráfico. En caso de detectarse un mal uso de los recursos de parte de los usuarios serán sancionados según lo que corresponda.

6.6.18. CIENTIFICA se reserva el derecho de realizar inspecciones y auditorías para asegurar el cumplimiento de estas directivas.

6.7. DISPOSITIVOS MÓVILES

6.7.1. El personal de CIENTIFICA que utilice celulares, provistos por la empresa, no deberá almacenar en el equipo móvil información confidencial.

6.7.2. Solo el personal que posee equipos celulares otorgados por la empresa podrá configurar el correo electrónico en tales dispositivos.

6.7.3. En caso de pérdida de un computador portátil (laptop) y celulares, el incidente deberá ser comunicado inmediatamente a la organización, según los canales establecidos.

6.8. ELIMINACIÓN DE DOCUMENTOS Y UNIDADES DE ALMACENAMIENTO

6.8.1. El propietario/dueño de información es el encargado de gestionar la eliminación de forma segura de los medios de almacenamiento (físico o lógico).

6.8.2. Toda información contenida en papel o en dispositivos de almacenamiento que contengan información clasificada como confidencial, y se desee eliminar, debe ser destruida de modo que sea imposible su recuperación.

6.8.3. De ser necesario, se podrá contratar a través del área de Logística una empresa especializada en destrucción segura de información con entrega de certificación correspondiente.

6.9. PROTECCION CONTRA EL MALWARE

6.9.1. Se debe adoptar las medidas necesarias para la prevención, detección y eliminación de malware a nivel de la red, servidores, estaciones de trabajo y equipos portátiles.

6.9.2. El personal de CIENTIFICA no debe abrir correos electrónicos sospechosos, ni acceder a links, ni abrir, descargar o ejecutar archivos adjuntos con extensiones desconocidas (.exe, .vbs, .bat, etc.) y cuando el remitente no sea de confianza. Ante duda, contactarse con el equipo de Seguridad de la Información.

6.9.3. Se debe asegurar que todas las estaciones de trabajo y equipos portátiles de la organización estén protegidas con una solución antimalware con capacidad de actualización automática de firmas, no permitiendo que los usuarios deshabiliten localmente el software en los dispositivos protegidos.

6.9.4. Se deben implementar medidas de control de software malicioso a nivel perimetral.

6.9.5. Se debe asegurar que el sistema operativo y los aplicativos de las estaciones de trabajo, servidores y equipos portátiles tengan las últimas actualizaciones de seguridad (parches) con la finalidad de evitar la explotación de vulnerabilidades técnicas.

6.9.6. Se deben implementar controles que eviten o detecten el uso de software no autorizado, ingreso a sitios web maliciosos o uso de dispositivos de almacenamiento extraíble no autorizado expresamente por CIENTIFICA, incluidos memorias USB o discos externos portátiles.

6.9.7. En caso de detección de software malicioso en la red se deben tomar las acciones necesarias para garantizar su contención, evitar su propagación y asegurar su erradicación.

6.10. SEGURIDAD EN EL DESARROLLO

6.10.1. Todo desarrollo de aplicaciones o sistemas para la atención de necesidades de la institución deberá cumplir con los lineamientos de la presente política y pasará a ser parte de la propiedad intelectual de CIENTIFICA.

6.10.2. Los requerimientos para desarrollo de nuevas aplicaciones o mejoras a los existentes deberán incorporar criterios y controles de seguridad siendo estos abordados desde la fase inicial del desarrollo y formando parte del alcance y documentación del proyecto.

6.10.3. Se debe implementar una metodología de desarrollo seguro siguiendo las mejores prácticas de la industria para el diseño, arquitectura, construcción, configuración y funcionamiento de las aplicaciones. Es recomendable, más no limitativa, la aplicación de las guías de desarrollo del proyecto abierto de seguridad de aplicaciones web (OWASP).

