SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001

24 de Julio de 2025

TABLA DE CONTENIDO

1. INTRODUCCION

FORVIS MAZARS adopta las políticas necesarias para la protección de la información preservando con calidad, confiabilidad, privacidad, integridad, disponibilidad, y confidencialidad, buscando concientizar a todos los funcionarios de la firma de la importancia del cumplimiento de las normas establecidas y que se aplica a todos los recursos y servicios informáticos existentes en la compañía.

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (Tics) en las entidades antes nombradas.

Propósito de la Organización: FORVIS MAZARS se enfoca en ayudar a las empresas a estructurarse de manera eficiente para maximizar su talento y recursos. Su propósito es apoyar a las organizaciones en el diseño de estructuras alineadas con sus estrategias y objetivos comerciales, asegurando que puedan adaptarse a los cambios y alcanzar el éxito.

Los compromisos de seguridad de la información de FORVIS MAZARS están directamente alineados con su propósito organizacional de ayudar a las empresas a estructurarse de manera eficiente y maximizar su talento y recursos. Se relacionan de la siguiente manera:

- **Protección de datos y confianza**: Al garantizar altos estándares de seguridad de la información, FORVIS MAZARS protege los datos de sus clientes y asociados, lo que refuerza la confianza en la estructura organizativa que diseña.

- **Gestión de riesgos**: La seguridad de la información permite minimizar riesgos operativos y estratégicos, asegurando que las organizaciones puedan adaptarse de manera segura a los cambios y alcanzar sus objetivos comerciales sin vulnerabilidades críticas.

- **Cumplimiento normativo**: El compromiso con la seguridad de la información también incluye el cumplimiento de normativas y regulaciones vigentes, lo que ayuda a las empresas a mantenerse alineadas con los estándares legales y de mercado.

- **Resiliencia y continuidad del negocio**: Al implementar buenas prácticas de seguridad, las organizaciones asesoradas por FORVIS MAZARS pueden garantizar la continuidad de sus operaciones y proteger sus activos digitales ante amenazas o incidentes.

1. OBJETIVO

Crear directrices que orienten a los usuarios empleados y contratistas de las entidades de **FORVIS MAZARS,** para un uso responsable de los diferentes recursos y servicios informáticos y de telecomunicaciones.

2. ALCANCE

Aplica a todos los usuarios que hagan uso de recursos y servicios informáticos y de Telecomunicaciones de la infraestructura de **FORVIS MAZARS.**

2.1 Principios Generales

- Las políticas de seguridad de la información se basan en proteger y resguardar tanto la información generada por FORVIS MAZARS como los recursos y servicios.
- El personal que tenga un vínculo laboral o contractual con FORVIS MAZARS, debe recibir en su proceso de inducción y reinducción la política de seguridad de la información.
- El personal que tenga un vínculo laboral o contractual con FORVIS MAZARS., debe aceptar las condiciones de confidencialidad y de uso adecuado de los bienes informáticos y de la información.
- Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencialidad de FORVIS MAZARS, o el que se le declare culpable de un delito informático.
- Los usuarios deben hacer buen uso de los recursos compartidos.

Los Objetivos de Seguridad de Información establecidos por la compañía son:

ID Objetivo	Nombre	Lo que se hará	Valor Esperado
MAZ.OBJ.01	Garantizar la disponibilidad de los sistemas críticos	Monitoreo continuo y redundancia de sistemas	90%
MAZ.OBJ.02	Capacitar al personal en seguridad	Realizar campañas de concienciación y cursos	70%

MAZ.OBJ.03	Mantener ISO27001 vigente	Revisar y aplicar políticas y controles conforme a lo estipulado en el SGSI	100%
MAZ.OBJ.04	Revisión de los tiempos y puntos de recuperación establecidos para DRP	Evaluar anualmente los tiempos y puntos objetivos de recuperación de los servicios criticos de negocio para identificar desviaciones y mantener actualizados dichos objetivos	>95%

Se encuentran establecidos en el documento MAZ-CO-SGSI-PRO4-1.0 Plan de Objetivos de Mejora Anual

2.2 Marco Normativo

El marco normativo aplicable a FORVIS MAZARS en asuntos relacionados con Seguridad de la Información y el cual es la base de la implementación del Sistema de Gestión de Seguridad de la Información se presenta a continuación:

