



Especialista de Redes y Comunicaciones

Firmado digitalmente por:
ERIK ALONSO PRADO VIERA
DNI:48786148 RUC:20103030791
Motivo: Soy el autor del
documento
Fecha: 07/10/2026 09:31:35-0500



Jefe de la Oficina de
Planeamiento y Mejora Continua

Firmado digitalmente por:
MIGUEL ARMANDO TITO ASCUE
DNI:42253883 RUC:20103030791
Motivo: Doy V° B°
Fecha: 09/10/2026 11:56:18-0500



Gerente de Administración
y Finanzas

Firmado digitalmente por:
JULIO CESAR TEMPLE
AGUILAR DNI:42302432
RUC:20103030791
Motivo: Doy V° B°
Fecha: 09/10/2026 11:35:46-0500



Devolvemos vida al planeta

Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones

Directiva

Código: S3.1.DR1
Versión: 05
Fecha: 06/10/2026

Directiva para el Uso de Servicios y Recursos de Tecnología de la Información y Comunicaciones

Versión	Fecha	Control de Cambios
05	06/10/2026	- Numeral 2.3.2. Se añadieron disposiciones específicas sobre cuentas de usuario. - Numeral 2.4.30. Se añadieron disposiciones sobre programas de utilidad privilegiados. - Numeral 2.4.17. Se incorporaron disposiciones para la evaluación periódica de riesgos físicos asociados a la ubicación de equipos críticos de TIC, con una frecuencia mínima anual.

Áreas Responsables	Nombres y Cargos
Elaborado: Departamento de Tecnologías de la Información y Comunicaciones	Erik Prado Especialista en Redes y Comunicaciones
Revisado: Departamento de Tecnologías de la Información y Comunicaciones	Moisés Palomino Jefe de Departamento de Tecnologías de la Información y Comunicaciones
Homologado: Oficina de Planeamiento y Mejora Continua	Deymer Barturén Especialista en Calidad y Mejora de Procesos Miguel Tito Jefe de la Oficina de Planeamiento y Mejora Continua
Revisado y Aprobado: Gerencia de Administración y Finanzas	Julio Temple Gerente de Administración y Finanzas

Este documento es propiedad de Activos Mineros S.A.C. Queda prohibida su reproducción sin su autorización escrita. Es una copia auténtica imprimible de un documento electrónico emitido por Activos Mineros S.A.C. Es responsabilidad del usuario asegurarse que corresponde a la versión vigente publicada en la red interna y/o página web institucional.



Jefe del departamento de Tecnologías de la Información y Comunicaciones

Firmado digitalmente por:
PALOMINO SUAREZ Moises
Reynaldo FAU 20103030791 hard
Motivo: Doy V° B°
Fecha: 07/10/2026 10:57:36-0500



Especialista en Calidad y Mejora de Procesos

Firmado digitalmente por:
DEYMER FRANK BARTUREN
HUAMAN DNI:40658548
RUC:20103030791
Motivo: Doy V° B°
Fecha: 08/10/2026 15:38:33-0500

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	---	---

INDICE

I.	OBJETIVO.....	3
II.	ALCANCE	3
III.	DOCUMENTOS DE REFERENCIA	3
IV.	VIGENCIA	3
V.	CONTENIDO	3
1.	DEFINICIONES / CONSIDERACIONES	3
2.	DESCRIPCIÓN	4
3.	ALCANCES FUNCIONALES	32
4.	REGISTROS / ANEXOS.....	32

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

I. OBJETIVO

Establecer las normas para el uso de los servicios y recursos de las Tecnologías de la Información y Comunicaciones (TIC), puestos a disposición de los usuarios de Activos Mineros S.A.C. (en adelante AMSAC), con el fin de regular su utilización.

II. ALCANCE

El presente documento se aplica a todos los funcionarios y trabajadores de AMSAC. Asimismo, se hace extensivo su cumplimiento a las personas a las que excepcionalmente se les proporcione equipo tecnológico (computadoras, accesorios de cómputo, accesorios de comunicaciones u otros), o se les asigne servicios TIC (internet, correo electrónico, impresora, sistemas de información u otros).

III. DOCUMENTOS DE REFERENCIA

- Directiva Corporativa de Gestión Empresarial de FONAFE.
- Ley N° 29733 Ley de Protección de Datos Personales N° 29733 y su Reglamento aprobado mediante Decreto Supremo N° 016-2024-JUS.
- Resolución Jefatural N° 088-2003-INEI, que aprueba Directiva sobre “Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública”.
- Resolución Directoral N° 022-2022-INACAL/DN, que aprueban Normas Técnicas Peruanas:
 - NTP ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información – Requisitos.
 - NTP ISO/IEC 27002 Controles de Seguridad de la Información.
- Norma ISO 9001 Sistema de Gestión de la Calidad – Requisitos.
- Norma ISO 14001 Sistema de Gestión Ambiental – Requisitos.
- Norma ISO 45001 Sistema de Gestión de Seguridad y Salud en el Trabajo – Requisitos.
- Norma ISO 37001 Sistema de Gestión Antisoborno – Requisitos.
- Norma ISO 27001 Sistema de Gestión de Seguridad de la Información – Requisitos
- Norma ISO 27002 Controles de Seguridad de la Información
- Norma ISO 27005 Guías para la Gestión de Riesgos de Seguridad de la Información.
- Norma ISO 27035 Gestión de Incidentes de Seguridad de la información.
- Código de Ética y Conducta de AMSAC.
- Política de Seguridad, Salud en el Trabajo, Medio Ambiente, Calidad, Integridad, Anticorrupción y Seguridad de la Información de AMSAC.

IV. VIGENCIA

Este documento entrará en vigencia a partir del primer día hábil después de la fecha de aprobación, derogándose su precedente Versión 04 de fecha 17.nov.2025.

V. CONTENIDO

1. DEFINICIONES / CONSIDERACIONES

- **Activo:** Cualquier cosa que tenga valor para la organización.
- **Activo de información:** Activo que es o que contiene información que tiene valor para la organización. También conocido como conocimiento o dato.
- **Amenaza:** Potencial causa de un incidente no deseado que puede resultar en daños a un sistema o a la organización.
- **Acceso privilegiado:** Derecho, permiso, rol, perfil o nivel de acceso superior al asignado a un usuario estándar, que permite administrar, configurar, modificar, supervisar o controlar infraestructura tecnológica, sistemas de información, servicios en nube, aplicaciones, bases de datos, dispositivos de comunicaciones, plataformas de seguridad u otros recursos TIC de AMSAC.
- **Confidencialidad:** Propiedad de la información de no estar disponible o sea divulgada a quienes no poseen autorización.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- **Control:** Medida que mantiene o modifica un riesgo.
- **Control de seguridad de la información:** Medida que mantiene o modifica un riesgo de seguridad de la información.
- **Correo electrónico** (o e-mail): Medio por el cual se pueden intercambiar mensajes a través de la red empresarial utilizando un dispositivo electrónico.
- **Computador personal:** Equipo de cómputo asignado a los usuarios para el desarrollo exclusivo de las tareas encomendadas.
- **Disponibilidad:** Propiedad de la información ser accesible y utilizable cuando se requiera por quien tiene autorización.
- **ERC:** Sigla de Especialista de Redes y Comunicaciones, perteneciente al Departamento de TIC.
- **ESI:** Sigla de Especialista en Sistemas de Información, perteneciente al Departamento de TIC.
- **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias.
- **Evento de seguridad de la información:** Ocurrencia identificada de un estado del sistema, servicio o red que indica una posible violación de la seguridad de la información o un fallo de controles o una situación previamente desconocida que puede ser relevante para la seguridad de la información.
- **Incidente de seguridad de la información:** Evento aislado o conjunto de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** propiedad de precisión y completitud de la información.
- **Internet:** Gran comunidad de computadoras conectadas entre sí por medio de líneas de comunicaciones especiales.
- **Intranet:** Red privada que utiliza tecnología de Internet pero cuyo contenido sólo está disponible al interior de una entidad.
- **Hardware o equipo informático:** Equipos, dispositivos y accesorios físicos utilizados para el procesamiento de la información.
- **Parte interesada:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.
- **Riesgo de seguridad de la información:** Puede ser expresado como el efecto de la incertidumbre en los objetivos de seguridad de la información. También está asociado con el potencial que tienen las amenazas para explotar vulnerabilidades de un activo de información o grupo de activos de información y así causar daño a la organización.
- **Seguridad de la información:** Preservación de confidencialidad, integridad y disponibilidad de la información.
- **Servidor:** Computadora de gran potencia que se encuentra a disposición y compartida por múltiples usuarios, para la provisión de servicios informáticos.
- **Software:** Conjunto de programas, documentos, procesamientos y rutinas asociados con la operación de un sistema de computadoras.
- **SPAM:** Correo no deseado.
- **TIC:** Sigla de Tecnologías de la Información y Comunicaciones.
- **UPS:** Uninterruptible Power Supply, traducido al Castellano como Sistema de alimentación ininterrumpida (SAI).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada para que un evento con una consecuencia negativa ocurra.

2. DESCRIPCIÓN

2.1 DISPOSICIONES GENERALES

- 2.1.1. El Jefe del Departamento de Tecnología de la Información y Comunicaciones, como dueño del proceso, es responsable que el uso de servicios y recursos de TIC se efectúe

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

cumpliendo los plazos y las disposiciones previstas en la normativa legal y el presente procedimiento.

- 2.1.2. El Departamento de TIC garantiza y asegura el soporte tecnológico de los procesos de la empresa, implementando soluciones ante contingencias acordes con los avances y especialización en el campo de la seguridad de la información.
- 2.1.3. El Departamento de TIC monitorea de forma constante la infraestructura y servicios de red que presta, implementando las herramientas que le permitan detectar, prevenir y recuperarse del ataque y vulnerabilidades que puedan encontrarse en la plataforma tecnológica.
- 2.1.4. El Departamento de TIC implementa mecanismos de disponibilidad y respaldo ante eventuales contingencias con la infraestructura de operaciones de cómputo y comunicaciones, garantizando la restauración del servicio informático en el más corto plazo posible.
- 2.1.5. El Departamento de TIC gestiona una constante capacitación y soporte que requiera el personal encargado de la implementación y sostenimiento de la seguridad de la información.
- 2.1.6. El Departamento de TIC implementa, difunde y supervisa el cumplimiento de las disposiciones para el uso de servicios y recursos de TIC, establecidas en la presente directiva, así como brinda capacitación y soporte que requieran los usuarios de AMSAC en esta materia.
- 2.1.7. Las áreas usuarias de AMSAC deben cumplir las disposiciones para el uso de servicios y recursos de TIC, establecidas en la presente directiva.

2.2 INFRAESTRUCTURA TIC

2.2.1 Equipos de cómputo y accesorios

1. La adquisición o arrendamiento de equipos y/o accesorios se realizan en el marco de la Directiva Corporativa de Gestión Empresarial de FONAFE y la normativa que resulte aplicable.
2. Los equipos de cómputo y accesorios tecnológicos asignados por AMSAC deberán utilizarse exclusivamente para fines institucionales y para el cumplimiento de las funciones laborales autorizadas. Los usuarios son responsables de su adecuado uso, conservación y custodia.
3. Solo el personal del Departamento de TIC o de empresas terceras debidamente autorizadas por el Departamento de TIC puede instalar, desconectar, trasladar, intervenir o abrir el equipo y sus componentes. La entrega, traslado, préstamo o devolución de los bienes se realizará en coordinación con el área de Patrimonio del Departamento de Administración y Logística (DAL).
4. Los daños ocasionados por: uso inadecuado, golpes o caídas, intervención sin autorización, derrame de líquidos o alimentos, negligencia o accidentes no se consideran como fallas propias del equipo sino provocadas, las mismas que serán determinadas técnicamente por el Departamento de TIC. El costo de los daños por reparación o sustitución serán asumidos por el usuario responsable previa conformidad del Departamento de TIC.
5. El usuario deberá comunicar de manera inmediata al Departamento de TIC cualquier incidente que pueda afectar la disponibilidad, integridad o seguridad del equipo asignado, incluyendo fallas de funcionamiento, pérdida, robo, extravío, daño físico,

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

acceso no autorizado o cualquier situación que comprometa la información institucional.