6.10.4. Para prevenir errores, pérdida, modificación o uso no autorizado de la información en los sistemas y aplicaciones de CIENTIFICA se deben incorporar los siguientes controles:

a. Acceso y Autenticación de Usuario

- Toda aplicación o sistema deberá contar con controles de autenticación que permita identifica plenamente a los usuarios.
- Deberá incorporar módulos para la gestión de accesos (alta, baja y modificación), configuración de roles, configuración de políticas de contraseña y mecanismos de autenticación multifactor (MFA), cuando no sea posible la integración con nuestro dominio (SSO).

b. Validación de Entrada de Datos

- La entrada de datos en los sistemas debe tener mecanismos de validación para comprobar si son correctos.
- Limitar los campos a rangos específicos de datos de entrada asociado al tipo de variable, para detectar caracteres inválidos, valores fuera del rango establecido o datos faltantes.
- Validación de la integridad de los datos ingresados.
- Comprobación o detección de entrada de código malicioso.
- Mecanismos de respuesta ante errores de validación, con mensajes genéricos sin exposición de información interna.

c. Controles de Procesamiento Interno

- El diseño de los sistemas y aplicaciones debe incluir controles internos para minimizar y detectar errores de los datos, en caso exista un fallo en el procesamiento de estos.
- Se deben implementar mecanismos de validación de integridad en el intercambio de información entre sistemas y aplicaciones.

d. Validación de Salida de Datos

- La salida de datos debe ser validada por los interesados para comprobar si son correctos y adecuados.
- Los sistemas o aplicaciones deben proveer información suficiente para que el usuario u otro sistema de procesamiento determine la exactitud, totalidad y estado de la información.

e. Protección de Datos de Prueba

- No está autorizado el uso de datos productivos en entornos de prueba, salvo autorización expresa del Oficial de Seguridad de la Información.
- Los datos que requieran ser utilizados en ambientes de prueba deben ser seleccionados adecuadamente garantizado el cifrado o anonimización de información sensible.

f. Separación de Ambientes

- Los ambientes de desarrollo, pruebas y producción deben contar con sistemas e infraestructura independiente para reducir los riesgos de acceso o cambios no autorizados en los entornos de operación regular.

g. Registros de Auditoría

- Las aplicaciones o sistemas deben contar con mecanismos para el registro de pistas de auditoría en todas las operaciones consideradas sensibles y de un alto impacto.
- Los registros de auditoría deben almacenar:
  - Fecha y hora de la operación
  - Usuario que accede y realiza la operación
  - Operación Realizada
  - Atributos modificados
  - Dispositivo desde donde se ejecutó la operación (deseable hostname o IP privada o pública del equipo).
- El tiempo de retención de las pistas de auditoría deberá definirse desde el inicio del desarrollo.

h. Control de acceso al código fuente

- El acceso al código fuente de las aplicaciones de CIENTIFICA es de carácter restringido según el principio de mínimo privilegio. Es deseable para el acceso a los repositorios que se tenga activo mecanismos de autenticación multifactor (MFA).
- El acceso debe brindarse de forma granular a los proyectos, carpetas o ramas que sean necesarias, bajo los roles definidos y autorizados por la Gerencia de Tecnología y Servicios y el Oficial de Seguridad de la Información.
- Todo cambio en el código debe tener trazabilidad mediante sistemas de control de versiones.
- Se deben implementar medidas para la revisión del código obligatorias antes de integrar cambios con las ramas principales.
- Los repositorios de código fuente deben ser respaldados periódicamente.

6.10.5. Se debe garantizar la aplicación de las mejores prácticas en el ciclo de vida de desarrollo de software que incluyan:

- Evitar incluir credenciales, claves o secretos en el código fuente.
- No dejar datos reales referenciados como comentario en el código fuente.
- Realizar pruebas de seguridad (estáticas y dinámicas)
- Gestión de cambios documentado

6.10.6. En el caso de tercerización o subcontratación de las actividades de desarrollo de software se debe asegurar una adecuada supervisión y seguimiento de la calidad de los entregables obligando a los proveedores al cumplimiento de los lineamientos de esta política y las indicaciones de la Gerencia de Tecnología y Servicios o quien esta designe como gestor de la relación con el tercero.

6.11. GESTION DE VULNERABILIDADES

6.11.1. Se deberá contar con procesos y procedimientos establecidos para asegurar la identificación, investigación y remediación de vulnerabilidades específicas y emergentes que puedan afectar la operación de los ambientes productivos, a través de la ejecución de servicios de escaneo periódicos de vulnerabilidades y procesos de Ethical Hacking y PenTesting por personal competente, formalmente autorizado y bajo supervisión del equipo de Seguridad de la Información.

