

	Política de Seguridad de la Información	Código: CYS-TICS-PL-01 Fecha de liberación de la política: 29 de agosto 2025 Versión: 10
---	--	---

Objetivo: Definir los lineamientos de la gestión de la seguridad de la información proporcionando confidencialidad, integridad y accesibilidad para los activos de información, de los activos y servicios de Consultores y Soporte AMD.

Alcance: La Política de Seguridad de la información aplica a todo el Sistema de Gestión Integral de Consultores y Soporte AMD S.A. de C.V., a todos los colaboradores de Consultores y Soporte AMD S.A. de C.V. así como también a clientes, usuarios, proveedores internos y/o externos y otras partes interesadas.

Documentos de Referencia normativos

ISO/IEC 20000-1:2018,

8.7.3.1 Política de Seguridad de la información

8.7.3.2 Controles de Seguridad de la Información

8.7.3.3 Incidentes de Seguridad de la información

Nivel de Confidencialidad: De uso interno

Políticas de Consultores y Soporte AMD.

1. La política de seguridad de la información es una directriz que proporciona reglas sobre el uso y mal uso de la seguridad de la información de Consultores y Soporte AMD S.A. de C.V. definidas por el Comité de Seguridad.
2. Se establece que el Comité de Seguridad deberá estar conformado por los siguientes puestos:

Puestos
Director de Administración y Finanzas
Director de TIC's
Coordinadora del SGI

3. La Dirección de TIC's debe presentar el calendario de revisiones de seguridad de la información al comité de seguridad para su ejecución por lo menos 2 veces al año, y/o cada vez que se identifique un riesgo a la seguridad de la información.
4. La Dirección de TIC's asignará a un ingeniero de TI para realizar la revisión de seguridad de la información en los periodos descritos.
5. En caso de detectar alguna desviación, o vulnerabilidad se deberá realizar un registro de incidente de seguridad de la información en la mesa de ayuda.
6. Al final de cada mes de revisión se analizará el reporte de incidentes de seguridad de la información emitido por la mesa de ayuda, estos se atenderán a través del procedimiento Gestión de Riesgo, donde el comité de seguridad de la información se deberá evaluar y documentar los controles de seguridad que se deberán determinar e implementar
7. Es responsabilidad de todos los empleados de CYS AMD conocer y aplicar la presente política de seguridad, a efecto de garantizar la seguridad de la información y los sistemas informáticos de CYS AMD.
8. Es responsabilidad de todos los empleados de CYS AMD conocer y aplicar el reglamento interno de trabajo de CYS AMD.
9. Los trabajadores de CYS AMD se comprometen a:
 - No divulgar información confidencial de la organización a personas ajenas a la organización.

	Política de Seguridad de la Información	Código: CYS-TICS-PL-01 Fecha de liberación de la política: 29 de agosto 2025 Versión: 10
---	--	--