- Ley 1581 de 2012: Habeas Data y Protección de datos personales.
- Ley 1273 de 2009: Delitos Informáticos.
- Ley 23 de 1993 y Ley 44 de 1993: Derechos de autor.
- Ley 679 de 2001 y Ley 1336 de 2009: Pornografía Infantil.
- Ley 1581 de 2012: Protección de datos personales.
- Ley 527 de 1999: Bases de datos, comercio electrónico y firmas digitales.
- Ley 1341 de 2009: Tecnologías de la Información y aplicación de seguridad
- ISO 27001 versión 2022

3. Relación compromiso política seguridad de información y objetivos de seguridad de información

3.1 Política de Usuario

Es fundamental para el correcto desarrollo de las actividades de FORVIS MAZARS que se cumpla con las siguientes normas para garantizar el correcto desempeño en las funciones diarias de cada usuario.

- Todo nuevo usuario que ingrese a FORVIS MAZARS. debe ser reportado por el gerente/jefe/líder de recursos humanos y jefe del área correspondiente al área de Tecnología Informática y Comunicaciones para la creación del correspondiente usuario de red, asignación de permisos informáticos, espacio de almacenamiento en red y asignación de equipo de cómputo del cual se hará responsable sobre su uso y cuidado.
- El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones de los colaboradores o servidores de FORVIS MAZARS.
- En el caso de retiro de un colaborar, este retiro debe ser reportado por el gerente/jefe/líder de recursos humanos y jefe del área correspondiente al área de Tecnología Informática y Comunicaciones para quitar todos los permisos informáticos; adicional el usuario debe entregar los usuarios, claves y equipo asignado por el área de Tecnología Informática y Comunicaciones en correcto estado y funcionamiento.
- Es responsabilidad de los colaboradores que usan los servicios prestados por el área de Tecnología Informática y Comunicaciones cumplir las Políticas y Estándares de Seguridad Informática plasmados en este documento.
- Todo funcionario de FORVIS MAZARS, debe usar claves complejas que contengan letras mayúsculas, letras minúsculas, números y caracteres especiales, para los sistemas de información de FORVIS MAZARS.
- Toda vez que un funcionario se ausente de su puesto debe dejar la estación de trabajo bloqueada para evitar daño, manejo inadecuado del equipo o pérdida de la información.
- En cualquier caso, el usuario a cargo del equipo informático y/o de telecomunicaciones se hará responsable por las medidas disciplinarias y legales que con lleve el no cumplimiento de las Políticas establecidas en este documento.
- La creación de Cuentas de usuarios, se realizarán con previa autorización o solicitud del Subgerente y/o Gerente General, adicionalmente deberá ser enviado el Contrato debidamente legalizado por parte del área Jurídica, este procedimiento aplica para adiciones y/o prorrogas.

- Sera deber del área de Tecnología Informática y Comunicaciones entregar el equipo al usuario cifrado con BitLocker, la clave de desbloqueo de BitLocker será enviada al correo electrónico del usuario y la clave de recuperación de BitLocker será resguarda en un sitio seguro por el área de Tecnología Informática y Comunicaciones.
- Los usuarios que no tengan contrato vigente, automáticamente se restringirá el ingreso al sistema, en el caso que se le renueve el contrato, el área Jurídica enviara un correo al personal encargado del área tecnológica con copia al supervisor Subgerente Técnico y/o Subgerente Administrativo, indicando la vigencia y el área de funcionamiento.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Los usuarios deberán enviar una solicitud por medio de la herramienta GLPI (mesa de ayuda o helpdesk) en la medida que requieran Soporte Técnico o Asesoría en uso de herramientas Tecnológicas o fallas en el sistema tanto de Hardware como de Software.
- El encargado del área de Tecnología Informática y Comunicaciones es el único responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los colaboradores de FORVIS MAZARS.
- Están contemplados como faltas muy graves y se prohíben los siguientes comportamientos del personal de FORVIS MAZARS., utilizando los medios de la compañía, medios propios, o recursos en comisión de terceros y clientes:
    - Obtener acceso informático abusivo a sistemas protegidos o no con sistemas de seguridad.
    - Obstaculizar sistemas informáticos y de telecomunicaciones.
    - Interceptación de datos informáticos sin autorización de emisor y/o receptor
    - Causar daños y sabotaje informático.
    - Uso de software malicioso.
    - Violación de datos personales.
    - Suplantar identidad en redes sociales, plataformas tecnológicas, o páginas web.
    - Extorsión, hurto o transferencia indebida de activos o amenaza usando medios tecnológicos.