6.11.2. Se deberá asignar responsabilidades en las tareas para la aplicación de la remediación de las vulnerabilidades identificadas garantizando la participación de las áreas de la Gerencia de Tecnología correspondientes.

6.11.3. Según la evaluación de criticidad de la vulnerabilidad, se deberá gestionar la aplicación de parches de seguridad y la actualización de versiones, asegurando pruebas previas al despliegue en entornos productivos. Sin perjuicio de lo anterior, deberá considerar los tiempos definidos para la subsanación:

Criticidad	Detalle	Tiempo máximo de subsanación
Crítico	Nivel de prioridad extrema, requiere acción urgente e inmediata	15 días
Alto	Nivel de prioridad mayor, requiere acción en corto plazo	30 días
Medio	Nivel de prioridad media, requiere acción a mediano plazo, puede aplicarse control compensatorio	90 días
Bajo	Nivel de prioridad menor, puede planificarse con acciones a largo plazo. No compromete el sistema o la infraestructura.	180 días

6.11.4. Las vulnerabilidades remediadas deberán ser re-evaluadas para garantizar que estas fueron adecuadamente cerradas.

6.12. SEGURIDAD DE LA RED

6.12.1. CIENTIFICA se obliga a la aplicación de una arquitectura de red segura que contemple:

- Segmentación de redes por niveles de criticidad
- Separación de entornos (producción, testing y desarrollo)
- Zonas desmilitarizadas (DMZ) cuando se trabajen servicios expuestos a internet.

6.12.2. Se debe aplicar controles de acceso seguro a la red mediante autenticación robusta (incluyendo autenticación multifactor – MFA), listas de control de acceso (ACL), políticas de firewall y navegación, en donde corresponda.

6.12.3. Con el fin de mitigar riesgos e impactos de intrusiones, abuso o uso indebido de la red que pudiera ocasionar un incidente de seguridad, se debe aplicar controles y soluciones de

protección perimetral contra intrusiones que permita detectar, informar y evitar la ocurrencia de ataques no autorizados a la red y los recursos o sistemas de información gestionados por CIENTIFICA, incluidos intentos de ataques de penetración, por denegación de servicio o intentos excesivos de acceso.

6.12.4. CIENTIFICA habilitará protección firewall en sus redes, entre los servidores y puertas de enlace (gateways) con exposición a la red pública, de modo que sólo sea habilitado los protocolos de comunicación necesarios para permitir y procesar las peticiones desde o hacia Internet.

6.12.5. En el caso de requerir conexión remota a la red que alberga los recursos de información de la Universidad se debe procurar la habilitación de conexiones remotas mediante canales seguros (VPN) y únicamente al personal autorizado.

6.12.6. Con el fin de asegurar la posibilidad de investigación de eventos o incidentes y recopilación de evidencias se debe mantener registros de actividad de los dispositivos de red y almacenarlos como mínimo por un período de 3 meses.

6.12.7. Se debe asegurar que toda la información y datos transmitidos por red se encuentren protegidos mediante cifrado garantizando la confidencialidad e integridad de estos contra la divulgación y manipulación no autorizada.

6.12.8. La Subgerencia de Operaciones de Tecnología deberá documentar, evaluar y sustentar cualquier cambio en los entornos productivos, asegurando que la actividad sea previamente autorizada por los responsables del Comité de Cambios o quienes se designe para dicha tarea.

6.13. SEGURIDAD DE LOS SERVIDORES Y BASES DE DATOS

6.13.1. Con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información en bases de datos se deberá almacenar los datos confidenciales de forma cifrada (por ejemplo, datos personales, contraseñas, etc.).

6.13.2. Se debe restringir el acceso físico y lógico a las bases de datos, archivos e información en general, asegurando sólo la conexión de usuarios previamente autorizados y siempre que la necesidad justifique el acceso.

6.13.3. Proteger el acceso a las bases de datos y archivos de datos a través de controles de autenticación que como mínimo incluyan la combinación de identificador de usuario y contraseña robusta.

6.13.4. Asegurar que los servidores que se destinen para la habilitación de los servicios de Tecnología cumplan con configuraciones seguras, deshabilitando usuarios por defecto o cambiando las contraseñas que vienen de fábrica, desactivando servicios no utilizados, habilitando herramientas de monitoreo y protección en el dispositivo y garantizando la aplicación regular de parches y actualizaciones del sistema, siguiendo las recomendaciones del fabricante.