6. En caso de pérdida, deterioro o robo de los equipos o accesorios tecnológicos asignados, se aplicará lo dispuesto en la Directiva de "Normas para la Administración, Uso, Control, Cuidado y Custodia de los Bienes de Activos Mineros".
7. El usuario debe tomar las medidas necesarias para resguardar el equipo y accesorios a su cargo. El Departamento de TIC no cuenta con accesorios en stock, por lo que en caso sea necesario, se requerirá un plazo para su reposición.
 - El usuario debe asegurarse que se mantenga la limpieza general de los equipos de cómputo y comunicaciones (parte externa) a su cargo; en caso sea necesario, debe requerir el soporte del Departamento de TIC.
 - No deben conectarse artefactos de alto consumo de energía en la misma línea de alimentación en la que se encuentra el equipo.
 - En las ubicaciones que se requiera, se deben utilizar estabilizadores de voltaje adecuados para evitar que las computadoras sufran desperfectos, debido a las interrupciones o alteraciones en el fluido eléctrico.
 - Se debe evitar que la disposición de cables cruce por lugares en que transita el personal.
8. La información de trabajo debe ser almacenada en las carpetas en la nube asignadas al usuario, así como en carpetas compartidas debidamente organizadas y fácilmente identificables. Los nombres de las carpetas y archivos deben ser breves y claros, a fin de facilitar la generación y gestión de copias de respaldo.
9. El Departamento de TIC es responsable de gestionar el acceso a los puertos USB en los equipos de cómputo, el cual estará habilitado únicamente para usuarios que cuenten con la debida autorización.
10. **Está prohibido:**
 - Almacenar información institucional en dispositivos externos sin cumplir las disposiciones de seguridad y respaldo establecidas por AMSAC, sin dejar copia idéntica en la nube o carpeta en red asignada al usuario.
 - Copiar o transferir información institucional de otras computadoras, sin la debida autorización.
 - Extraer información en dispositivos de almacenamiento externo o a través de servicios TIC (correo electrónico, internet) sin la debida autorización y para fines no autorizados.
 - Eliminar la información histórica del equipo de cómputo, de las carpetas en la nube asignadas o de cualquier repositorio utilizado en el marco del trabajo.
 - Guardar información ajena a los fines laborales como: programas, videos, música, presentaciones personales u otros, que afecte los recursos institucionales.
 - Instalar software, aplicaciones, extensiones o herramientas no autorizadas por el Departamento de TIC.
 - Deshabilitar, alterar o interferir con los mecanismos de seguridad implementados por AMSAC, tales como antivirus, cifrado, herramientas de monitoreo, control de dispositivos o actualizaciones de seguridad.
 - Utilizar cuentas de terceros o permitir que otros usuarios utilicen la cuenta asignada para acceder a equipos o recursos tecnológicos institucionales.
 - Manipular, retirar o modificar componentes de hardware, periféricos o accesorios tecnológicos sin autorización del Departamento de TIC.
11. Después de concluidas las labores diarias, los usuarios deben cerrar sus sesiones de trabajo y apagar sus equipos. Cuando los usuarios no estén utilizando sus equipos, deben bloquear o cerrar sesión de trabajo.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

12. La información generada en sus estaciones de trabajo es de propiedad de AMSAC, por lo cual éste se reserva el derecho de titularidad.
13. El Departamento de Administración y Logística es responsable de implementar y gestionar la energía estabilizada en las sedes y bases operativas de AMSAC, incluyendo la adquisición de sistemas UPS y demás componentes necesarios (pozos a tierra, tableros eléctricos, etc.), con el objetivo asegurar la disponibilidad y continuidad operativa de los equipos de cómputo ante posibles restricciones en el suministro eléctrico. Para ello, contará con el soporte técnico del Departamento de TIC en la definición de las especificaciones técnicas de los equipos asociados cuando corresponda.

2.2.2 Almacenamiento en la nube y respaldo de información

- Cada usuario dispone de un espacio en la nube institucional asignado por AMSAC para el almacenamiento de información relacionada exclusivamente con sus funciones laborales o contractuales. Es responsabilidad del usuario mantener su espacio de almacenamiento depurado y organizado, conforme a los principios de buen uso de los recursos institucionales.
- El almacenamiento de datos o información en la nube es exclusivo para fines laborales, por lo que no se deben almacenar programas, videos, música, archivos personales u otros.
- El Departamento de TIC programará un método establecido de respaldo según el Procedimiento S3.2.P1 Gestión de respaldo y recuperación. Las copias de respaldo serán imperativas en los casos siguientes:
 - Cambio de equipo (computador).
 - Falla severa del hardware o software del computador.
 - Cese laboral del trabajador o finalización del servicio de locación de servicios de proveedores.
- El Departamento de TIC no realiza respaldo de la información almacenada localmente en los equipos de los usuarios, salvo en los casos previstos en el procedimiento mencionado. Cada usuario es responsable de respaldar oportunamente su información en los repositorios institucionales autorizados.
- La información almacenada en las carpetas en la nube y en las copias de respaldo generadas es de propiedad de AMSAC, por lo cual esta se reserva el derecho de titularidad. No obstante, se resalta que cualquier transferencia de información por parte del personal debe contar con la debida autorización, conforme a lo establecido en la Ley de Protección de Datos Personales.
- Cada gerencia y cada departamento, oficina o área dispondrá de un espacio propio en el almacenamiento en la nube Departamental / Gerencial para el almacenamiento interno de documentos generados por su propia área (ver Figura 1). Este espacio está destinado a la gestión operativa, la recopilación de información de proveedores, la elaboración de informes periódicos y demás actividades internas.
- La Intranet será utilizada exclusivamente para la publicación y acceso a los documentos que hayan sido previamente revisados, validados y/o aprobados por los gerentes, jefes y/o supervisores de área correspondientes.
- El nivel de almacenamiento empresarial provee plantillas, directrices y políticas que las gerencias y departamentos adaptan y utilizan en sus espacios.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

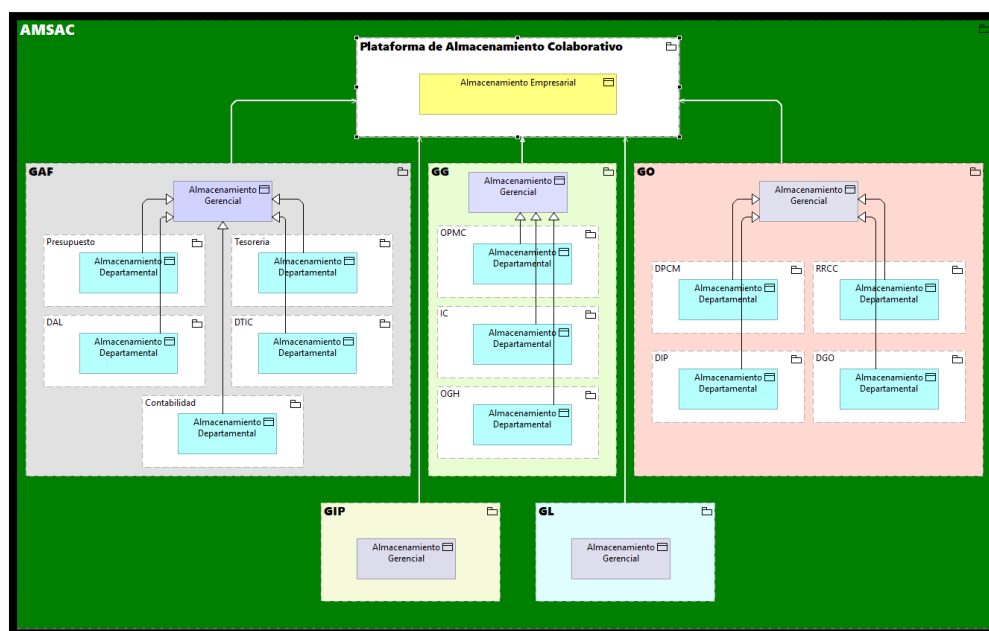


Figura 1: Arquitectura de Almacenamiento Colaborativo de AMSAC

2.2.3 Dispositivos de almacenamiento externo (USB)

- Está prohibido que los usuarios utilicen dispositivos de almacenamiento externo como medio principal para realizar sus labores de trabajo. Estos dispositivos deben ser empleados únicamente como medios de tránsito, asegurando que la información permanezca almacenada en los repositorios oficiales de AMSAC. No se permitirá su uso sin la solicitud del jefe directo o de la gerencia correspondiente, la cual deberá gestionarse mediante el formato S3.2.P2.F3 “Exoneración de restricción de TIC”, con la debida autorización conforme al procedimiento S3.2.P2 “Procedimiento de Gestión de Accesos”.
-
- El uso de dispositivos de almacenamiento externo deberá ser solicitado al Departamento de TIC mediante el formato S3.2.P2.F3 “Exoneración de restricción de TIC”, con la debida autorización conforme al procedimiento S3.2.P2 “Procedimiento de Gestión de Accesos”. La solicitud será evaluada por el Oficial de Seguridad y Confianza Digital y, de ser aprobada, contará con la firma del Jefe del Departamento de TIC.
- El Departamento de TIC no gestiona los dispositivos de almacenamiento externo de los usuarios. Cada usuario es responsable por la información que almacena en los USB y por cualquier daño en el equipo asignado y/o a la red de AMSAC producto de la utilización de estos dispositivos.
- El uso de dispositivos de almacenamiento externo que pudiera autorizarse será exclusivamente para fines laborales, en el marco de las funciones asignadas al usuario y conforme a las políticas y directivas de seguridad de la información de AMSAC. Este acceso podrá ser objeto de monitoreo y auditoría posteriores. El uso indebido o no autorizado de estos dispositivos podrá conllevar la revocación del permiso otorgado, así como la aplicación de las medidas disciplinarias que correspondan.

2.3 SERVICIOS TIC

2.3.1 Condiciones Generales para el Uso de Equipos y Recursos TIC

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

2.3.1.1 Asignación de Equipos de Cómputo:

- **Responsabilidad del Usuario:** Al recibir un equipo de cómputo (PC, laptop, tablet, etc.), el usuario es responsable de su cuidado y uso adecuado. Se debe firmar un acta de entrega que detalle el equipo asignado y las condiciones de uso.
- **Configuración Inicial:** El Departamento de TIC se encargará de configurar los equipos con el software necesario para las funciones laborales, incluyendo el sistema operativo, aplicaciones corporativas y herramientas de seguridad.
- **Accesorios:** Los accesorios como teclados, ratones, monitores y otros deben ser utilizados exclusivamente para actividades relacionadas con el trabajo y deben mantenerse en buen estado.

2.3.1.2 Conexión a la Red Corporativa:

- **Acceso a la Red:** Los usuarios deben conectarse a la red corporativa de AMSAC únicamente a través de los dispositivos autorizados. El acceso remoto debe realizarse a través de una VPN segura.
- **Red de Invitados:** Los usuarios deben evitar el uso de la red de invitados para acceder a recursos corporativos, salvo en casos excepcionales autorizados por el Departamento de TIC.
- **Restricciones de Red:** Está prohibido instalar software de terceros que no haya sido aprobado por el Departamento de TIC o conectar dispositivos no autorizados (como dispositivos USB personales) sin el debido proceso de aprobación.
- **Autenticación:** El acceso a nuestra suite de productividad en la nube requerirá autenticación multifactor (MFA) para garantizar la seguridad de la información.
- **Cifrado:** Todos los datos almacenados en el almacenamiento en la nube están cifrados tanto en tránsito como en reposo, siguiendo las mejores prácticas de seguridad.

