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

Versión	Fecha	Control de Cambios
04	17/11/2025	• Numerales V.1 y 2.4. Se incorporaron definiciones y disposiciones específicas necesarias para la implementación del Sistema de Gestión de Seguridad de la información según la norma ISO 27001. • Numerales 2.2.2 y 2.3.5. Se actualizaron disposiciones del servicio de Intranet y se establecieron condiciones de uso del almacenamiento, restricciones de acceso, así como criterios de publicación y mantenimiento de documentos. • Numeral 2.3.1.5. Se añadieron lineamientos para la publicación y gestión de tableros de inteligencia de negocio. • Numeral 2.3.3 Se incorporó la obligatoriedad del uso de la plataforma institucional de colaboración digital para la gestión de comunicaciones, reuniones virtuales y coordinación de actividades laborales.

Áreas Responsables	Nombres y Cargos
Elaborado: **Departamento de Tecnologías de la Información y Comunicaciones**	Moisés Palomino Jefe del 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

INDICE

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, plataforma institucional de colaboración digital 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 Nº 022-2022-INACAL/DN, que aprueban Normas Técnicas Peruanas:
  - NTP ISO/IEC 27001:2022 Sistema de Gestión de Seguridad de la Información – Requisitos.
  - NTP ISO/IEC 27002:2022 Controles de Seguridad de la Información.
- Norma ISO 9001:2015: Sistema de Gestión de la Calidad – Requisitos.
- Norma ISO 14001:2015: Sistema de Gestión Ambiental – Requisitos.
- Norma ISO 45001:2018: Sistema de Gestión de Seguridad y Salud en el Trabajo – Requisitos.
- Norma ISO 37001:2016: Sistema de Gestión Antisoborno – Requisitos.
- Norma ISO 27001:2022: Sistema de Gestión de Seguridad de la Información – Requisitos
- Norma ISO 27002:2022 Controles de Seguridad de la Información
- Norma ISO 27005:2022 Guías para la Gestión de Riesgos de Seguridad de la Información.
- Norma ISO 27035: 2022: 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 03 de fecha 19.jun.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.
- **Confidencialidad**: Propiedad de la información de no estar disponible o sea divulgada a quienes no poseen autorización.
- **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.
- **Plataforma de colaboración digital:** Herramienta institucional que permite la comunicación, coordinación y trabajo colaborativo entre los usuarios, mediante funciones de mensajería instantánea, videollamadas, intercambio de archivos y gestión de proyectos.

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

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/o legislación que corresponda.

2. El equipo y sus accesorios sólo pueden ser usados para fines institucionales y para apoyo de las actividades del trabajo del usuario. Los usuarios darán a las computadoras un uso cuidadoso y apropiado a sus fines, con el objeto de evitar su deterioro.

3. Solo el personal del Departamento de TIC o de empresas terceras debidamente autorizadas por el Departamento de TIC puede instalar, desconectar, mover 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. En caso de pérdida, deterioro o robo de los equipos asignados, aplicará lo señalado en la Directiva de "Normas para la Administración, Uso, Control, Cuidado y Custodia de los Bienes de Activos Mineros".

6. 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.

7. 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.

8. 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.

9. **Está prohibido:**
   - Almacenar la información de trabajo en cualquier dispositivo externo (USB, disco duro externo, CD RW, etc.) sin dejar copia idéntica en la nube o carpeta en red asignada al usuario.
   - Copiar información 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 distintos al trabajo.
   - Borrar 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.

10. 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.

11. La información generada en sus estaciones de trabajo es de propiedad de AMSAC, por lo cual éste se reserva el derecho de titularidad.

12. 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.

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.