3.2 Política de administración de perfiles y contraseñas

Para el correcto inicio de sesión en cualquiera de las plataformas de FORVIS MAZARS, es necesario garantizar la seguridad informática de la siguiente manera:

- Todo colaborador debe poseer un nombre de usuario con contraseña para tener acceso a los recursos informáticos prestados por el área de Tecnología Informática y Comunicaciones y es el único responsable por las actividades que sean realizados por ese nombre de usuario.
- Las cuentas de los usuarios deben ser configuradas para que exijan cambio de contraseña cada 60 días con el objetivo de garantizar mayor seguridad en el uso de los recursos y accesos a información con diferentes niveles de confidencialidad.
  Nota: De acuerdo con las mejores prácticas de gestión de cuentas de usuarios, no es recomendable que se superen los 60 días de vencimiento para exigir el cambio de la contraseña.
- Las contraseñas no pueden contener el valor samAccountName (Nombre de cuenta) del usuario o el valor displayName completo (valor Nombre completo del usuario). Ambas comprobaciones no distinguen mayúsculas de minúsculas.
- Toda nueva contraseña establecida por los usuarios debe cumplir los siguientes requisitos:
  - Longitud mínima: 12 caracteres
  - Requisitos de complejidad: Mayúsculas de los idiomas europeos (de A a la Z con marcas diacríticas, griego y caracteres cirílicos), Minúsculas de los idiomas europeos (de a a la a, s nítidass, marcas diacríticas, griego y caracteres cirílico), Dígitos de base 10 (del 0 al 9), Caracteres no alfanuméricos (caracteres especiales) (¡por ejemplo, !, $, #, %), Cualquier carácter Unicode que se clasifica como carácter alfabético, pero que no está en mayúsculas o minúsculas. Esto incluye caracteres Unicode de idiomas de Asia.

  Ejemplo: Murc13l@g0/+!-(Correcta) – Murcielago1234 (incorrecta)

- En caso de que se olvide la contraseña o que se bloquee la cuenta de usuario, el funcionario podrá solicitar al área de Tecnología Informática y Comunicaciones el restablecimiento de esta a través de GLPI (mesa de ayuda o helpdesk), correo electrónico o de forma escrita.
- Los usuarios no deben construir palabras clave que sean idénticas o similares a palabras claves utilizadas anteriormente.
- Las palabras clave no se deben mostrarse en pantallas o en documentos impresos. Esto con el fin de evitar que personas no autorizadas las conozcan y puedan usar los sistemas de forma no autorizada.
- Las palabras clave no se deben almacenar en forma legible en archivos batch, log-in automáticos, software de macros, terminales, computadores sin controles de acceso o en otros sitios en donde personas no autorizadas puedan conocerlas.
- Las claves suministradas al usuario (acceso a la red, impresión, telefonía, Red Inalámbrica, sistema de información, entre otras) deben ser para uso personal e intransferible, evitando de

esta manera accesos no autorizados que puedan ocasionar incidentes en la seguridad informática.