- Restringir el uso de los sistemas informáticos a personal ajeno a CYS AMD a menos que sea solicitado y autorizado mediante un ticket en el sistema de mesa de ayuda.
 - Sera responsabilidad única del director de TIC's autorizar dichas solicitudes.
 - Utilizar los sistemas informáticos dando prioridad a las actividades que estén directamente relacionadas con el trabajo en la organización.
 - Reportar cualquier falla en los sistemas informáticos inmediatamente través de la mesa de ayuda.
10. Será responsabilidad del usuario **generar un ticket en la mesa de ayuda reportando la pérdida o robo de cualquier componente de hardware y/o tarjeta de acceso a las instalaciones de CYSAMD**, adicionalmente; se deberá notificar a su jefe inmediato **y a la Coordinadora de Recursos Humanos**.
 11. Si el colaborador no cuenta con los recursos o medios para generar el ticket, deberá de solicitar a su jefe directo o a la coordinadora de Recursos Humanos, el apoyo para generar el incidente en la mesa de ayuda.
 12. Será responsabilidad de la Dirección de TIC's establecer las restricciones, para asegurar que los usuarios no utilicen la infraestructura tecnología para propósitos ajenos a la operación de CYS AMD (restricción de contenido de entretenimiento, políticas de AD).
 13. Toda persona ajena a CYSAMD deber de llenar un formulario de Registro en Formulario de la Página de CYSAMD, para poder acceder a las instalaciones de CYSAMD, reportar si se ingresa con equipo de cómputo y si se requiere conexión a Wi-Fi
 14. Cuando el personal de CYS AMD reciba a un invitado que requiera el servicio del Wi-Fi de invitados, deberá Registrarlo en el formulario de **Registro de la página de CYSAMD**
 15. **Sera responsabilidad del área de Recursos Humanos** solicitar altas, bajas o cambios de un colaborador por medio de un ticket registrado en la mesa de ayuda.
 16. El ingeniero responsable de **dar atención al** ticket registrado en la mesa de ayuda por Recursos Humanos para Altas, Bajas o Cambios se debe asegurarse de habilitar la opción en el sistema que solicite al usuario cambiar el Password en la primera sesión. (S.O y ofimática)
 17. El personal de CYSAMD cuenta con un usuario y contraseña para acceso a su equipo misma que no deberá de ser divulgada ni distribuida a ninguna persona ajena, ya que las claves son personales.
 18. La Dirección de TIC' **es la única que puede autorizar la instalación de software** nuevo en los equipos de cómputo de CYS AMD.
 19. En caso de que el personal de CYS AMD requiera instalar o modificar un software necesario para el desempeño de sus actividades, deberá registrar su solicitud en la herramienta de mesa de ayuda y dicha solicitud estará sujeta a evaluación y aprobación por el área de Tic's y su jefe inmediato.
 20. **Todos los colaboradores deberán asegurarse de bloquear su equipo al no estar en su lugar de trabajo dentro y fuera de las instalaciones.**
 21. **Todos los colaboradores deberán asegurarse de apagar su equipo al terminar su jornada laboral.**
 22. **Todos los colaboradores son responsables de aceptar y ejecutar las actualizaciones que el sistema le notifique (actualizaciones de antivirus y del sistema operativo).**
 23. **Los equipos de cómputo y/o celulares asignados a los colaboradores son propiedad de CYSAMD.**
 24. En los equipos de cómputo asignados a los colaboradores queda prohibido almacenar información ajena a su puesto de trabajo (Música, Imágenes y Videos).
 25. Todos los colaboradores que tengan acceso a información de clientes, proveedores y/o partes interesadas deberán utilizar SharePoint como único repositorio de almacenamiento de información.

	Política de Seguridad de la Información	Código: CYS-TICS-PL-01 Fecha de liberación de la política: 29 de agosto 2025 Versión: 10
---	--	---

26. Cada colaborador que genere una carpeta en SharePoint será responsable de mantener actualizados los miembros y gestionar los permisos de lectura y edición para evitar incidentes de seguridad en la información.
27. Si se detecta un incidente de Seguridad de la información SGI y los servicios, se deberá registrar en Mesa de Ayuda para poder clasificar, priorizar, escalar, solucionar y cerrar el incidente.
28. Cuando cualquier colaborador detecte una brecha en la seguridad de la información SGI, servicios y activos debe ser registrado en Mesa de Ayuda para poder clasificar, priorizar, escalar, solucionar y cerrar el incidente.
29. Al final de cada mes se analizará el reporte de incidentes de seguridad de la información emitido por la mesa de ayuda, estos se analizarán a través del procedimiento Gestión de Riesgo, donde se deberá evaluar y documentar los controles de seguridad que se deberán determinar e implementar
30. La organización debe comunicar a través de NDA's, contratos o comunicados, la importancia de cumplir con la Política de Seguridad de la Información aplicables a SGS y los servicios a clientes y proveedores, internos y externos.
31. Queda prohibido almacenar información propiedad de CYS AMD en dispositivos o repositorios que no sea SharePoint, almacenamiento oficial de la empresa.
32. El personal de CYS AMD deberá asegurarse de que los visitantes ingresen a las oficinas a través de la puerta ubicada en Francisco Pimentel #55, teniendo que realizar su registro en el portal de Registro de Visitas de CYSAMD
33. Toda persona que visite a CYS AMD, en caso de que porte laptop, iPad o Tablet, deberá registrarlo en la columna correspondiente en el Portal de Registro de Vistas, que será resguardado por CYSAMD.
34. Todos los registros de Portal de Registro de Visitas serán guardados en una Base de Datos dentro de una Maquina Virtual alojado en Data Center de CYSAMD
35. Todo el personal de CYS AMD estará obligado a cerrar su oficina cuando no se encuentre dentro de ella o sea el último en dejar su puesto de trabajo al finalizar el día laboral.
36. Queda estrictamente prohibido el acceso a la oficina de CYS AMD personal externo que visite por temas personales o ajenos a alguna relación comercial con CYS AMD.