2.3.1.3 Almacenamiento y Gestión de la Información:

- **Unidades de Almacenamiento Virtuales:** El almacenamiento en la nube serán configurados por el Departamento de TIC como unidades de red virtuales o carpetas accesibles desde los dispositivos corporativos. Los usuarios podrán acceder a estas carpetas como lo hacen con cualquier unidad de red tradicional.
- **Acceso a Almacenamiento en la nube:** Cada usuario tendrá una carpeta personal en la nube, accesible a través de su perfil de usuario. Esta carpeta debe ser utilizada para el almacenamiento de documentos de trabajo individuales. Además, las áreas y proyectos específicos tendrán asignadas bibliotecas de documentos en la nube. Los usuarios accederán a estas bibliotecas según los permisos establecidos por el Departamento de TIC.
- **Sincronización y Acceso Remoto:** Los archivos locales del computador asignado están sincronizados con la nube, lo que permite el acceso desde cualquier dispositivo autorizado. Los usuarios deben asegurarse de que los documentos importantes están sincronizados correctamente para evitar pérdidas de datos.
- **Gestión de Espacio:** Los usuarios deben gestionar de manera eficiente el espacio asignado en el almacenamiento en la nube.
- **Nombres de Archivos y Carpetas:** Los nombres de archivos y carpetas deben ser claros y descriptivos para facilitar la identificación y recuperación de información.
- **Copia de Seguridad:** El Departamento de TIC realizará copias de seguridad automáticas de los datos almacenados en la red. Los usuarios deben asegurarse de que sus archivos estén actualizados y almacenados correctamente.
- **Backup Automático:** La suite de productividad cuentan con mecanismos de respaldo automático en la nube, gestionados por los proveedores de servicios. Sin embargo, los usuarios deben asegurarse de que la sincronización de archivos está activada para garantizar que todos los documentos estén respaldados.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- **Recuperación de Archivos:** En caso de pérdida accidental de archivos, los usuarios pueden recuperar documentos desde la Papelera de Reciclaje del almacenamiento en la nube dentro de un período de tiempo definido por las políticas de AMSAC.

2.3.1.4 Uso de Software:

- **Instalación de Software:** Todo software adicional que el usuario requiera debe ser solicitado al Departamento de TIC mediante el procedimiento establecido. Está prohibido instalar software por cuenta propia.
- **Actualización de Software:** El Departamento de TIC gestionará las actualizaciones de software para garantizar la seguridad y el rendimiento. Los usuarios deben reiniciar sus equipos cuando se les solicite para aplicar las actualizaciones.
- **Licencias de Software:** Solo se debe utilizar software con licencia aprobada por la empresa. El uso de software pirata o sin licencia está estrictamente prohibido.
- **Monitoreo de Uso de Software:** Con el objetivo de garantizar el uso adecuado y eficiente de las licencias de software adquiridas para labores administrativas y especializadas, el Departamento de TIC implementará mecanismos automáticos de monitoreo y alertamiento para detectar la instalación, ejecución o uso de programas de utilidad privilegiados, herramientas administrativas, software de acceso remoto, aplicaciones de escaneo, explotación o diagnóstico que no hayan sido previamente autorizadas por AMSAC. Toda alerta generada deberá ser evaluada y gestionada conforme al Procedimiento de Gestión de Incidentes de Seguridad de la Información. Estos mecanismos se llevarán a cabo de manera periódica e inopinada, con el fin de asegurar el uso eficiente de los activos informáticos de AMSAC.

2.3.1.5 Publicación de Tableros de Inteligencia de Negocio

- Las áreas de la empresa pueden generar y publicar tableros de inteligencia de negocio (BI) en coordinación con el Departamento de TIC, conforme se establece en el Procedimiento S3.2.P6 "Gestión de Tableros de Inteligencia de Negocios".
- Cada área debe designar un responsable principal y un responsable alterno de tableros BI, de manera documentada, los cuales recibirán la capacitación del Departamento de TIC. El responsable principal recibirá la licencia correspondiente y será el encargado de gestionar los tableros del área una vez publicados.
- La organización de los tableros BI en el repositorio oficial se realizará bajo el concepto de dominio y subdominio: cada gerencia será considerada un dominio y, dentro de cada gerencia, los departamentos funcionarán como subdominios. Esto permitirá una estructura jerárquica, ordenada y segura para la administración y acceso a los tableros (ver figura 2).
- Adicionalmente, cada responsable deberá mantener un registro actualizado de los cambios realizados en los tableros BI, asegurando la trazabilidad y facilitando auditorías internas cuando sean requeridas.
- La visualización de los tableros BI se realizará a través del intranet institucional designado para cada gerencia y/o departamento, permitiendo que los tableros sean accesibles dentro del espacio correspondiente a cada unidad organizacional.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

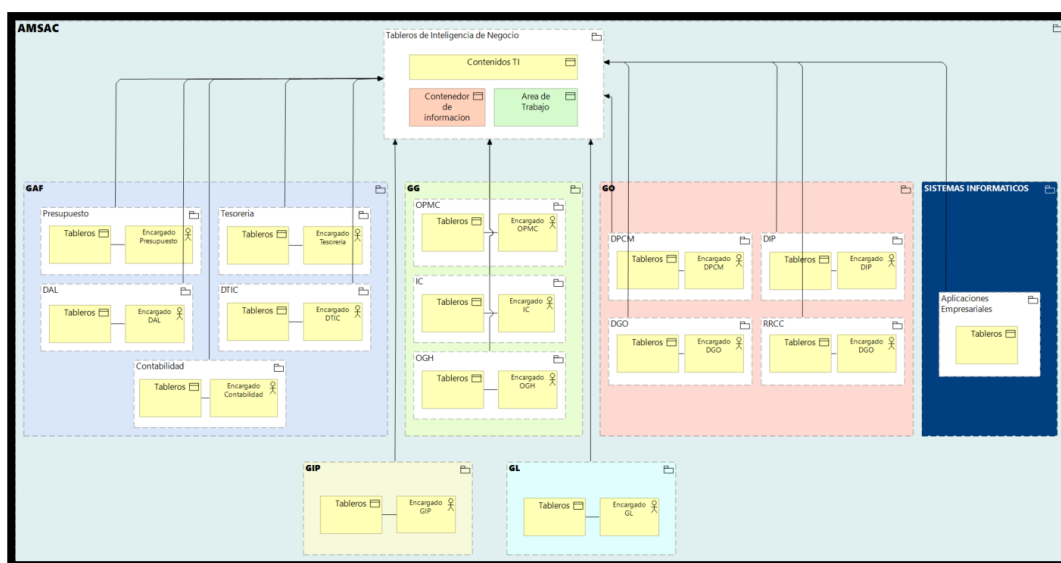


Figura 2: Arquitectura de Publicación de Tableros de Inteligencia de Negocio

2.3.1.6 Seguridad del Equipo:

- **Contraseñas:** Las contraseñas de acceso a los equipos y sistemas deben cumplir con las políticas de seguridad establecidas (por ejemplo, longitud mínima, complejidad, y cambio periódico). El usuario no debe compartir sus contraseñas con terceros.
- **Bloqueo de Sesión:** Los usuarios deben bloquear su sesión o cerrar sesión cuando se alejen de su estación de trabajo, incluso por cortos períodos.
- **Protección Física:** Los equipos portátiles deben ser transportados en estuches adecuados y nunca deben dejarse desatendidos en lugares públicos. En la oficina, los equipos deben estar asegurados con los mecanismos físicos disponibles (como anclajes de seguridad).

2.3.1.7 Uso de Dispositivos Móviles (BYOD):

- **Autorización de Dispositivos:** Antes de utilizar un dispositivo personal para acceder a la red o aplicaciones corporativas, los usuarios deben obtener la autorización del Departamento de TIC y configurar el dispositivo conforme a las políticas de MDM (Mobile Device Management).
- **Seguridad en Dispositivos Móviles:** Todos los dispositivos móviles utilizados para fines laborales deben tener activado el cifrado, bloqueo por PIN o biometría, y deben ser compatibles con las políticas de seguridad establecidas por la empresa.
- **Aplicaciones Móviles:** Solo se deben instalar y utilizar aplicaciones móviles aprobadas para el trabajo. Las aplicaciones que no cumplan con los estándares de seguridad de la empresa están prohibidas.

2.3.1.8 Uso de Recursos Compartidos:

- **Impresoras y Escáneres:** Los recursos compartidos, como impresoras y escáneres, deben utilizarse sólo para actividades relacionadas con el trabajo. Los usuarios deben seguir las instrucciones para el uso eficiente y responsable de estos recursos.
- **Archivos Compartidos:** Los archivos y documentos almacenados en carpetas compartidas deben ser accesibles según los permisos asignados. Los usuarios deben respetar los permisos de acceso y no modificar o eliminar archivos sin la debida autorización.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- **Telefonía:** El uso de teléfonos fijos y móviles de la empresa debe limitarse a comunicaciones laborales. Las llamadas personales deben ser evitadas, y en caso de emergencia, deben ser breves.

2.3.1.9 Soporte técnico:

- **Solicitud de Soporte:** Los usuarios deben contactar al Departamento de TIC para cualquier problema técnico o de seguridad a través de los canales oficiales de soporte (sistema de tickets). El personal de TIC proporcionará asistencia de acuerdo con las prioridades establecidas.
- **Reporte de Incidencias:** Cualquier incidente de seguridad o fallo crítico debe ser reportado de inmediato al Departamento de TIC. Los usuarios deben proporcionar toda la información necesaria para facilitar la resolución del problema.
- **Mantenimiento Preventivo:** El Departamento de TIC programará mantenimiento preventivo de los equipos, durante el cual los usuarios deben colaborar y permitir acceso a los dispositivos para asegurar su correcto funcionamiento y conservación.

2.3.2 Cuenta de usuario y servicio de correo electrónico

- El personal de AMSAC contará con una cuenta de usuario del dominio para el acceso a la red y una cuenta de correo electrónico, la cual deberá ser solicitada por intermedio y con la autorización de la Oficina de Gestión Humana utilizando la plataforma Web SIGAP "Sistema Integrado de Gestión de Accesos y Permisos", mediante el formato S3.2.P2.F1 "Solicitud de Alta/Baja de Usuario o Cambio de Perfil". En caso se trate de personal externo, la solicitud debe ser gestionada por el Jefe de Departamento y/o Gerencia del área, según el Procedimiento S3.2.P2 "Gestión de accesos". Esta solicitud debe ser elevada al Jefe del Departamento de TIC para su evaluación y aprobación final.
- Las cuentas de usuario son de uso personal e intransferible, no permitiéndose que otras personas hagan uso de ella, salvo los casos de control técnico administrativo que puede realizar el Departamento de TIC, siempre y cuando las Gerencias autoricen dicho acceso por escrito expresamente.
- El usuario es responsable de la información que se guarde en su computador y de la información que sea enviada desde su cuenta, por ello debe asegurar el uso adecuado y ético de la información que disponga.
- La información contenida en las computadoras y los mensajes de correo electrónico no podrán reproducirse o utilizarse para fines ajenos a las funciones de la empresa.
- El Departamento de TIC proveerá y gestionará recursos de software que preserven la integridad, disponibilidad y confidencialidad de las cuentas de usuario.
- El usuario debe proteger sus credenciales y evitar su divulgación. Las contraseñas deberán cumplir los requisitos de seguridad establecidos por el Departamento de TIC respecto a longitud, complejidad, historial, vigencia y bloqueo de cuentas. Asimismo, AMSAC podrá exigir el uso de autenticación multifactor para los servicios definidos como críticos o que procesen información sensible.
- El usuario debe depurar los correos electrónicos que recibe para evitar sobrepasar el tamaño de buzón de correo asignado de acuerdo con su perfil. El respaldo del buzón de correo dependerá del Plan de respaldo definido por el Departamento de TIC. Los demás mensajes deberán mantenerse en carpetas personales.
- El envío de archivos confidenciales a través del correo electrónico se realizará con la debida autorización del Gerente de área y utilizando mecanismos de seguridad que podrán ser recomendados por TIC.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- Los archivos que se adjuntan en los mensajes de correo electrónico, en lo posible deben de comprimirse a fin de evitar el saturamiento involuntario de los buzones de los usuarios. La cuota límite por archivo adjunto para la red interna de AMSAC es de 20 MB. Otras entidades pueden tener cuotas inferiores, por lo que mensajes 'grandes' no podrían ser recibidos. Asimismo, los mensajes externos con cuotas superiores a 20 MB no podrán ingresar a los buzones de correo de AMSAC, el requerimiento de una ampliación de la cuota de ser solicitado utilizando la plataforma Web SIGAP "Sistema Integrado de Gestión de Accesos y Permisos", mediante el formato S3.2.P2.F1 "Solicitud de Alta/Baja de Usuario o Cambio de Perfil" y con la debida autorización según el procedimiento S3.2.P2 Gestión de accesos.
- Al responder comunicados generales o para un grupo específico de usuarios, el usuario debe cuidar de no generar cadenas y/o múltiples destinos, salvo cuando ésta sea la finalidad de la respuesta.
- El correo electrónico es un servicio de comunicación en intercambio de información institucional, no siendo un servicio de difusión indiscriminada de información.
- La firma del usuario debe estar en concordancia con las directrices de imagen institucional de AMSAC, de acuerdo con la firma designada por el Departamento de TIC.
- Está expresamente prohibido:
 - Enviar o contestar cadenas de correo.
 - El uso de la cuenta para fines distintos a las actividades de la institución.
 - El uso de un lenguaje inapropiado en sus comunicaciones.
 - Suscribirse a listas de interés que no guarden relación con la actividad laboral asignada.
 - Adjuntar o retransmitir archivos con información de procedencia dudosa, que podría contener spam o virus.
- En caso de cese laboral de un funcionario o trabajador de AMSAC, la Oficina de Gestión Humana debe notificar el hecho utilizando la plataforma Web SIGAP "Sistema Integrado de Gestión de Accesos y Permisos", mediante el formato S3.2.P2.F1 "Solicitud de Alta/Baja de Usuario o Cambio de Perfil". En caso de finalización del servicio de personal externo, el área usuaria deberá notificar el hecho utilizando el mismo formato. En ambos casos, la baja de usuario debe seguir el procedimiento S3.2.P2 Gestión de accesos, a efecto del bloqueo de la cuenta.
- En caso se requiera un cambio de perfil del usuario asignado a un funcionario o trabajador de AMSAC, el Jefe de Departamento y/o Gerencia del área debe elevar esta solicitud al Departamento de TIC utilizando la plataforma Web SIGAP "Sistema Integrado de Gestión de Accesos y Permisos", mediante el formato S3.2.P2.F1 "Solicitud de Alta/Baja de Usuario o Cambio de Perfil" según el procedimiento S3.2.P2 Gestión de accesos, a fin de efectuar el cambio.
- **Gestión de cuentas de usuario**
 - Toda cuenta de usuario deberá ser única e individual, permitiendo identificar inequívocamente al usuario responsable de las actividades realizadas mediante dicha cuenta. La nomenclatura de las cuentas institucionales será definida y administrada por el Departamento de TIC, manteniendo criterios uniformes para su identificación y trazabilidad.
 - Las cuentas de usuario deberán estar asociadas a una persona, área o servicio debidamente identificado y contar con la documentación de autorización correspondiente conforme al Procedimiento S3.2.P2 "Gestión de accesos".