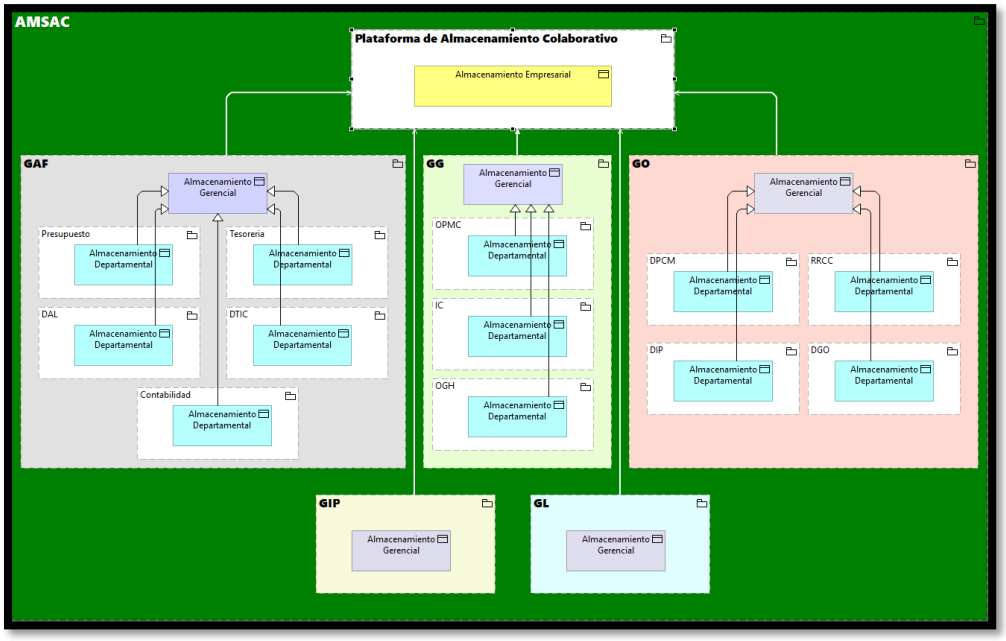

Figura 1: Arquitectura de Almacenamiento Colaborativo de AMSAC

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”.

- Está prohibido que los usuarios utilicen dispositivos de almacenamiento externo como medio habitual para realizar sus labores de trabajo. Estos dispositivos deben ser utilizados exclusivamente como medios temporales para el traslado de información, garantizando en todo momento que los datos se mantengan almacenados de forma segura en los repositorios oficiales de AMSAC.

- 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 éstos 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

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.
- **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 realiza auditorías del uso de software informático, siempre que la herramienta incluya dicha funcionalidad. Estas auditorías 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.

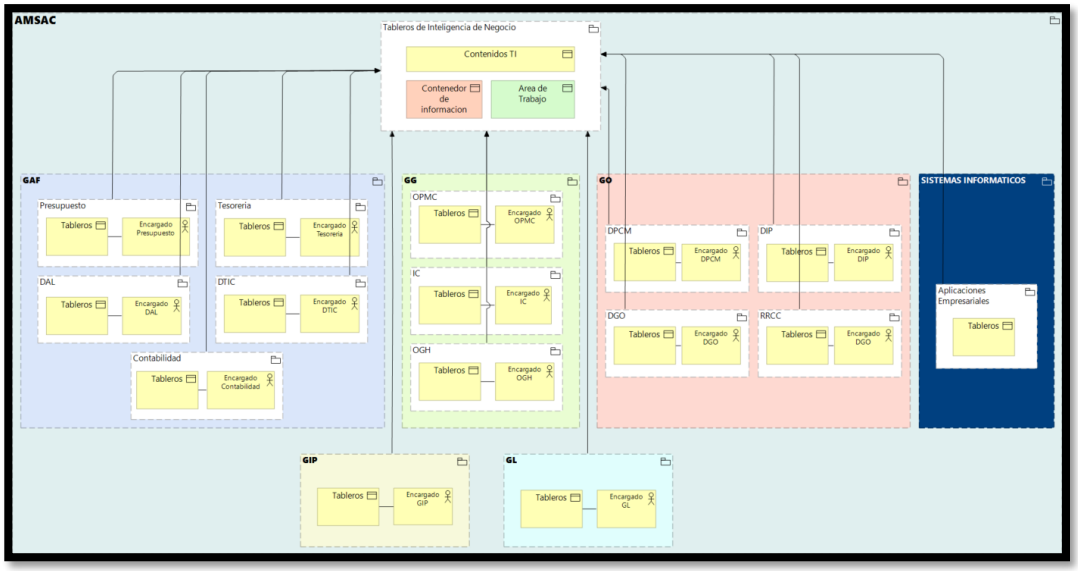

Figura 2: Arquitectura de Publicación de Tableros de Inteligencia de Negocio

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.

- **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 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 cambiar su contraseña y evitar su divulgación, cumpliendo con las normas que se definen acerca del manejo de contraseñas seguras. El tiempo de vida de las contraseñas será de 90 días de acuerdo con las disposiciones de TIC.

- 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.

- 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 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 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 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.