Políticas para la Dirección de Administración y Finanzas

1. La Dirección de Administración y Finanzas debe asegurarse de que las partes interesadas conocen la política de seguridad de la información.
2. Los tipos de información confidencial y/o restringida que deberá resguardar la Dirección de Administración y Finanzas son:
 - Información de clientes,
 - Expedientes de personal,
 - Contratos de clientes,
 - Contratos con proveedores
 - Información financiera y contable.
 - Facturas de clientes
 - Facturas proveedores,
 - Carta de entrega de equipo de clientes
 - Acuse de recibos de nómina,
 - Constancias de capacitación,
 - Evaluaciones del desempeño del personal.
 - Información de clientes prospectos,
 - Convenios de confidencialidad de clientes

	Política de Seguridad de la Información	Código: CYS-TICS-PL-01 Fecha de liberación de la política: 29 de agosto 2025 Versión: 10
---	--	--

- Base de datos de CRM.
- Cartera de clientes activos y prospectos.
- Documentación generada como evidencia del cumplimiento de los procedimientos.
- Lista de precios de mayoristas para CYSAMD
- Documentación generada como evidencia del cumplimiento de los procedimientos.
- 3. La Coordinadora de Recursos Humanos con apoyo de los diferentes directores se asegura de conocer y dar a conocer la política de seguridad de la información y la importancia del cumplimiento de esta a todos los colaboradores de CYS AMD, a través de una campaña de concientización.
- 4. Es responsabilidad de la Coordinadora de Recursos Humanos incluir en el programa anual de capacitación y en el plan de comunicación una campaña de concientización de **Seguridad de la Información**.
- 5. La Coordinadora de Recursos humanos al realizar un cambio, baja o reasignación de activos tecnológicos deberá notificar a la Dirección de Tic's y Servicios.
- 6. La Coordinadora de Recursos Humanos al recoger un activo tecnológico deberá registrar un ticket en la herramienta de mesa de ayuda, solicitando el respaldo de la información, **Formateo simple** y firmar acuse de recibido en la responsiva de activos, deslindando al usuario.
- 7. La Coordinadora de Recursos Humanos deberá asegurarse de contar con la firma de todos los colaboradores en el Convenio de Confidencialidad, Aviso de Privacidad y Política de CCTV.

Políticas para la Dirección Tics y servicios

1. El área de TIC's será la responsable de gestionar la configuración de los equipos de cómputo de CYS AMD aplicando las políticas de seguridad establecidas en Active Directory y conforme a la matriz de asignación de software.
2. La Dirección de TIC's será el responsable de gestionar que se mantenga la política de gestión como fondo de pantalla de los equipos de cómputo de todos los colaboradores.
3. Es responsabilidad del director de TIC's y Servicios que exista acuerdo de confidencialidad (NDA) con proveedores de servicios.
4. El área de TIC's es responsable de gestionar autorización y ejecutar el acceso a la red, Creación y administración de cuentas de correo electrónico, creación y administración de usuarios en el Directorio Activo, Control de acceso a los sistemas informáticos de CYSAMD.
5. Es responsabilidad del área de TIC's TI crear y administrar una conexión Wi-Fi exclusiva para invitados.
6. La contraseña de la conexión Wi-Fi invitados deberá ser cambiada de manera mensual (**primer día hábil de cada mes**).
7. CYS AMD declara SharePoint como repositorio institucional único de toda información digital.
8. La información que resguarda la Dirección de Tics y servicios:
 - Información de clientes.
 - Licenciamientos de software de CYSAMD y/o clientes,
 - Información contenida en los equipos administrador y/o propiedad de CYS AMD.
 - Base de datos de herramienta de mesa de ayuda.
 - Documentación generada como evidencia del cumplimiento de los procedimientos.
9. Los servidores físicos y virtuales gestionados por CYSAMD se encontrarán protegidos por contraseña, misma que será resguarda por el Coordinador de Servicios Data Center.
10. Será responsabilidad del área de TIC's realizar los respaldos apegado al procedimiento Programa de Backup y restauración de la información.