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- **Gestión de cuentas genéricas y compartidas**

- La creación y utilización de cuentas genéricas o compartidas deberá restringirse únicamente a casos debidamente justificados por necesidades operativas o técnicas que impidan la utilización de cuentas nominativas individuales.
- Toda cuenta genérica o compartida deberá contar con un responsable designado por el área usuaria, quien será responsable de su uso, custodia, revisión y solicitud de baja cuando deje de ser necesaria.
- La creación de cuentas genéricas o compartidas requerirá autorización expresa del Jefe del Departamento de TIC y deberá registrarse en los controles de acceso administrados por el Departamento de TIC.
- Las cuentas genéricas o compartidas deberán ser revisadas como mínimo una vez por semestre con el fin de validar su vigencia, necesidad operativa y nivel de acceso autorizado.

- **Gestión de accesos privilegiados**

- La gestión de accesos privilegiados comprende los derechos, roles, perfiles o permisos administrativos otorgados mediante cuentas privilegiadas, grupos administrativos u otros mecanismos de autorización que permitan administrar, configurar o modificar infraestructura tecnológica, servidores, dispositivos de comunicaciones y seguridad, bases de datos, sistemas de información, aplicaciones, plataformas y servicios en nube, sitios SharePoint, cuentas de servicio y demás recursos TIC críticos de AMSAC.
- Se encuentran comprendidos en esta gestión, según corresponda, los administradores de infraestructura, sistemas, aplicaciones, bases de datos, dispositivos de comunicaciones y seguridad; los miembros de grupos administrativos; los administradores de plataformas y servicios en nube; los propietarios o administradores de sitios SharePoint; las cuentas de servicio con privilegios elevados; así como el personal interno o externo al que se otorguen capacidades administrativas sobre los recursos TIC de AMSAC.
- La asignación de accesos privilegiados deberá responder a una necesidad operativa debidamente justificada y autorizada por el Jefe del Departamento de TIC, aplicando los principios de mínimo privilegio y necesidad de conocer. Los privilegios otorgados deberán limitarse exclusivamente a aquellos necesarios para el cumplimiento de las funciones o actividades autorizadas.
- Cuando la tecnología lo permita, las cuentas utilizadas para realizar actividades administrativas deberán ser nominativas y diferenciadas de las cuentas empleadas para las actividades cotidianas del usuario, con la finalidad de asegurar la identificación y trazabilidad de las acciones ejecutadas con privilegios elevados.
- Los accesos privilegiados deberán utilizarse exclusivamente para actividades de administración, configuración, mantenimiento, soporte u otras funciones técnicas previamente autorizadas. Las cuentas administrativas diferenciadas no deberán utilizarse para actividades de usuario estándar, tales como navegación web, correo electrónico o procesamiento habitual de documentos.
- El Departamento de TIC gestionará los accesos privilegiados durante todo su ciclo de vida, comprendiendo su solicitud, evaluación, aprobación, asignación, modificación, revisión periódica, suspensión y retiro, de acuerdo con lo establecido en el Procedimiento S3.2.P2 "Gestión de Accesos".
- El Departamento de TIC mantendrá un registro actualizado de los accesos privilegiados asignados sobre los recursos TIC de AMSAC, que permita identificar, como mínimo, al usuario o cuenta asociada, el recurso o sistema, el rol, grupo o privilegio otorgado, la justificación, la autorización, la vigencia, el estado del acceso y la fecha de su última revisión.
- Las actividades realizadas mediante cuentas o accesos privilegiados deberán estar sujetas a mecanismos de registro, monitoreo y auditoría, de acuerdo con las capacidades disponibles en cada recurso o plataforma tecnológica. Los registros deberán permitir, cuando técnicamente corresponda, identificar accesos, cambios de

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

configuración, creación o modificación de usuarios, asignación de permisos y demás acciones administrativas relevantes.

- Los accesos privilegiados deberán ser revisados como mínimo trimestralmente, con la finalidad de verificar su vigencia, necesidad operativa, correspondencia con las funciones asignadas y cumplimiento del principio de mínimo privilegio. Los resultados de estas revisiones deberán conservarse como evidencia de su ejecución.
 - Los accesos privilegiados deberán ser modificados, suspendidos o retirados oportunamente cuando desaparezca la necesidad operativa que justificó su asignación, se produzca un cambio de funciones o perfil, ocurra el cese del personal o la finalización de la relación contractual, venza una autorización temporal, el resultado de una revisión determine que el privilegio ya no es requerido o se identifique un riesgo de seguridad que requiera su revocación.
- **Gestión de cuentas de servicio**
 - Las cuentas de servicio utilizadas por aplicaciones, procesos automatizados, integraciones o componentes de infraestructura deberán contar con un propietario funcional y un responsable técnico claramente identificados.
 - Las cuentas de servicio deberán ser utilizadas exclusivamente para la operación de los servicios tecnológicos autorizados y no podrán emplearse para el inicio de sesión interactivo por parte de usuarios, salvo que exista una justificación técnica documentada y aprobada por el Departamento de TIC.
 - El Departamento de TIC mantendrá un inventario actualizado de las cuentas de servicio, indicando como mínimo el nombre de la cuenta, sistema asociado, responsable, fecha de creación, privilegios asignados y fecha de revisión.
 - Las cuentas de servicio y cuentas privilegiadas serán revisadas periódicamente para verificar que mantengan únicamente los permisos necesarios para el cumplimiento de sus funciones y que continúen siendo requeridas por la organización.
 - **Gestión de autenticación y protección de credenciales**
 - Toda cuenta de usuario deberá utilizar los mecanismos de autenticación definidos por el Departamento de TIC, garantizando la identificación inequívoca del usuario y la trazabilidad de las actividades realizadas sobre los recursos tecnológicos de AMSAC.
 - El acceso al correo electrónico institucional, servicios en la nube, sistemas de información, plataformas administrativas y demás recursos definidos por el Departamento de TIC deberá utilizar mecanismos de autenticación multifactor (MFA), cuando la tecnología lo permita y de acuerdo con la criticidad del servicio.
 - Las credenciales de acceso, contraseñas, códigos de autenticación, tokens, certificados digitales, aplicaciones autenticadoras y demás mecanismos de autenticación son personales e intransferibles, quedando prohibida su divulgación o compartición con terceros.
 - El Departamento de TIC implementará controles destinados a proteger las credenciales frente a accesos no autorizados, pérdida, modificación, divulgación o uso indebido.
 - Las credenciales asociadas a cuentas privilegiadas, cuentas de servicio, dispositivos de red, plataformas de administración y demás sistemas críticos deberán almacenarse únicamente en repositorios seguros o gestores de credenciales autorizados por AMSAC.
 - Está prohibido almacenar credenciales en archivos de texto, hojas de cálculo, correos electrónicos, aplicaciones de mensajería u otros medios que no cuenten con mecanismos adecuados de protección y control de acceso.
 - **Bloqueo de cuentas**
 - AMSAC implementará mecanismos automáticos de bloqueo temporal de cuentas ante intentos fallidos de autenticación, con la finalidad de prevenir accesos no autorizados,

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

ataques de fuerza bruta y otras amenazas relacionadas con la seguridad de la información.

- Los criterios de bloqueo de cuenta, duración del bloqueo y restablecimiento del contador de intentos fallidos serán definidos y administrados por el Departamento de TIC de acuerdo con los estándares de seguridad vigentes.
- Los eventos asociados al bloqueo de cuentas deberán registrarse y mantenerse disponibles para fines de monitoreo, auditoría e investigación de incidentes de seguridad de la información.

• **Revisión periódica de accesos y credenciales**

- El Departamento de TIC realizará revisiones periódicas de las cuentas de usuario, cuentas privilegiadas, cuentas compartidas, cuentas genéricas y cuentas de servicio como mínimo una vez por trimestre.
- Durante las revisiones se verificará la vigencia del acceso, la necesidad operativa, el responsable asignado, el nivel de privilegios otorgado y el cumplimiento del principio de mínimo privilegio.
- Toda cuenta que no cuente con justificación operativa vigente o cuyo responsable no pueda ser identificado deberá ser evaluada para su suspensión, restricción o eliminación.
- Los resultados de las revisiones deberán conservarse como evidencia de cumplimiento de los controles de acceso y seguridad de la información establecidos por AMSAC.

2.3.3 Servicio de Internet

- El acceso a internet debe ser solicitado al Departamento de TIC utilizando la plataforma Web SIGAP “Sistema Integrado de Gestión de Accesos y Permisos”, mediante el formato S3.2.P2.F1 “Solicitud de Alta/Baja de Usuario o Cambio de Perfil” y con la debida autorización según el procedimiento S3.2.P2 Gestión de accesos. En el caso que el acceso a internet se solicite como parte del alta de usuario, la solicitud es por intermedio de la Oficina de Gestión Humana; de lo contrario, la solicitud es por intermedio del Jefe de Departamento y/o Gerencia del área.
- Según el perfil de la cuenta asignada, desde el equipo asignado será posible hacer uso del servicio de acceso a Internet de acuerdo con su perfil, únicamente para fines institucionales y relacionados con actividades de trabajo. Cada usuario es responsable de las actividades realizadas en el uso de internet, así como de las páginas a las que accede desde su computadora y cuenta asignada.
- El Departamento de TIC proveerá y gestionará recursos de software que minimicen los riesgos provenientes del servicio de internet. El Departamento de TIC tiene la facultad de controlar y negar el acceso a sitios Web que violen lo dispuesto en la presente directiva y otras normas de la empresa.
- El Departamento de TIC no ejerce control sobre el contenido y calidad de la información proveniente de Internet o de quien la genere. El usuario es responsable exclusivo por cualquier información obtenida o remitida a través de este servicio.
- El acceso a las páginas web bloqueadas debe ser solicitado al Departamento de TIC utilizando el formato S3.2.P2.F3 “Exoneración de restricción de TIC” y con la debida autorización según el procedimiento S3.2.P2 “Procedimiento de Gestión de Accesos”. El Oficial de Seguridad y Confianza Digital evaluará la solicitud y, de ser procedente, el Jefe del Departamento de TIC suscribirá la aprobación final.
- El acceso a páginas web bloqueadas que pudiera autorizarse será únicamente para actividades laborales justificadas, dentro del ámbito de las funciones del usuario y

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

conforme a las políticas y directivas de seguridad de la información de AMSAC. Dicho acceso podrá ser objeto de monitoreo y auditoría posteriores. El uso indebido o no autorizado podrá derivar en la revocación del permiso concedido y en la aplicación de las medidas disciplinarias correspondientes.