- Las palabras clave emitidas por cualquier sistema o plataforma tecnológica deben ser validadas únicamente en la primera conexión del usuario. Es en este momento en el cual el usuario debe cambiar la palabra clave antes de realizar cualquier otra actividad.
- El cambio de clave de Helisa NIIF y Recurso Humano 4, se realizará cada 15 días de forma programada, o tras previa solicitud de los usuarios por GLPI (mesa de ayuda o helpdesk).
- El cambio de clave de accesos a servidores y demás, se realizará cada 10 días de forma programada, o tras previa solicitud de los usuarios por correo electrónico a GLPI (mesa de ayuda o helpdesk).
- Las palabras clave siempre deben estar encriptadas cuando se almacenen por cualquier período de tiempo significativo o cuando sean transmitidas por las redes. Lo anterior evitará que sean conocidas por interceptaciones de líneas de comunicación o por personas que puedan leer archivos log u otras partes no autorizadas.
- El usuario podrá realizar el cambio de clave del correo corporativo desde el portal web ingresando al link https://changepassword.mazars-co.local, el ingreso a este link solo es posible desde la red local de Forvis Mazars-CO, en caso de que se le olvide podrá solicitar al área de área de Tecnología Informática y Comunicaciones el restablecimiento de esta a través de GLPI (mesa de ayuda o helpdesk), correo electrónico o de forma escrita.
- Los usuarios deben de dejar el equipo con el usuario bloqueado cuando no estén presentes en su lugar de trabajo para evitar accesos no autorizados a la información. El sistema operativo debe bloquearse con contraseña automáticamente a los 15 minutos de no detectar acción alguna sobre el equipo.
- Está prohibido para los usuarios proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de FORVIS MAZARS, a menos que se tenga el visto y/o la autorización del Gerente General.
- Las palabras clave proporcionadas por el proveedor o fabricante, se deben cambiar antes de que en FORVIS MAZARS, se utilice cualquier sistema de computación o de comunicaciones.

3.3 Políticas sobre la información

Con el fin de garantizar el adecuado manejo de la información por cada uno de los funcionarios y colaboradores de **FORVIS MAZARS**, se define:

- Toda información digital que se genere o que se manipule dentro de la red de FORVIS MAZARS debe ser resguardada en los servidores destinados para el almacenamiento de la información.
- Es obligatorio el uso de las unidades de red, SharePoint y/o OneDrive (Office365) y no unidades locales ni el escritorio del sistema para almacenar la información crítica del negocio, para lo cual cada usuario debe tener configurado en su equipo la unidad virtual de red, según los accesos. **Está prohibido compartir carpetas desde el OneDrive a externos (clientes), para esto se debe utilizar el sitio de SharePoint.**

otorgados que le direccione a la carpeta personal en el servidor de almacenamiento, en la cual deberá guardar toda la información a la cual será realizado copias de respaldo.

- La información digital que se genere por los colaboradores de FORVIS MAZARS., debe cumplir con los principios fundamentales de Privacidad, Integridad, Disponibilidad, Control de Acceso y auditabilidad.
- La información digital debe contar con niveles de protección adecuada según su nivel de sensibilidad de tal manera que permita el acceso y uso únicamente a los usuarios autorizados.
- El material impreso o digitalizado que sea procesado en la red FORVIS MAZARS, no podrá ser retirado de la firma, sin previa autorización de Gerente de Área y/o Supervisor.
- Está prohibido extraer información de FORVIS MAZARS desde dispositivos de almacenamientos externo como discos extraíbles. Los medios de acceso a dispositivos externos se encuentran bloqueados dado cumplimiento a la política de seguridad, y es aplicable de manera general para todos los usuarios. Solo se podrá acceder con previa autorización del Socio/Gerente de FORVIS MAZARS con apoyo del área de Tecnología Informática y Comunicaciones.
- Es obligación la revisión de información en las unidades de red con el fin de auditar a los usuarios que almacenan información no permitida o redundante en la red. El uso de unidades de red se encuentra limitado exclusivamente a información corporativa.
- En caso de pérdida, daño, accesos no autorizados, o mal uso de la información confidencial de la compañía (digital o impresa) el responsable del proceso debe informar inmediatamente al área de área de Tecnología Informática y Comunicaciones, detallando lo ocurrido y las implicaciones que esto puede tener sobre la operación del negocio.
- Se deberá realizar el backup a la información de los usuarios que se retiren de FORVIS MAZARS., incluyendo correos electrónicos. Los usuarios que requieran estos backups deberán solicitar al Gerente de cada Área y/o Gerente General autorización quien por medio de correo electrónico al área de tecnología autorizara el acceso al backup a consultar especificando los permisos correspondientes de lectura y estableciendo el tiempo de consulta de la información solicitada, en cualquier caso, los permisos otorgados sobre la información a consultar serán exclusivamente de lectura.
- FORVIS MAZARS, deberá contar adicionalmente con un respaldo de la información en un sitio externo a las oficinas de la firma, en caso de desastres naturales como terremotos, incendios, inundaciones que involucren el daño total o parcial de las instalaciones de **“**FORVIS MAZARS**”**. Para tal caso se deberá garantizar el correcto almacenamiento con confiabilidad, integridad, disponibilidad, y confidencialidad, en cualquier momento.
- Está prohibido el uso de memorias USB y unidades de CD/DVD. Solo personal autorizado podrá tener acceso a estos dispositivos con el fin de cumplir procesos netamente del área. Para lo cual cada jefe de cada área debe reportar al área de Tecnología Informática y Comunicaciones el listado de funcionarios a su cargo que manejaran estos tipos de dispositivos, indicando el tiempo de uso, tipo de dispositivo al que tiene acceso (USB, CD-ROM), el tipo de acceso (lectura, escritura).