6.13.5. Con el fin de asegurar la posibilidad de investigación de eventos o incidentes y recopilación de evidencias se debe mantener registros de actividad y auditoría de las bases de datos y almacenarlos como mínimo por un período de 3 meses.

6.13.6. Asegurar el respaldo de la información siguiendo los lineamientos establecidos en el punto 6.15 Respaldo y Recuperación, de la presente política.

6.13.7. Todo acceso privilegiado debe ser revocado inmediatamente al finalizar la relación laboral o cambio en funciones y en el caso de cuentas de servicio debe asegurarse el cambio de la contraseña.

6.14. GESTION DEL CAMBIO

6.14.1. La Gerencia de Tecnología y Servicios es responsable de la ejecución de los cambios en los servicios de Tecnología que se encuentran bajo su administración.

6.14.2. Todo cambio en los entornos productivos deberá ser justificado y documentado a través de una solicitud en la herramienta de gestión de servicios de TI generada por las áreas usuarias de CIENTIFICA.

6.14.3. El área usuaria debe registrar la solicitud de modificación, ya sea por un ticket de requerimiento o de incidente, proporcionando el mayor detalle posible para que la Gerencia de Tecnología pueda realizar el análisis de factibilidad, así como de riesgo e impacto asociado al cambio.

6.14.4. Los encargados del desarrollo o promotores del cambio deberán planificar y documentar las actividades a realizar, así como gestionar las pruebas y validación previa del área usuaria solicitante del cambio, garantizando que el cambio no genere interrupción de los servicios de Tecnología.

6.14.5. La Gerencia de Tecnología y Servicios es responsable de habilitar entornos de prueba que permitan validar los cambios antes de su puesta en producción, cuando sea posible.

6.14.6. El área usuaria solicitante del cambio es responsable de realizar las pruebas y validaciones de que los cambios requeridos se han aplicado conforme a su solicitud en los entornos de prueba.

6.14.7. Los cambios en los entornos productivos deberán ser aprobados por los responsables del Comité de Cambios, designado por la Gerencia de Tecnología y Servicios en sus procedimientos asociados.

6.14.8. Se debe establecer ventanas de cambio para permitir la ejecución de este con un impacto mínimo en la disponibilidad de los servicios de Tecnología y la operación de CIENTIFICA, en la medida de lo posible. Todo cambio que genere indisponibilidad de los servicios de Tecnología debe ser previamente comunicado a los interesados, informando el periodo de tiempo en el que se recuperará el servicio.

6.14.9. Todo cambio debe considerar un plan de marcha atrás (rollback) el cual podrá ejecutarse en caso el cambio no tenga los efectos deseados y genere impacto en la disponibilidad de los servicios de Tecnología.

6.14.10. Cualquier excepción al proceso de gestión de cambios deberá ser autorizado por la Gerencia de Tecnología y Servicios o los responsables que esta designe en sus procedimientos asociados.

6.15. RESPALDO Y RECUPERACIÓN DE LA INFORMACIÓN

6.15.1. Las copias de respaldo de la información de CIENTIFICA deben ser realizadas, registradas y controladas periódicamente. Estas copias de seguridad se deben de realizar considerando la criticidad de la información.

6.15.2. La frecuencia de las copias de restauración se realizará en base a la importancia y sensibilidad de la información almacenada.

6.15.3. Las copias de respaldo de la información considerada como crítica o confidencial para la institución deberán ser realizadas en su totalidad y con una frecuencia mínima de una vez al día.

6.15.4. Las copias de respaldo deben realizarse con herramientas automatizadas o por procesos manuales que permitan:

- Gestión de acceso para usuarios privilegiados en la herramienta.
- Resguardo en línea y fuera de línea, asegurando su protección y disponibilidad ante ataques que comprometan la infraestructura tecnológica de la institución.
- Almacenamiento en repositorios físicos o virtuales en el ambiente tecnológico que custodia el activo o fuera de este.
- Cifrado de las copias de respaldo
- Trazabilidad y auditoría de la gestión de las copias de respaldo o restauración

6.15.5. Se deben de realizar pruebas de restauración a las copias de seguridad a fin de asegurar que se pueda obtener correctamente la información almacenada al momento de ser necesaria.