- **Está prohibido:**
 - Descargar audio, videos, imágenes o acceder a lugares que distribuyan material que no tengan relación con las actividades laborales.
 - Utilizar los servicios de radio, televisión, mensajería instantánea y juegos que congestione el ancho de banda y exponga a riesgo a la red de AMSAC.
- Cuando se permita el acceso a internet, se requerirá el uso de canales seguros como VPN con autenticación robusta para proteger la confidencialidad e integridad de la información.
- El personal externo y visitantes que requieran acceso a internet deberán contar con la autorización previa del Departamento de TIC. Estos usuarios deberán conectarse exclusivamente a una red separada y externa a la red principal de AMSAC, diseñada para garantizar la seguridad en el uso de los recursos institucionales.
- El uso del servicio de internet sin la solicitud y autorización correspondiente será considerado una infracción a las políticas de seguridad de AMSAC. En tales casos, el Departamento de TIC procederá a restringir o bloquear el acceso a internet del usuario, y podrá iniciar las acciones disciplinarias y/o administrativas correspondientes conforme al reglamento interno de la entidad.
- El Departamento de TIC realizará monitoreo continuo del tráfico de internet para detectar actividades sospechosas, intentos de intrusión, accesos no autorizados o cualquier comportamiento que pueda afectar la seguridad y estabilidad de la red.
- En caso de detectar actividades maliciosas o violaciones de seguridad asociadas al uso de internet, el Departamento de TIC activará los protocolos de respuesta inmediata para contener, mitigar y reportar el incidente conforme a las políticas de seguridad.

2.3.4 Servicio de Intranet

- El acceso a la intranet institucional estará restringido únicamente a usuarios autorizados, salvo que se disponga expresamente su carácter público.
- La información publicada en la intranet es de uso interno y está prohibida su divulgación, extracción o transferencia fuera del ámbito de la empresa, así como su utilización para fines distintos a los establecidos oficialmente.
- La intranet constituye el medio oficial para el acceso controlado a documentos institucionales vigentes. Los espacios de almacenamiento interno de cada área (departamental o gerencial) están destinados exclusivamente a la gestión y archivo de documentos operativos internos, sin carácter de publicación oficial.
- Es responsabilidad de cada usuario mantener actualizada la información bajo su competencia y revisar periódicamente los contenidos publicados en la intranet institucional. El desconocimiento de la información publicada no exime de responsabilidad.
- La visualización de los tableros BI se realizará a través del intranet institucional, en los espacios designados para cada gerencia y departamento. El acceso a los tableros estará segmentado conforme a la estructura de dominios y subdominios, permitiendo que cada unidad organizacional acceda únicamente a la información que le corresponde, de acuerdo con los niveles de autorización establecidos.

2.3.5 Sitio web de la empresa

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- Todas las áreas que tienen información publicada en el sitio web de la empresa, bajo responsabilidad, deben revisar y realizar las gestiones para la actualización de la información que sea de su competencia, en coordinación con el área de Imagen Corporativa, según lo establecido en el Procedimiento E4.1.P2 “Actualización de Contenidos de la Página Web Institucional”.
- La publicación de información en el sitio web del Portal de Transparencia Estándar de la empresa se realiza según lo establecido en el Procedimiento E2.1.2.P1 “Transparencia y Acceso a la Información Pública”.

2.3.6 Sistemas de Información

- El acceso a los Sistemas de Información o aplicaciones será configurado por perfiles de usuario, de acuerdo al requerimiento de las áreas usuarias. Para gestionar este acceso, el área usuaria debe presentar su solicitud al Departamento de TIC utilizando la plataforma Web SIGAP “Sistema Integrado de Gestión de Accesos y Permisos”, mediante el formato S3.2.P2.F2 “Solicitud de Uso de Aplicaciones”, y con la autorización del Jefe, Supervisor o Coordinador del área usuaria, según el Procedimiento S3.2.P2 “Gestión de accesos”.
- La información generada en los sistemas de información es de uso exclusivo de AMSAC, encontrándose prohibida la divulgación, extracción y transferencia de la información fuera del ámbito de la empresa y para fines ajenos a los establecidos.
- El Departamento de TIC gestionará recursos de software y hardware que garanticen la disponibilidad, integridad y resguardo de la información.
- Para garantizar el cumplimiento de las normativas legales y éticas en el uso de software y propiedad intelectual, AMSAC establece lo siguiente:
 - Se debe utilizar exclusivamente software con licencias adquiridas legalmente por la empresa.
 - Está prohibida la instalación o uso de software no autorizado, versiones piratas o sin licencia.
 - Las actualizaciones y renovaciones de licencias serán gestionadas por el Departamento de TIC.
 - Se debe respetar la propiedad intelectual de terceros en documentos, imágenes, videos y cualquier contenido digital.
 - Se deben citar y reconocer adecuadamente las fuentes de información utilizadas en el trabajo.
- El usuario es responsable de gestionar de manera diligente la información que ingresa, modifica y/o anula en el sistema. Toda acción realizada queda registrada y sujeta a control mediante los mecanismos de auditoría disponibles.

2.3.7 Impresiones

- El acceso a los recursos compartidos para imprimir, copiar y/o escanear documentos puede ser solicitado al Departamento de TIC por el área usuaria utilizando la plataforma Web SIGAP “Sistema Integrado de Gestión de Accesos y Permisos”, mediante el formato S3.2.P2.F1 “Solicitud de Alta/Baja de Usuario o Cambio de Perfil” y con la debida autorización según el procedimiento S3.2.P2 “Gestión de accesos”.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- Los servicios de los recursos compartidos están disponibles para imprimir, copiar y/o escanear documentos institucionales y trabajos relacionados con la labor de los usuarios. Está prohibido el uso del recurso compartido para la impresión, copia o escaneo de material particular ajeno al interés de la empresa.
- El Departamento de TIC implementará y ejecutará los controles que permitan el cumplimiento de las disposiciones señaladas en el párrafo anterior.

2.3.8 Telefonía (fija y móvil)

- Se podrá solicitar el uso de telefonía fija utilizando la plataforma Web SIGAP “Sistema Integrado de Gestión de Accesos y Permisos”, mediante el formato S3.2.P2.F1 “Solicitud de Alta/Baja de Usuario o Cambio de Perfil” y con la debida autorización según el procedimiento S3.2.P2 “Gestión de accesos”. En el caso de telefonía móvil, el acceso a equipos, el nivel de servicio de plan de datos, radio, bolsa de minutos, entre otros, depende de las disposiciones internas de la empresa.
- El Departamento de TIC gestionará la central telefónica, redes de comunicaciones y los servicios contratados de telefonía móvil, que garanticen una buena calidad y disponibilidad del servicio.
- El Departamento de TIC gestionará la central telefónica, redes de comunicaciones y los servicios contratados de telefonía móvil, que garanticen una buena calidad y disponibilidad del servicio.
- Está prohibido utilizar el servicio de telefonía otorgada por AMSAC para fines distintos a las labores de trabajo.

2.3.9 Comunicaciones

- El Departamento de TIC gestionará los enlaces dedicados de datos y radio.

2.4 Seguridad de la información

2.4.1 Disposiciones para la relación con proveedores

El Departamento de TIC establece las siguientes disposiciones de seguridad de la información en su relación con proveedores:

- Identificar y documentar los tipos de servicios que pueden afectar la confidencialidad, integridad y disponibilidad de la información de AMSAC.
- Definir, documentar y clasificar los requisitos de seguridad de la información que deben cumplir los postores y contratistas antes de realizar una contratación, que signifique el acceso, uso, procesamiento, mantenimiento o custodia de activos de información de AMSAC, se debe identificar, dichos requisitos deben ser establecidos sobre una base de análisis de riesgos de seguridad de la información.
- Determinar el nivel de acceso a la información de AMSAC utilizando la plataforma Web SIGAP “Sistema Integrado de Gestión de Accesos y Permisos”, mediante el formato S3.2.P2.F1 “Solicitud de Alta/Baja de Usuario o Cambio de Perfil” según el Procedimiento S3.2.P2 “Gestión de accesos”.
- Suscribir acuerdos de confidencialidad, no divulgación, protección de datos personales, buen uso de los activos de información al momento del inicio de la contratación.
- Identificar y evaluar a los proveedores, determinando los niveles a los que se permitirá su acceso a la información de AMSAC, monitoreando y controlando periódicamente sus actividades, detallando las funciones del proveedor y de AMSAC.
- Determinar cómo se puede afectar la confidencialidad, integridad y disponibilidad de la información de AMSAC, con los accesos concedidos a los proveedores, estableciendo

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

los controles adecuados de tal manera que los riesgos definidos puedan ser mitigados de forma adecuada.

- Realizar la selección, monitoreo y evaluación adecuados de los proveedores de los servicios en nube.
- Establecer y monitorear todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TIC que dan soporte, a la información de AMSAC.
- Solicitar a los proveedores que suministren productos TIC, la funcionalidad del software utilizado por el producto, la debida información de la seguridad de éste, estableciendo los procedimientos de monitoreo y validación.
- Identificar y documentar los productos y/o servicios críticos brindados y/o gestionados por el proveedor, en especial aquellos que se encuentren, ejecuten, gestionen o desarrollen fuera de AMSAC, especialmente aquellos en los cuales el proveedor subcontrate el producto y/o servicio.
- Exigir certificados en ISO/IEC 27001 actualizados y vigentes, a los proveedores más críticos, tales como servicios tercerizados de TIC, proveedores de servicios de seguridad de TIC, entre otros.
- Verificar que el proveedor cuenta con las capacidades y experiencia relacionados con los requerimientos solicitados, a fin de garantizar los niveles de continuidad de servicio.
- Garantizar que los productos y/o servicios brindados por el proveedor sean originales y no se modifiquen sus especificaciones.
- Asegurar que el proveedor comunique a AMSAC todos los incidentes de seguridad de la información que se presenten durante la prestación de su servicio, los cuales deben ser revisados de acuerdo con los procedimientos establecidos.
- Garantizar la terminación segura de la relación con el proveedor; para ello se debe considerar:
 - La revocación de los accesos brindados al proveedor.
 - El manejo de la información de AMSAC en posesión del proveedor.
 - La determinación de la propiedad intelectual del software desarrollado y/o utilizado por el proveedor durante la prestación de sus servicios.
 - La transferencia de la información en caso de cambio de proveedor.
 - La gestión de los registros generados durante la prestación de los servicios del proveedor.
 - Se debe constatar que el proveedor no mantenga en sus propias instalaciones o en aquellas gestionadas por el proveedor, activos de información que son propiedad de AMSAC.
 - La eliminación en forma segura de los activos de información en diferentes dispositivos y unidades de almacenamiento del proveedor.
 - La continuidad de los acuerdos de confidencialidad, no divulgación, protección de datos personales, buen uso de los activos de información, una vez finalizados los servicios brindados por el proveedor.
- **Revisión de continuidad y seguridad de proveedores**
 - Para los servicios críticos brindados por proveedores que soporten el procesamiento, almacenamiento, transmisión o protección de información institucional, AMSAC deberá verificar que existan planes de continuidad, contingencia o recuperación ante desastres apropiados para los servicios contratados.
 - El Departamento de TIC realizará como mínimo una revisión anual de los planes de contingencia asociados a los servicios críticos contratados, con la finalidad de verificar su vigencia, efectividad y alineamiento con los requisitos de seguridad de la información de AMSAC.
 - Adicionalmente, las revisiones deberán efectuarse cuando se produzcan cambios significativos en los servicios, en la infraestructura tecnológica, en los requisitos regulatorios o en los controles de seguridad de la información que puedan afectar la continuidad o disponibilidad de los servicios contratados.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- AMSAC podrá solicitar al proveedor evidencias documentadas de pruebas, simulacros, actualizaciones o revisiones realizadas a sus planes de continuidad y contingencia.
- El Departamento de TIC realizará seguimiento periódico al cumplimiento de los compromisos de seguridad establecidos con los proveedores críticos, considerando indicadores o métricas relacionadas con disponibilidad, incidentes de seguridad, tiempos de atención, recuperación de servicios, gestión de vulnerabilidades y cumplimiento de los niveles de servicio establecidos contractualmente.
- Los resultados de las revisiones y evaluaciones deberán conservarse como evidencia para fines de auditoría, gestión de riesgos y mejora continua.