2.3.3 Uso de la plataforma institucional de colaboración digital

- El uso de la plataforma institucional de colaboración digital es obligatorio para todos los funcionarios y trabajadores de AMSAC, para la gestión de comunicaciones, reuniones virtuales y coordinación de actividades laborales.

- La plataforma debe emplearse para reuniones virtuales, mensajería instantánea, llamadas de voz y video, intercambio de archivos y colaboración en documentos institucionales.

- El Departamento de TIC es responsable de la administración, soporte técnico y capacitación sobre el uso de la plataforma institucional de colaboración digital.

- El acceso y uso de la plataforma se realizará conforme a los lineamientos de seguridad y confidencialidad establecidos en la presente directiva.

- El uso de la plataforma está limitado exclusivamente a fines laborales y actividades relacionadas con la empresa. Queda prohibido su uso para fines personales o ajenos a las funciones institucionales.

2.3.4 Servicio de Internet

- El acceso a internet debe ser solicitado al Departamento de TIC utilizando 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 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.

2.3.5 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.

2.3.6 Sitio web de la empresa

- 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.

2.3.7 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 el formato S3.02.04-F.02 “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.

2.3.8 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 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.

- 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.

2.3.9 Telefonía (fija y móvil)

- Se podrá solicitar el uso de telefonía fija utilizando 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.

2.3.10 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, 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 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.

2.4.2 Disposiciones de uso seguro de los servicios de red

El Departamento de TIC debe asegurar que los servicios de red deben:

- Mantener activos y en operación los firewalls que protegen las redes.
- Contar con una DMZ para proteger la red del área local contra el tráfico no confiable.
- Detectar y proteger la red de datos que pueda ser vulnerada por malware (virus, hackers) o accesos no autorizados.
- No permitir la conectividad de equipos móviles y/o de cómputo personales a la red de datos de AMSAC, ya que al estar contaminados podrían propagar un ataque de malware.
- Verificar que los usuarios que se conecten a la red interna de AMSAC desde redes no confiables tales como internet, teléfono, etc., deben cumplir con las políticas y controles de seguridad establecidos para estas conexiones, a fin de mantener y preservar la integridad, confidencialidad de la información.

2.4.3 Disposiciones de uso de los servicios en la nube

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.

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.

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 procesamientos 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.

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 8 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 5 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.

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.

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.

- 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:

- 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 del 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.

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

2.4.18 Disposiciones para la gestión de la videovigilancia

El Departamento de TIC 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.
- 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 a las instalaciones de AMSAC, sin contar autorización previa.
- Todo equipo trasladado deberá registrarse en un control de salida, indicando responsable, destino y motivo del traslado.
- Se deben aplicar medidas de seguridad como cifrado de información y respaldo previo antes del desplazamiento.
- Los equipos deben transportarse en mochilas o estuches adecuados para evitar daños físicos y mantenerse siempre bajo custodia del personal responsable.
- No se debe dejar equipos sin supervisión en lugares públicos, transportes compartidos o áreas de alto riesgo.
- En caso de utilizar redes externas, se debe emplear VPN y evitar conexiones abiertas o públicas.
- Los equipos deben mantenerse bloqueados con contraseñas y, en caso de laptops, utilizar sistemas de seguridad como cables antirrobo cuando sea necesario.

- En caso de pérdida, robo o daño del equipo, se debe notificar inmediatamente al Oficial de Seguridad y Confianza Digital.

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.

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.

2.4.26 Disposiciones sobre el uso de controles criptográficos

El Departamento de TIC establece las siguientes disposiciones para el uso de controles criptográficos:

- Implementar controles criptográficos para el acceso a los sistemas de información.
- Desarrollar e implantar mecanismos para el uso de controles criptográficos para la protección de información con el objetivo de salvaguardar la confidencialidad, integridad, no repudio y autenticación.
- Toda información a ser transportada en medios de respaldo debe ser cifrada.
- Gestionar las claves criptográficas y la recuperación de información cifrada para los casos de claves perdidas, comprometidas o dañadas.

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.

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 (antes S3.02.04-F.01) Solicitud de Alta/Baja de Usuario o Cambio de perfil.
- Formato S3.02.04-F.02 Solicitud de Uso de Aplicaciones.
- Formato S3.2.P2.F2 Formato de Matriz de Perfiles de Usuario de Recursos TIC.
- Formato S3.2.P2.F3 Exoneración de restricción de TIC.