6.15.6. Los equipos de respaldo o contingencia deben contar con un programa de mantenimiento preventivo para asegurar su correcto funcionamiento cuando sea necesaria su utilización.

6.15.7. Las solicitudes de copia de respaldo de cuentas de correo electrónico de personal cesado u otros recursos de colaboración asignados, sólo podrán ser realizados por los jefes del área al que perteneció el colaborador. Es responsabilidad del jefe, el resguardo adecuado de la información una vez esta le haya sido entregada.

6.15.8. La Subgerencia de Operaciones de Tecnología es responsable de ejecutar, resguardar y controlar las copias de respaldo.

6.15.9. El propietario o dueño de la información es responsable de definir la criticidad de la información y el tiempo de retención de las copias de respaldo.

6.16. USO DE CONTROLES CRIPTOGRAFICOS

6.16.1. A todo sistema, aplicación e infraestructura que alberga información considerada como Confidencial se le deben aplicar técnicas de controles criptográficos como certificados SSL para la conexión, los mismos que contribuyen a preservar confidencialidad e integridad de la información consumida desde estaciones cliente.

6.16.2. Se utilizarán controles criptográficos para la protección de contraseñas de acceso a sistemas, datos críticos o servicios de red, así como en la transmisión o almacenamiento y resguardo de información de CIENTIFICA, de acuerdo con el nivel de clasificación de esta.

6.16.3. Los algoritmos de cifrado y longitud de clave que se utilizarán deben ser aquellos definidos y autorizados por el equipo de Seguridad de la Información asegurando que se manejen algoritmos considerados seguros por la industria.

6.16.4. Todas las claves deben ser protegidas contra alteración y en especial las claves secretas y privadas contra copia o divulgación no autorizada.

6.16.5. El uso de firma electrónica deberá aplicarse a documentos que requieran validez legal en procesos académicos o administrativos.

6.16.6. Sólo se deben usar certificados digitales emitidos por entidades certificadoras reconocidas y en el caso de firma electrónica aquellas que sean reconocidas por el gobierno peruano (RENIEC, INDECOPI, etc.).

6.17. SEGURIDAD FÍSICA

6.17.1. El personal de CIENTIFICA que atienda a personas externas a la organización (incluyendo suministradores) deberá asegurar que los datos quedan anotados en el registro de visitas.

- Se ha establecido una clasificación de las áreas para definir el nivel de seguridad de las mismas, las cuales se describen a continuación:

TIPO DE ÁREA	DESCRIPCIÓN
Restringida	Son zonas seguras donde la información que se genera, trata o almacena es crítica para la organización (Información clasificada como confidencial). Los accesos a estos despachos son controlados.
Común	Son zonas de uso común para personal de CIENTIFICA.
Pública	Son zonas que son de utilización pública y de recepción de personas externas a la organización.

6.17.2. Todas las visitas de personas externas a la institución deben ser consignadas en el registro de visitas.

6.17.3. Toda persona externa a CIENTIFICA podrá acceder a las áreas definidas como restringidas, siempre que cuente con la autorización respectiva y debe estar siempre acompañado por personal de la organización.

6.17.4. Los visitantes a las instalaciones deben portar su pase de visita.

6.17.5. Se debe contar con autorización para el retiro de equipos, de información o software de propiedad de CIENTIFICA.

6.17.6. Las medidas de protección contra amenazas externas y ambientales deben incluir:

- Controles de acceso y seguridad física
- Extintores
- Sistema de alimentación ininterrumpida (UPS)
- Sistema de puesta a tierra

6.17.7. Se deben proteger a los equipos de tecnología de la información críticos de fallas por falta de suministro de energía y otras anomalías eléctricas.

6.17.8. El cableado de la red de comunicaciones y suministro de energía debe protegerse para evitar intercepción o daño.

6.17.9. El cableado de suministro de energía eléctrica en las zonas de tratamiento de información debe contar con un sistema de pozo a tierra, el que debe ser revisado periódicamente para garantizar su adecuado funcionamiento.

6.17.10. Se debe considerar un programa de mantenimiento de los equipos de tecnología de información y de los sistemas de energía ininterrumpida (UPS), sistemas de detección y extinción de fuego según las especificaciones del fabricante.