2.4.2 Disposiciones de uso seguro de los servicios de red

El Departamento de TIC deberá garantizar la protección y el uso seguro de los servicios de red de AMSAC mediante la implementación, mantenimiento y supervisión de controles de seguridad acordes con la criticidad, exposición y riesgos asociados. Para ello, deberá:

- Mantener activos, actualizados y en operación los firewalls y demás mecanismos de seguridad destinados a proteger las redes y controlar las comunicaciones.
- Mantener una zona desmilitarizada (DMZ) u otros mecanismos de segregación equivalentes para aislar los servicios expuestos y proteger la red interna frente al tráfico proveniente de redes no confiables.
- Implementar mecanismos para detectar, prevenir y bloquear amenazas que puedan comprometer la infraestructura de red, incluyendo malware, accesos no autorizados y otras actividades que representen riesgos para la seguridad de la información.
- Restringir la conexión de equipos personales o dispositivos no autorizados a la red interna de AMSAC, salvo aquellos casos expresamente autorizados y sujetos a los controles de seguridad establecidos por el Departamento de TIC.
- Asegurar que las conexiones hacia la red interna de AMSAC provenientes de redes externas o no confiables utilicen mecanismos de acceso seguro y cumplan con los controles de autenticación y seguridad establecidos por la organización, con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información.
- Asegurar que los servicios críticos de red, incluyendo resolución de nombres (DNS), acceso remoto mediante VPN, correo electrónico, acceso a Internet y otros servicios de comunicaciones que correspondan, cuenten con configuraciones y controles de seguridad acordes con su criticidad, exposición y riesgos asociados.
- Definir, implementar, mantener y revisar periódicamente las configuraciones de seguridad de los servicios críticos de red, considerando, según corresponda, mecanismos de autenticación, control de accesos, protección frente a amenazas, monitoreo, registro de eventos, disponibilidad y actualización de las configuraciones.
- Aplicar los requisitos mínimos de configuración segura establecidos en el Instructivo S3.3.IN1 “Configuración Segura y Hardening de Activos TIC”, administrado por el Departamento de TIC.
- Mantener mecanismos de segmentación y segregación de red de acuerdo con la función, criticidad y nivel de exposición de los activos y servicios tecnológicos, restringiendo las comunicaciones entre segmentos a aquellas necesarias y autorizadas para la operación.
- Verificar periódicamente la eficacia de los controles de segmentación y segregación implementados y realizar, como mínimo una vez al año y ante cambios significativos que puedan afectar la segmentación, pruebas técnicas sobre los segmentos críticos para validar que las restricciones establecidas impidan comunicaciones no autorizadas y contribuyan a reducir el riesgo de movimiento lateral.
- Documentar y conservar los resultados de las revisiones y pruebas realizadas como evidencia de cumplimiento. Las desviaciones identificadas deberán ser evaluadas y gestionadas oportunamente por el Departamento de TIC.

2.4.3 Disposiciones de uso de los servicios en la nube

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

Para una adecuada seguridad de la información para el uso de los servicios en la nube, el Departamento de TIC debe:

- Realizar el monitoreo y supervisión del uso de los servicios en la nube para la gestión eficiente de la seguridad de la información, teniendo como propósito la mitigación de los riesgos de seguridad de la información asociados a información almacenada en la nube, a fin de prevenir la pérdida, robo y/o manipulación de información.
- Establecer controles que garanticen que la información almacenada en la nube permanezca protegida.
- Crear y/o actualizar los accesos a la nube sólo a las partes interesadas autorizadas según las disposiciones establecidas por AMSAC y de acuerdo al rol desempeñado.
- Monitorear de forma permanente las actividades realizadas en la nube; tales como: el ingreso, el cierre de sesión, carga y actualización de información, entre otros.
- El Departamento de TIC deberá establecer periodos de retención para las copias de respaldo almacenadas en servicios en la nube, considerando la criticidad de la información y de los servicios, necesidades de recuperación, capacidad de almacenamiento y requisitos legales, regulatorios o contractuales aplicables.
- Las copias de respaldo almacenadas en la nube deberán estar sujetas a un ciclo de vida definido que contemple su generación, conservación, verificación, recuperación y depuración o eliminación al finalizar el periodo de retención establecido, salvo que exista una necesidad técnica, legal o de continuidad del negocio que justifique su conservación por un periodo mayor.
- El Departamento de TIC deberá verificar periódicamente el cumplimiento de los periodos de retención y depuración establecidos para los respaldos en nube, conservando las evidencias que permitan acreditar su aplicación.
- Las frecuencias, periodos de retención, responsables y demás condiciones específicas aplicables a los respaldos serán gestionados conforme al Procedimiento S3.2.P1 “Gestión de Respaldo y Recuperación”.

2.4.4 Disposiciones de transferencia de información

El Departamento de TIC establece las siguientes disposiciones sobre transferencia de información:

- Proteger toda transferencia de información de la interceptación, acceso no autorizado, copia, enrutamiento incorrecto, reproducción, modificación, denegación de servicio o destrucción que no se encuentre autorizado por AMSAC.
- Implementar controles que garanticen la trazabilidad de la información y el no repudio, incluido el mantenimiento de una cadena de custodia de la información que sea adecuada durante el tránsito de la información.
- Proteger la información que se transmite vía correo electrónico, además de los datos adjuntos.
- Proteger el uso de medios de comunicación electrónica, tales como correo electrónico, repositorios digitales u otros, que es de entera responsabilidad del usuario que emplea estos medios, a fin de no comprometer la información de AMSAC.
- Implementar controles y restricciones para detectar los reenvíos de información a través del correo electrónico o enlaces del almacenamiento en la nube; y, en general establecer autorización para utilizar servicios públicos externos, mensajería instantánea, redes sociales, uso compartido de archivos y almacenamiento en nube.
- Aplicar mecanismos que puedan restringir al trabajador revelar información sensible o confidencial de AMSAC, mediante medios físicos, tecnológicos u otros.
- Contar con una lista aprobada de proveedores que presten el servicio de transferencia de información de manera física.
- Asegurar que se establezcan mecanismos para evaluar posibles incumplimientos de las disposiciones contenidas en la presente directiva y determinar la aplicación de las medidas disciplinarias que correspondan.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

2.4.5 Disposiciones de creación y control de accesos de TI

El Departamento de TIC establece las siguientes disposiciones para asegurar que la empresa cuente con un sistema de control de acceso adecuado:

- Prohibir el acceso físico y lógico para los trabajadores, practicantes y terceros, salvo que sea expresamente solicitado y autorizado.
- Establecer los controles correspondientes para las áreas físicas cuyo ingreso requiere autorización.
- Procedimiento de acceso seguro y controles de seguridad, como HTTPS, uso de usuario y contraseña, los cuales deben ser establecidos en los sistemas y aplicaciones.
- Llevar a cabo por parte de cada usuario un registro de los controles concedidos, el cual se tendrá que actualizar como mínimo anualmente o al presentarse cualquier cambio. El control general estará gestionado por el Departamento de TIC.
- Eliminar los derechos de acceso a información, activos de información e instalaciones de procesamiento de información de los trabajadores, practicantes y terceros al término de su empleo o convenio.
- Otorgar derechos de acceso temporal por un período de tiempo limitado y revocarlos en la fecha de vencimiento.
- Establecer horarios de acceso para los servicios y equipos, así como monitorear los accesos a los servicios y equipos que ocurren fuera de estos horarios establecidos para identificar potenciales comportamientos anómalos.
- Monitorear los accesos de los usuarios privilegiados, usuarios relacionados a proveedores y la actividad realizada por estos.
- Llevar un registro de las actividades realizadas durante el acceso a los servicios o equipos.
- El Departamento de TIC monitoreará el uso de herramientas con privilegios elevados o capacidad de modificación de controles de seguridad, manteniendo registros de auditoría y alertas ante actividades no autorizadas.

2.4.6 Disposiciones de contraseñas seguras de TI

El Departamento de TIC establece las siguientes disposiciones para la creación y gestión de contraseñas seguras, que permitan garantizar la protección de la información y prevenir accesos no autorizados:

- La contraseña debe tener al menos 12 caracteres y debe incluir letras mayúsculas y minúsculas, números y caracteres especiales.
- Las contraseñas deben cambiarse mínimo cada 03 meses y no se deben reutilizar las últimas 24 contraseñas.
- Las contraseñas son personales y no se debe compartir con terceros.
- No escribirlas en documentos accesibles ni almacenarlas sin cifrado.
- Usar gestores de contraseñas autorizados por la empresa.

2.4.7 Disposiciones de continuidad de la seguridad de la información.

El Departamento de TIC realiza copias de seguridad periódicas y mantiene un plan de continuidad informático que incluye:

- Procedimientos de respaldo y restauración de datos en caso de incidentes.
- Pruebas regulares de respaldo y recuperación, para asegurar la disponibilidad de los sistemas críticos.
- Los planes de continuidad, contingencia y recuperación asociados a los servicios tecnológicos críticos deberán revisarse como mínimo una vez al año.
- Asimismo, deberán revisarse y actualizarse cuando se produzcan cambios relevantes en la infraestructura tecnológica, procesos críticos, riesgos identificados, proveedores estratégicos o controles de seguridad de la información.
- El Departamento de TIC mantendrá registros de las revisiones efectuadas, así como de las acciones de mejora identificadas durante dichas evaluaciones.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

2.4.8 Disposiciones de uso de software legal y respeto a la propiedad intelectual.

El Departamento de TIC establece las siguientes disposiciones para garantizar el uso de software legal y el respeto a la propiedad intelectual:

- Utilizar exclusivamente software con licencias adquiridas legalmente por la empresa.
- Está prohibida la instalación o uso de software no autorizado, versiones piratas o sin licencia.
- Las actualizaciones y renovaciones de licencias serán gestionadas por el Departamento de TIC.
- Respetar la propiedad intelectual de terceros en documentos, imágenes, videos y cualquier contenido digital.
- Citar y reconocer adecuadamente las fuentes de información utilizadas en el trabajo.

2.4.9 Disposiciones de protección de registros de eventos

El Departamento de TIC establece las siguientes disposiciones de protección de registros de eventos:

- Todos los sistemas críticos deben generar y almacenar logs de actividad.
- Los registros deben contener información detallada como usuario, fecha, hora, origen y tipo de evento.
- Los logs deben almacenarse en servidores seguros con acceso restringido.
- Solo el personal autorizado podrá acceder y gestionar los registros.
- Los logs deben protegerse contra modificaciones no autorizadas y eliminación accidental o intencional.
- Los registros de eventos deberán incluir la instalación, ejecución, actualización o eliminación de software considerado privilegiado o de alto riesgo, manteniéndose mecanismos de correlación y alertamiento automático sobre actividades no autorizadas.

2.4.10 Disposiciones de confidencialidad

El Departamento de TIC establece las siguientes disposiciones de confidencialidad:

- Firmar acuerdos de confidencialidad y/o no divulgación de la información, los cuales serán revisados y firmados de forma periódica o de existir un cambio normativo o legal.
- El trabajador, al terminar su relación contractual con AMSAC, deberá cumplir con la obligación de preservar la confidencialidad de la información, protección de propiedad intelectual y otros conocimientos que se detallan en los acuerdos de confidencialidad.