	Política de Seguridad de la Información	Código: CYS-TICS-PL-01 Fecha de liberación de la política: 29 de agosto 2025 Versión: 10
---	--	---

11. La Dirección de TIC's deberá gestionar con el área de TIC's un monitoreo semestral al software instalado en todos los equipos de CYS AMD y entregar el reporte en la junta de Seguridad de la Información (**calendario de revisiones de seguridad de la información y matriz de SW**).
12. La Dirección de Tics deberá establecer los protocolos de seguridad necesarios para garantizar el correcto funcionamiento de la infraestructura TI.
13. Todos los equipos de cómputo asignados al personal de CYS AMD deberán de tener activo Windows Defender o contar con cualquier otro antivirus autorizado por CYSAMD. A excepción que por la naturaleza de las aplicaciones instaladas dentro del equipo entren en conflicto
14. Todos los servidores gestionados por CYS AMD deberán contar con un antivirus o tener activo Windows Defender, a excepción que por la naturaleza de las aplicaciones instaladas dentro del servidor entren en conflicto.
15. Sera responsabilidad del área de TIC's asegurarse que el antivirus o Windows Defender, este instalado y activado en los equipos de cómputo y servidores de CYS AMD este actualizado con la versión más reciente.
16. EL personal de CYSAMD tiene prohibido instalar cualquier tipo software no autorizado por la Dirección de TIC's y Servicios en los equipos de cómputo.
17. Los colaboradores deberán notificar al área de TICS y servicios sobre cualquier comportamiento anómalo en su equipo de cómputo o cualquier aplicativo instalado que no sea reconocido y/o reportándolo a la mesa de ayuda.
18. Todo dispositivo propiedad de CYS AMD que se determine como infectado y/o con comportamiento sospechoso deberá ser aislado de manera inmediata hasta garantizar que se encuentre libre de cualquier virus.
19. Coordinador y Administrador de Data Center cuenta con acceso inmediato al Data Center de CYS AMD.
20. El director de Administración y Finanzas cuenta con una llave de respaldo para el acceso al Data Center de CYS AMD.
21. Se deberá contar con un formulario de registros actualizada donde se registren los accesos al Data Center de CYS AMD.

Políticas de Directorio Activo:

1. El equipo de cómputo solicitará cambio de contraseña al hacer login por primera vez.
2. Todas las contraseñas tienen una longitud de al menos 8 caracteres, una letra mayúscula y minúscula, un número y un carácter especial
3. El ID utilizado para acceder al dominio se bloquea después de 3 intentos fallidos de autenticación.
4. La contraseña no será visible al ingresarla.

Medición de la eficacia de las Políticas de Seguridad de la Información.

Descripción	Métricas e Indicadores
1. Actualizaciones de seguridad de S.O. 2. Diagnostico mensual de los activos de clientes internos y externos 3. Realización de respaldos de los equipos de cómputo al menos 1 mensual. 4. Control de accesos (permisos, usuarios, contraseñas).	$\% \text{ Efectividad Contra Ataques} = \left(\frac{\text{Cantidad de equipos infectados o atacados}}{\text{Cantidad total de equipos en CYS AMD}} \right) \times 100$ % de Efectividad $\geq 92\%$

	Política de Seguridad de la Información	Código: CYS-TICS-PL-01 Fecha de liberación de la política: 29 de agosto 2025 Versión: 10
---	--	---

Control de cambios

Fecha	Versión	Descripción del Cambio
15-diciembre-2016	0	Documento Nuevo
24-abril-2017	1	Revisión con los responsables
13-junio-2017	2	Modificación de Políticas
21-agosto-2018	3	Modificación de Políticas
04-julio-2019	4	Modificación de Políticas
9-octubre-2020	5	Modificación de Políticas
03-noviembre-2021	6	Modificación de Políticas
05-noviembre-2021	7	Modificación de Políticas
18-julio-2022	8	Modificación de Políticas
02-septiembre-2024	9	Modificación de Políticas
29 – agosto - 2025	10	Modificación de Políticas Actualización de logo Liberación de la Política de Seguridad de la Información

Esta información es de uso interno y para uso de Consultores y Soporte AMD, S.A. de C.V.

Aprobaciones

Elaboró: <i>Hermenegildo Martínez Peña</i> Ingeniero de implementación
Nombre y firma

Revisó: <i>Enrique Rodríguez Aquiles</i> Director de TIC's
Nombre y firma

Aprobó: <i>Esteban Sánchez Guzmán</i> Director de Administración y Finanzas
Nombre y firma