6.17.11. Las áreas de carga y descarga deben definirse en la organización y señalarse como zona pública.

6.18. SEGURIDAD EN RELACIONES CON TERCEROS

6.18.1. Cuando exista necesidad de otorgar acceso a información o a los servicios de Tecnología de CIENTIFICA a terceros, el propietario de la información o gestor de la relación con el proveedor deberá diligenciar la firma obligatoria por parte del tercero del Acuerdo de Confidencialidad (NDA) de la institución, antes del inicio de la ejecución de las actividades del proveedor.

6.18.2. Cuando lo amerite, el gestor de la relación con el proveedor generará las solicitudes de acceso a través de la herramienta de gestión de servicios TI adjuntando el Acuerdo de Confidencialidad debidamente firmado, los motivos por el que se solicita el acceso, el tipo de acceso, el recurso al que se solicita brindar acceso y el tiempo de acceso requerido.

6.18.3. Toda solicitud de acceso de terceros será evaluada y aprobada por el Oficial de Seguridad de la Información, pudiendo rechazarse si se considera un riesgo a la seguridad de la información de CIENTIFICA.

6.18.4. En todos los contratos con terceros deberán adherirse los términos de seguridad de CIENTIFICA, aplicables según la naturaleza del servicio que provean.

6.18.5. La selección o adjudicación de proveedores que presten servicios tecnológicos o procesamiento de información para CIENTIFICA deberá tener aprobación expresa de la Gerencia de Tecnología y Servicios, el Oficial de Seguridad de la Información y quienes se designe para dicha tarea.

6.18.6. La Gerencia de Tecnología y Servicios deberá llevar a cabo las evaluaciones y validaciones debidas (due dilligence) de los terceros que se busque contratar para la prestación de servicios tecnológicos o procesamiento de información para CIENTIFICA, asegurando que el proveedor cumpla con los controles mínimos necesarios establecidos en esta política. Se debe evaluar los siguientes aspectos:

- Cumplimiento con estándares de Seguridad de la Información y Protección de Datos (ISO 27001, ISO 27002, ISO 27032, SOC Type II, PCI-DSS, GDPR, etc.)
- Infraestructura adecuada para la custodia de la información de CIENTIFICA.
- Acuerdo de Niveles de Servicio (SLA)
- Cumplimiento con los términos de la Política de Seguridad de CIENTIFICA.

6.18.7. Se deben establecer mecanismos de control con proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por ellos, cumplan con los lineamientos de acuerdo con la política de seguridad de la información. Asimismo,

cualquier cambio en los servicios que preste un proveedor debe ser comunicado, acordado y planificado antes de realizarse, siguiendo los lineamientos del punto 6.14 Gestión del Cambio, de la presente política.

6.19. GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

6.19.1. Todo el personal de CIENTIFICA debe reportar inmediatamente los eventos que atenten contra la seguridad de la información o cuando detecte o tome conocimiento de una debilidad de los controles de seguridad de la organización, por medio de los canales establecidos por la empresa para dicho fin: Canal de soporte "Te ayudamos" o al equipo de Seguridad de la Información al correo segurinfo@cientifica.edu.pe.

6.19.2. Se encuentra prohibido cualquier intento de escaneo, pruebas, explotación o demostración para detectar posibles debilidades o fallas de seguridad sin la autorización expresa de la Gerencia de Tecnología y Servicios y del Oficial de Seguridad de la Información. El incumplimiento de esta directiva facultará a CIENTIFICIA a aplicar las sanciones correspondientes incluyendo medidas legales en contra del infractor.

6.19.3. El Oficial de Seguridad de la Información y el subgerente de Operaciones de Tecnología establecerán un procedimiento de respuesta a eventos e incidentes, indicando la acción que debe tomarse ante la ocurrencia o materialización de un incidente o violación de los controles de seguridad establecidos en CIENTIFICA, para que se puedan destinar los recursos necesarios para la investigación y contención de estos.

6.19.4. Todos los eventos e incidentes de seguridad de la información deben ser registrados, evaluados y gestionados para minimizar su impacto y evitar su recurrencia.

6.19.5. Se deben establecer criterios para clasificar los eventos e incidentes de seguridad de la información, y gestionarlos según su prioridad.

6.19.6. La gestión de eventos e incidentes de seguridad de la información debe incluir la identificación, recolección y conservación de las evidencias necesarias para el análisis de la causa raíz.