2.4.11 Disposiciones de privacidad y protección de datos personales

El Departamento de TIC establece las siguientes disposiciones para garantizar la seguridad de la información y protección de datos:

- Los datos serán recopilados y tratados conforme a la normativa vigente, con el consentimiento del titular cuando sea requerido.
- La información solo se usará para los fines determinados y legítimos de la organización.
- Se recolectará y procesará solo la información estrictamente necesaria.
- Se implementarán medidas de seguridad para evitar accesos no autorizados, alteraciones o pérdidas de datos.
- Solo se recopilarán datos personales cuando sean necesarios para las operaciones de AMSAC.
- Se informará a los titulares sobre el propósito y alcance del uso de su información.
- No se compartirán datos personales con terceros sin autorización expresa, salvo por obligaciones legales o contractuales.
- Se adoptarán medidas de seguridad físicas, técnicas y organizativas para proteger la información contra accesos no autorizados, filtraciones o alteraciones.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- Se aplicarán controles de acceso restringido según los roles y funciones de los empleados.
- Los titulares de los datos podrán solicitar acceso, rectificación, actualización o eliminación de su información.
- Se establecerán procedimientos internos y canales de contacto para gestionar estas solicitudes de manera oportuna.

2.4.12 Disposiciones de revisión de cumplimiento

El Departamento de TIC establece las siguientes disposiciones para la revisión de cumplimiento:

- Identificar, documentar y actualizar los requisitos legales y contractuales relevantes, así como de normativa interna, para cada sistema de información de AMSAC.
- Implementar procedimientos adecuados que aseguren el cumplimiento de los requerimientos legales, contractuales y de normativa interna respecto a los derechos de propiedad intelectual de los sistemas de información y el uso de productos de software patentados que utiliza AMSAC.
- Velar por que todo software de la empresa cuente con la respectiva licencia y se obtengan las licencias adicionales que fueren necesarias para cubrir sus operaciones. Queda prohibido el uso de software que no cuente con su respectiva licencia.
- Todo software desarrollado para AMSAC, ya sea por un trabajador o un tercero, se considera como propiedad intelectual de la empresa.
- Los datos personales y sensibles provenientes de las personas naturales que AMSAC adquiera y maneje, deben contar con un nivel de protección de seguridad apropiada que asegure la debida confidencialidad y/o privacidad, de conformidad con la legislación vigente.
- Implementar los controles de protección de los datos personales almacenados en las bases de datos o que se transmiten electrónicamente, según lo establecido en la Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales.
- Utilizar controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, la transmisión de información clasificada y/o el resguardo de información relevante en atención a los resultados de la evaluación de riesgos realizada por AMSAC.

2.4.13 Disposiciones de seguridad de la información a los trabajadores

El Departamento de TIC coordina con la Oficina de Gestión Humana para asegurar que se establezcan las siguientes medidas de seguridad de la información a los trabajadores:

- Realizar una verificación de antecedentes y competencias en seguridad antes de la contratación de personal.
- Evaluar a los candidatos mediante pruebas técnicas y entrevistas que aborden temas de seguridad de la información, siempre que esté acorde a las funciones y perfil del puesto.
- Exigir la firma de acuerdos de confidencialidad y compromisos éticos en el manejo de la información.
- Realizar capacitación periódica al personal de AMSAC sobre vulnerabilidades, amenazas, importancia de la ejecución de controles de seguridad y mejores prácticas de seguridad de la información.
- Efectuar sensibilización al personal de AMSAC sobre gestión de incidentes y simulacros de incidentes para reforzar las acciones de respuesta.

2.4.14 Disposiciones de respuesta ante la detección de delitos informáticos

El Departamento de TIC establece las siguientes medidas para minimizar impactos ante la ocurrencia de delitos informáticos:

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- Realizar una detección temprana mediante la implementación de herramientas de monitoreo y detección de actividades sospechosas en sistemas y redes.
- Todo incidente debe ser reportado de forma inmediata al Oficial de Seguridad y Confianza Digital.
- Se tomarán medidas inmediatas para contener el impacto, como la desconexión de equipos comprometidos o la revocación de accesos.
- Realizar análisis técnicos para identificar el alcance del delito y aplicar medidas de mitigación.
- En caso de que el incidente tenga implicaciones legales, se informará a las autoridades correspondientes.
- Aplicar lecciones aprendidas para fortalecer la ciberseguridad de la organización.

2.4.15 Disposiciones sobre cese de personal

El Departamento de TIC coordina con la Oficina de Gestión Humana para asegurar que, al finalizar la relación laboral con el personal o al cambiar de puesto, se realicen las siguientes acciones:

- Se revoquen inmediatamente los accesos y se recuperen todos los activos asignados.
- Se documente y supervise el proceso de desvinculación de manera que no queden brechas de seguridad.

2.4.16 Disposiciones para el trabajo no presencial

El Departamento de TIC, cuando se requiera, dispondrá los mecanismos que faciliten el trabajo no presencial, remoto o teletrabajo, para la ejecución de labores de los trabajadores de la empresa de forma externa, teniendo acceso a los sistemas e información empresarial. Para el trabajo no presencial, se debe considerar lo siguiente:

- Difundir disposiciones para que el trabajo no presencial se efectúe de forma adecuada, de tal manera que los trabajadores de la empresa consideren su importancia.
- Asegurar que los trabajadores que realicen trabajo no presencial lo efectúen desde una zona segura, verificando la seguridad física de la zona y llevando a cabo un chequeo de las condiciones adecuadas.
- Asegurar que la conexión remota hacia los sistemas internos de la empresa sea realizada siempre a través de una VPN que incluya un usuario y contraseña.
- Ejecutar el almacenamiento de la información en los sistemas internos de la empresa como SharePoint, OneDrive u otros que autorice AMSAC.
- Asegurar que todo dispositivo móvil de AMSAC para el teletrabajo debe contar con una aplicación para prevenir el software malicioso (malware).
- Asegurar que los trabajadores que realicen trabajo no presencial no cuenten con privilegios de administrador en el uso de dispositivos móviles o equipos de cómputo.
- Concientizar a los trabajadores que realicen trabajo no presencial que no debe brindar sus credenciales de acceso ni los dispositivos asignados a otras personas (familiares, amigos u otro usuario externo).

Se deberá realizar el proceso de auditorías periódicas para verificar el cumplimiento de estas disposiciones.

2.4.17 Disposiciones para la seguridad física y del ambiente

El Departamento de TIC establece las siguientes disposiciones para la seguridad física y del ambiente:

- Adoptar medidas de identificación y videovigilancia en las áreas sensibles.
- Llevar el registro de entradas y salidas, limitando el acceso solo a personal autorizado.
- Asegurar que todos los dispositivos, equipos y medios de almacenamiento se encuentren en zonas protegidas contra robos, daños o accesos no autorizados.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- Establecer un procedimiento para la eliminación segura o reutilización de equipos, garantizando que la información se borre de forma irreversible antes de su disposición final.

Evaluación periódica de riesgos físicos asociados a la ubicación de equipos

El Departamento de TIC, en coordinación con las áreas responsables de infraestructura y servicios generales, seguridad, salud ocupacional y medio ambiente, cuando corresponda, realizará una evaluación de riesgos físicos asociados a la ubicación de los equipos críticos de procesamiento de información, comunicaciones, almacenamiento y respaldo, por lo menos una vez al año.

Dicha evaluación deberá considerar, entre otros aspectos:

- Riesgos de acceso físico no autorizado.
- Riesgos de robo, vandalismo o sabotaje.
- Riesgos asociados a incendios, inundaciones, filtraciones de agua, humedad y polvo.
- Riesgos derivados de fallas eléctricas, variaciones de voltaje o interrupciones prolongadas del suministro eléctrico.
- Riesgos ambientales que puedan afectar la disponibilidad, integridad o funcionamiento de los equipos.
- Cambios en la infraestructura, distribución física o condiciones del entorno donde se encuentren ubicados los activos.

Los resultados de la evaluación deberán documentarse, mantenerse como evidencia del SGSI y generar las acciones de tratamiento correspondientes cuando se identifiquen riesgos que excedan los niveles aceptables establecidos por AMSAC.

2.4.18 Disposiciones para la gestión de la videovigilancia

AMSAC establece las siguientes disposiciones para la gestión de la videovigilancia:

- La videovigilancia se utilizará exclusivamente para la seguridad de las instalaciones, protección de bienes y prevención de incidentes.
- Se informará a los trabajadores y visitantes sobre la existencia de cámaras mediante señalización visible.
- Solo se captarán imágenes en áreas necesarias y se evitará la grabación de espacios privados.
- Los registros de videovigilancia serán almacenados en servidores seguros con acceso restringido.
- Solo el personal autorizado podrá acceder a las imágenes, conforme a los procedimientos internos de seguridad.
- Las grabaciones solo podrán ser utilizadas para investigaciones internas, cumplimiento normativo o por solicitud de autoridades competentes.
- Queda prohibida la difusión o uso indebido de las imágenes con fines distintos a los establecidos en esta política.

2.4.19 Disposiciones de escritorio limpio

El Departamento de TIC coordina con las gerencias y jefaturas para asegurar que se ejecuten las siguientes disposiciones de escritorio limpio.

- Todos los colaboradores deben mantener sus áreas de trabajo libres de documentos o notas que contengan información sensible.
- Al finalizar la jornada o al ausentarse, deben guardar o eliminar adecuadamente la información visible, especialmente cuando los trabajadores estén ubicados cerca de zonas de atención o acceso al público.
- Utilizar protectores de pantalla y bloquear las sesiones de trabajo de manera automática.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- Retirar todos los documentos con información confidencial del escritorio de trabajo y ubicarlos en cajones, armarios asegurados con llaves; incluye los dispositivos de almacenamiento masivo con información confidencial, como CD, DVD y unidades USB.

2.4.20 Disposiciones para la seguridad en el desplazamiento de los equipos TI

El Departamento de TIC establece las siguientes disposiciones para la seguridad en el desplazamiento de los equipos TI:

- No se debe realizar el retiro de los equipos de cómputo y accesorios tecnológicos asignados de las instalaciones de AMSAC, sin contar autorización previa correspondiente.
- Todo traslado de equipos de cómputo y accesorios tecnológicos deberá registrarse en los controles establecidos por AMSAC, consignando como mínimo el responsable, destino y motivo del traslado.
- Los equipos de cómputo asignados a practicantes, así como aquellos entregados bajo la modalidad de préstamo, asignación temporal, reemplazo por mantenimiento o cualquier otra forma de cesión de uso, deberán permanecer en el área, oficina, sede o base operativa para la cual fueron autorizados y no podrán ser retirados para fines personales ni ajenos a las funciones encomendadas. Su retiro o traslado fuera de dicha ubicación requerirá la autorización previa del responsable de la base o del jefe del área usuaria correspondiente, así como el visto bueno del Jefe del Departamento de Tecnologías de la Información y Comunicaciones (DTIC). Toda autorización deberá registrarse conforme a los mecanismos de control de activos establecidos por AMSAC.
- Queda prohibida la transferencia, préstamo, intercambio o reasignación de equipos de cómputo y accesorios tecnológicos entre usuarios, áreas, sedes o bases operativas sin la autorización previa del Departamento de Tecnologías de la Información y Comunicaciones (DTIC) y el registro correspondiente en los controles institucionales de activos.
- Se deben aplicar medidas de seguridad como cifrado de información y respaldo previo antes del desplazamiento.
- Durante los desplazamientos entre sedes, bases operativas o ubicaciones externas, los usuarios deberán adoptar las medidas razonables de custodia necesarias para prevenir la pérdida, robo, daño o acceso no autorizado a los equipos e información institucional.
- En caso de comisión de servicios, trabajo remoto o actividades desarrolladas fuera de las instalaciones de AMSAC, el usuario continuará siendo responsable de la custodia, protección y uso adecuado de los equipos y accesorios tecnológicos asignados.
- Los equipos deberán transportarse en maletines, mochilas o estuches adecuados que permitan protegerlos contra daños físicos y deberán mantenerse bajo la custodia del personal responsable durante todo el desplazamiento.
- No se deberán dejar equipos de cómputo o accesorios tecnológicos sin supervisión en lugares públicos, medios de transporte, hoteles, aeropuertos, espacios compartidos o zonas que representen un riesgo para la seguridad física de los activos o de la información institucional.
- En caso de utilizar redes externas para el acceso a recursos o información institucional, se deberán emplear los mecanismos de acceso seguro autorizados por el Departamento de TIC, evitando el uso de redes públicas o conexiones que no garanticen condiciones adecuadas de seguridad.
- Los equipos deberán mantenerse protegidos mediante los mecanismos de autenticación y bloqueo definidos por el Departamento de TIC. Adicionalmente, cuando las condiciones operativas lo requieran, se deberán implementar medidas razonables de protección física para prevenir la pérdida, robo o acceso no autorizado a los equipos.
- En caso de pérdida, robo, extravío o daño de un equipo de cómputo o accesorio tecnológico durante su desplazamiento o uso, el usuario responsable deberá comunicar el hecho de forma inmediata al Departamento de TIC, al Oficial de Seguridad y Confianza Digital y a las áreas competentes, a fin de adoptar las acciones de control y atención correspondientes.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

•

2.4.21 Disposiciones de uso de dispositivos móviles y medios de almacenamiento

El Departamento de TIC establece las siguientes disposiciones para el uso de dispositivos móviles y medios de almacenamiento que:

- Solo los dispositivos autorizados podrán conectarse a la red corporativa o almacenar información de la organización.
- Todo dispositivo que almacene información sensible debe contar con cifrado y medidas de protección adecuadas.
- Se deben emplear contraseñas robustas, autenticación de doble factor en dispositivos móviles.
- No se debe almacenar información sensible en dispositivos personales o medios no autorizados.
- Se debe utilizar VPN y evitar conexiones a redes Wi-Fi públicas o no seguras.
- No se permite la instalación de software no autorizado en dispositivos corporativos.
- En caso de extravío, se debe notificar de inmediato al Departamento de TI para la desactivación o bloqueo remoto del equipo.
- Antes de conectar cualquier dispositivo externo, se debe realizar un escaneo antivirus.
- La información debe eliminarse de los dispositivos extraíbles una vez utilizada y no debe almacenarse permanentemente.