6.19.7. Considerar la asignación de recursos especializados para la revisión de los eventos e incidentes de seguridad de la información, incluyendo la contratación de consultores y servicios externos cuando lo amerite.

6.19.8. El Oficial de Seguridad de la Información documentará y llevará registro de los eventos e incidentes revisados, las acciones tomadas, los impactos, las soluciones, las medidas de amonestación generadas y las lecciones aprendidas de cada caso, informando al Comité de Seguridad de la Información sobre los mismos.

6.19.9. Sin perjuicio del reporte al Comité de Seguridad de la Información y a las autoridades internas de la Universidad de los incidentes de seguridad detectados, el Oficial de Seguridad de la Información podrá comunicar los incidentes o violaciones de seguridad que afecten los datos personales de la comunidad CIENTIFICA, conforme a las disposiciones legales de la Ley N° 29733 – Ley de Protección de Datos Personales, su Reglamento y directivas asociadas.

6.20. CONTINUIDAD

6.20.1. La continuidad del negocio nos permite asegurar una respuesta efectiva durante una crisis o desastre que pueda afectar a la operación y disponibilidad de los servicios, por lo cual CIENTIFICA debe asegurar la existencia de recursos redundantes para el tratamiento de la información que satisfacen los requerimientos de disponibilidad. Así mismo se generará y actualizará el documento DRP (Disaster Recovery Plan) para poder garantizar el completo control del procedimiento de recuperación ante desastres y pérdida de información y servicios de TI.

6.21. PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

6.21.1. La Universidad CIENTIFICA y todo su personal, socios y proveedores se encuentran comprometidos con la protección de los datos personales en cumplimiento de la ley peruana N° 29733 – Ley de Protección de Datos Personales, su reglamento y directivas asociadas.

6.21.2. Todo personal de CIENTIFICA se encuentra obligado a proteger los datos personales y la información a la que acceda en cumplimiento del ejercicio de sus funciones, garantizando el cumplimiento de la cláusula de confidencialidad contractual y comprometiéndose a:

- Utilizar los datos personales, exclusivamente para el desarrollo de sus funciones y en línea con las instrucciones impartidas por la institución.
- Tratar, custodiar y proteger los datos personales a los que pudiese acceder como consecuencia del ejercicio de sus funciones, cumpliendo con las medidas de índole jurídica, técnica y organizativa establecidas por CIENTIFICA.
- Con relación a los datos personales que conozca en el ejercicio de sus funciones, deberá mantener el deber de secreto y confidencialidad de manera indefinida; es decir, durante la vigencia del presente contrato de trabajo, así como una vez concluida éste.
- El incumplimiento de las obligaciones en el tratamiento de datos personales por parte del personal de CIENTIFCA, y en concordancia a lo estipulado en el contrato de trabajo y a la normativa aplicable de la materia, pueden tener como consecuencia la imposición de sanciones disciplinarias.

6.21.3. CIENTIFICA desarrolla su política de privacidad en el tratamiento de datos personales en atención a los principios rectores establecidos en la Ley Nº 29733 - Ley de Protección de Datos Personales y por lo tanto se establece lo siguiente:

- Se rechaza la recopilación de los datos personales de nuestros usuarios por medios fraudulentos, desleales o ilícitos.
- Para el tratamiento de los datos personales de nuestros usuarios mediará su consentimiento, conforme a dicho principio.
- Los datos personales de nuestros usuarios se recopilarán para una finalidad determinada, explícita y lícita, y no se extenderá a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

- Todo tratamiento de datos personales será adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.
- Los datos personales que vayan a ser tratados serán veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Se conservarán de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.
- La Universidad Científica del Sur en su calidad de Titular de los Bancos de Datos Personales y, en caso, los Encargados de Tratamiento asociados, adoptan las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad y confidencialidad de los datos personales, estableciendo las medidas de seguridad apropiadas y acorde con el tratamiento que se vaya a efectuar y con la categoría de datos personales que se traten.
- Se garantiza el ejercicio de los derechos de los titulares de datos personales a solicitar el acceso, rectificación, cancelación y oposición recogidos en la Ley y su Reglamento, a través del correo electrónico soluciones@cientifica.edu.pe
- Para el flujo transfronterizo de datos personales, se debe asegurar el nivel adecuado de protección de los datos personales de los usuarios, como mínimo de protección equiparable a lo previsto por la Ley Nº 29733 o por los estándares internacionales de la materia.

6.21.4. CIENTIFICA se obliga a solicitar el consentimiento previo, expreso e informado de los titulares de los datos personales sobre los que se requiera realizar tratamiento.

6.21.5. Los datos personales facilitados se almacenarán en los bancos de datos que forman parte del registro de CIENTIFICA ante la Autoridad de Protección de Datos Personales y serán tratados para poder llevar a cabo las finalidades expuestas anteriormente.

6.21.6. CIENTIFICA se compromete a observar y cumplir el nivel de medidas de seguridad que correspondan a los datos tratados, tanto si están contenidos en Bancos de datos de la organización, asimismo a exigir el mismo nivel de cumplimiento a terceros que presten servicios a la institución y en tal sentido el personal debe:

- Evitar tratar Bancos con datos de carácter personal en los discos de los equipos personales, incluidos los portátiles salvo autorización expresa del responsable de seguridad o delegado del banco de datos.
- No acceder al sistema utilizando el identificador y la contraseña de otro usuario. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que hubiera sido asignado.
- Comunicar toda incidencia relativa a la seguridad siguiendo las instrucciones del procedimiento de gestión de incidentes.
- No sacar ningún soporte conteniendo datos personales fuera de los locales de la entidad sin la autorización de la persona responsable de la protección de datos personales de la empresa.

6.21.7. En caso CIENTIFICA realice transferencias internacionales de datos personales deberá asegurar que la entidad mantenga un nivel suficiente de protección para los datos personales

que se vayan a tratar o, por lo menos, equiparable a lo previsto por la Ley.

6.22. CUMPLIMIENTO

6.22.1. Todas las legislaciones, regulaciones y requerimientos contractuales deben cumplirse, ser identificadas y documentadas.

6.22.2. Toda información debe ser retenida conforme a los requisitos legales.

6.22.3. El personal de CIENTIFICA no debe destruir o eliminar registros o información importante, sin la aprobación respectiva de los propietarios de información.

6.22.4. Se deben de garantizar la protección y la privacidad de los datos conforme a la legislación aplicable.

6.22.5. Se deben establecer los términos, condiciones y finalidades para datos personales en cumplimiento con la Ley existente y su Reglamento.

6.22.6. Se debe asegurar que las políticas y procedimientos se cumplen. El incumplimiento de los lineamientos de esta política facultará a la institución a aplicar las medidas de sanción establecidas en el punto 6.2 Sanciones por Incumplimiento, de la presente política.

6.22.7. Se tiene como política el respeto a los derechos de propiedad intelectual, para lo cual todo el software que se utiliza en la organización debe contar con la respectiva licencia de uso.

6.22.8. Se debe considerar revisiones independientes de la seguridad de la información mediante auditorías para asegurar que se mantenga de forma eficaz, eficiente y efectiva.

7. Control de Cambios

Revisión	Descripción del cambio	Fecha
00 (Versión 1.0)	-	16.10.2018
01 (Versión 2.0)	Se incorporan lineamientos de seguridad adicionales, así como se actualizan los existentes en la versión 00. • 4. Información Complementaria (Actualizado) • 5. Lineamientos Generales (Actualizado) • 6.1 Responsabilidades (Actualizado) • 6.3 Clasificación de la Información (Actualizado) • 6.4 Control de Accesos (Actualizado) • 6.5 Políticas de Pantalla y Escritorio Limpio (Nuevo) • 6.6 Uso Aceptable de Activos (Nuevo) • 6.9 Protección contra el malware (Actualizado) • 6.10 Seguridad en el Desarrollo (Nuevo) • 6.11 Gestión de Vulnerabilidades (Nuevo) • 6.12 Seguridad de la red (Nuevo) • 6.13 Seguridad de los Servidores y Bases de Datos (Nuevo) • 6.14 Gestión del Cambio (Nuevo) • 6.15 Respaldo y Recuperación de la Información (Actualizado) • 6.16 Uso de Controles Criptográficos (Actualizado) • 6.18 Seguridad en Relaciones con Terceros (Actualizado) • 6.19 Gestión de Eventos e Incidentes de Seguridad de la Información (Actualizado) • 6.21 Privacidad y Protección de Datos Personales (Nuevo) • 6.22 Cumplimiento (Actualizado)	01.08.2025