2.4.22 Disposiciones de buen uso de activos

El Departamento de TIC establece las siguientes disposiciones para el uso adecuado, seguro y responsable de los activos:

- Los activos de la organización deben utilizarse únicamente para fines laborales y no para actividades personales o no autorizadas.
- Cada usuario es responsable de la conservación y correcto uso de los activos asignados, evitando negligencias o daños por mal uso.
- Se deben aplicar medidas de seguridad física y digital para evitar el deterioro, robo o acceso no autorizado a los activos.
- Todo activo debe estar identificado en un inventario, y su asignación o traslado debe ser registrado y autorizado.
- Los accesos a sistemas y plataformas deben ser personales e intransferibles, manteniendo la confidencialidad de las credenciales.
- La información debe resguardarse en servidores o nubes corporativas y no en dispositivos personales o externos sin autorización.
- Todo activo de información debe ser clasificado y etiquetado conforme al nivel de sensibilidad, criticidad y uso, siguiendo lo establecido en el Procedimiento S3.3.P2 "Clasificación, Etiquetado y Uso de Activos de Información".
- El etiquetado de activos de información es obligatorio para todo el personal que administre, procese o almacene información institucional, incluyendo personal interno y externo, con el fin de garantizar la protección adecuada de los activos de información.
- La clasificación deberá realizarse al momento de la creación o incorporación del activo al entorno de AMSAC, y su etiquetado deberá reflejar claramente el nivel de protección requerido.

2.4.23 Disposiciones de seguridad de información antimalware

El Departamento de TIC debe ejecutar las siguientes disposiciones de seguridad de información antimalware:

- Implementar controles para la detección, prevención y recuperación ante afectaciones de malware.
- Mantener instalados y actualizados los sistemas de protección antivirus en cada equipo de cómputo, así como en las conexiones de la red interna.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

2.4.24 Disposiciones de gestión de amenazas, vulnerabilidades y riesgos

El Departamento de TIC establece las siguientes disposiciones para la gestión de amenazas, vulnerabilidades y riesgos:

- Gestionar la ejecución de análisis de vulnerabilidades técnicas a los sistemas de información y la infraestructura tecnológica más relevante de AMSAC, a fin de adoptar las acciones necesarias para prevenir o mitigar los riesgos identificados en el análisis.
- Exigir a los proveedores de equipamiento, sistemas de información y sus componentes, que comuniquen las vulnerabilidades de los productos ofrecidos, así como los controles aplicables para su mitigación.
- El Departamento de TIC planifica y ejecuta pruebas de penetración y detección de vulnerabilidades a ser realizadas por personal especializado, considerando los riesgos que pueden comprometer la seguridad de los sistemas informáticos de la empresa.

2.4.25 Disposiciones de cambios de configuración de equipos

El Departamento de TIC establece las siguientes disposiciones para los cambios de configuración de equipos:

- Definir e implementar procesos y herramientas para hacer cumplir las configuraciones definidas para los equipos durante su vida útil.
- Definir roles, responsabilidades y procedimientos para garantizar un control satisfactorio de todos los cambios de configuración en equipos.
- Mantener registros de todos los cambios en la configuración de equipos y almacenarlos de forma segura en plantillas de configuración.
- El Departamento de TIC establecerá y mantendrá una Línea Base de Configuración Segura aplicable a estaciones de trabajo y equipos portátiles institucionales.
- Todos los equipos corporativos deberán incorporarse al servicio de gestión centralizada Microsoft Intune y cumplir las políticas de seguridad definidas por AMSAC.
- Los usuarios finales no deberán contar con privilegios de administrador local, salvo autorización expresa y temporal aprobada por el Departamento de TIC.
- El firewall del sistema operativo deberá permanecer habilitado en todo momento.
- La protección antimalware deberá permanecer instalada, habilitada y actualizada.
- El cifrado de disco mediante BitLocker será obligatorio en equipos portátiles y en aquellos equipos que procesen o almacenen información clasificada como Interna, Restringida o Confidencial.
- El bloqueo automático de sesión deberá activarse tras un período máximo de 5 minutos de inactividad.
- Las actualizaciones de seguridad del sistema operativo y aplicaciones deberán gestionarse de forma centralizada mediante las herramientas autorizadas por AMSAC.
- Los puertos USB permanecerán restringidos conforme a las políticas de seguridad vigentes y sólo podrán habilitarse mediante autorización formal.
- Los equipos deberán cumplir las políticas de acceso condicional, autenticación multifactor y acceso remoto seguro definidas por AMSAC.
- Se restringirá la instalación de software no autorizado por el Departamento de TIC.
- El Departamento de TIC realizará verificaciones periódicas del cumplimiento de la Línea Base de Configuración Segura y gestionará las desviaciones identificadas.
- Las configuraciones mínimas de seguridad aplicables a estaciones de trabajo y equipos portátiles institucionales se encuentran definidas en el Lineamiento de Configuración Segura y Hardening de Equipos de Usuario Final administrado por el Departamento de TIC.

2.4.26 Disposiciones sobre el uso y gestión de controles criptográficos

El Departamento de TIC deberá implementar y administrar controles criptográficos para proteger la confidencialidad, integridad, autenticidad y, cuando corresponda, el no repudio de la información de AMSAC. Para ello deberá:

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- Implementar mecanismos de cifrado para proteger la información institucional almacenada o transmitida a través de redes y servicios tecnológicos.
- Utilizar protocolos y mecanismos criptográficos seguros en servicios publicados, conexiones remotas, VPN y demás canales de comunicación institucional.
- Utilizar certificados digitales emitidos por entidades o mecanismos de certificación autorizados para los servicios que requieran autenticación o cifrado.
- Restringir el acceso a certificados digitales, llaves criptográficas y demás material criptográfico exclusivamente al personal autorizado.
- Gestionar el ciclo de vida de certificados digitales y llaves criptográficas conforme a lo establecido en el Procedimiento S3.2.P4 "Procedimiento de Cifrado de Seguridad Informática".
- Realizar revisiones periódicas sobre la vigencia, protección y uso de los certificados digitales y llaves criptográficas administrados por AMSAC.

2.4.27 Disposiciones para el desarrollo seguro

El Departamento de TIC estandariza el ciclo de vida del desarrollo del software, a fin de:

- Definir actividades a llevarse a cabo en un proyecto de desarrollo de software.
- Unificar criterios para el desarrollo de software.
- Proporcionar puntos de control y revisión.

2.4.28 Disposiciones de entorno seguro de desarrollo, prueba y producción

El Departamento de TIC establece los siguientes controles y buenas prácticas para garantizar la seguridad en los entornos de desarrollo, prueba y producción:

- Los entornos de desarrollo, prueba y producción deben estar completamente aislados para evitar interferencias y riesgos de seguridad.
- Solo el personal autorizado podrá acceder a cada entorno según su rol y función específica.
- Se prohíbe el uso de datos reales en entornos de desarrollo y prueba sin anonimización.
- Toda modificación debe pasar por procesos de validación y aprobación antes de llegar a producción.

2.4.29 Disposiciones para la gestión de cambio

El Departamento de TIC debe documentar y controlar la configuración de sistemas y aplicaciones. Además, cualquier cambio en los sistemas y aplicaciones debe:

- Ser evaluado y autorizado formalmente.
- Ser registrado para garantizar la trazabilidad y la continuidad del servicio.

2.4.30 Disposiciones sobre programas de utilidad privilegiados.

El Departamento de TIC establece las siguientes disposiciones sobre los programas de utilidad privilegiados:

- El uso de programas de utilidad privilegiados que puedan modificar configuraciones del sistema, eludir controles de seguridad, capturar información, administrar equipos remotamente o realizar actividades de diagnóstico avanzado estará estrictamente restringido al personal autorizado.
- El Departamento de TIC mantendrá una relación actualizada de herramientas autorizadas y prohibidas.
- Se implementarán mecanismos automáticos para detectar y generar alertas sobre la instalación, ejecución o uso de utilidades privilegiadas no autorizadas.
- Todas las alertas generadas serán registradas, evaluadas y tratadas conforme al Procedimiento de Gestión de Incidentes de Seguridad de la Información.

	Directiva para el Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones Directiva	Código: S3.1.DR1 Versión: 05 Fecha: 06/10/2026
---	--	---

- El incumplimiento de estas disposiciones será considerado una infracción a las políticas de seguridad de la información de AMSAC.

3. ALCANCES FUNCIONALES

3.1 Gerente de Administración y Finanzas

- Aprobar la presente directiva.

3.2 Jefe del Departamento de Tecnología de la Información y Comunicaciones

- Conducir la directiva de uso de servicios y recursos de TIC, cumpliendo los plazos y las disposiciones previstas en los lineamientos de FONAFE, la norma ISO 27001, la normativa legal aplicable y el presente documento.
- Velar por el cumplimiento de la presente directiva.
- Velar porque la directiva se mantenga vigente, siendo responsable de realizar revisiones y actualizaciones periódicas, así como de su difusión.

3.3 Personal del Departamento de TIC

- Elaborar los procedimientos técnicos necesarios para garantizar un óptimo uso y control de los servicios y recursos TIC en AMSAC, como gestión de respaldo y recuperación, gestión de accesos, entre otros.
- Garantizar el desempeño, disponibilidad y seguridad informática en cada uno de los servicios y recursos TIC, brindando soporte técnico oportuno a los usuarios.
- Instalar los componentes de los servicios y recursos TIC en todas las áreas usuarias, tanto en la sede principal como en las bases en provincia de AMSAC.
- Actualizar y monitorear permanentemente los programas y dispositivos de seguridad (antivirus, cortafuegos, etc.).
- Verificar el registro de los eventos de auditoría y controles de seguridad en cada uno de los servicios y recursos TIC.
- Informar a la Jefatura del Departamento de TIC respecto a los siguientes aspectos:
 - Cumplimiento de la normativa aplicable sobre TIC.
 - Gestión de los proyectos TIC
 - Gestión de usuarios y sus credenciales.
 - Sensibilización al personal acerca del buen uso de las TIC y seguridad de la información.

3.4 Personal de AMSAC

- En calidad de usuarios de los servicios de tecnologías de la información y recursos de AMSAC, es responsable de cumplir las disposiciones establecidas en la presente directiva.

4. REGISTROS / ANEXOS

- Formato S3.2.P2.F1 Solicitud de Alta/Baja de Usuario o Cambio de perfil.
- Formato S3.2.P2.F2 Solicitud de Uso de Aplicaciones.
- Formato S3.2.P2.F3 Exoneración de restricción de TIC.
- Formato S3.2.P2.F5 Matriz de Perfiles de Usuario de Recursos TIC.
- Formato S3.2.P2.F6 Registro de Accesos Privilegiados.