- El funcionario que tenga autorización para utilizar dispositivos externos (USB, CD-ROM) será el responsable de la información que en este se maneje y del buen uso de estos.

3.4 Políticas sobre la información

Se pretende enfocar las medidas mínimas para fortalecer adecuadamente el acceso físico a los dispositivos informáticos e infraestructura de red y servicios de comunicaciones de la firma.

- Todo usuario deberá reportar de forma inmediata al área de tecnología cuando se presenten riesgos sobre la infraestructura tecnológica de “FORVIS MAZARS”, como choques eléctricos, caídas de líquidos sobre cualquier dispositivo, golpes, etc.
- Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones de “FORVIS MAZARS” únicamente con autorización expedida por el área de Tecnología Informática y Comunicaciones y teniendo en cuenta el área de operación. Esta autorización deberá relacionar el tipo de dispositivo así:
    - Marca
    - Referencia
    - Código de inventario
    - Serial
    - Destino
    - Fecha y hora de salida
    - Persona a cargo
    - Fecha y hora de regreso a las instalaciones
    - Firma de las dos partes.
- Los servidores y dispositivos de conexión de red y comunicaciones se deben alojar en un cuarto de datos aislado a los usuarios con puerta, en el que se pueda restringir y controlar el ingreso de personal, este cuarto debe contar condiciones ambientales adecuadas para evitar daño a los equipos y poseer un nivel de seguridad física mínimo.
- El cableado estructurado o cualquier elemento físico de red solo puede ser manipulado por personal del área de Tecnología Informática y Comunicaciones o un tercero que sea autorizado únicamente por esta misma área.
- Está prohibido el acceso a usuarios de FORVIS MAZARS sin previa autorización del personal del área de Tecnología Informática y Comunicaciones a centros de cómputo y Servidores; solo está autorizado el acceso a personal del área de Tecnología Informática y Comunicaciones. Cualquier persona externa de FORVIS MAZARS que ingrese a centros de cómputo deberá tener acompañamiento por personal del área de Tecnología Informática y Comunicaciones y así proteger la información y los bienes informáticos.
- Todo personal sin excepción que ingrese al centro de cómputo de la firma debe registrarse en el formato diseñado para tal caso, en el que se dejara:
    - Fecha de ingreso
    - Hora ingreso
    - Nombre y Apellido

- Motivo
- Autorizado por
- Fecha de salida y firma.

- Los equipos de cómputo que funcionan como servidores deben estar bajo la responsabilidad de personal con habilidad y experiencia para realizar las tareas de administración.
- La administración de los servidores podrá realizarse por parte del personal interno o a través de la contratación con terceros.
- Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información, que se encuentre almacenada en los equipos de cómputo que tenga asignados.
- Se debe evitar colocar objetos como carpetas, folios, hojas, bebidas encima del equipo de cómputo o tapar las salidas de ventilación del monitor o de la CPU.
- Mientras se opera el equipo de cómputo, no se debe consumir alimentos o ingerir líquidos ya que esto puede llegar a ocasionar daños a los dispositivos.
- El usuario debe asegurarse que los cables de conexión del equipo de cómputo eléctrico y de datos no sean pisados al colocar otros objetos, en caso de que no se cumpla el usuario debe solicitar la reubicación de cables con el personal del área de Tecnología Informática y Comunicaciones.
- Solo el personal del área de Tecnología Informática y Comunicaciones está autorizado para abrir o destapar los diferentes equipos de cómputo, realizar los mantenimientos correctivos o preventivos o por parte de un tercero con el que se suscriba contrato para tal fin.
- El usuario que tenga a su cargo un equipo de cómputo, periférico, cámara, video proyector, etc, será el responsable directo de su uso y cuidado, respondiendo por este bien de acuerdo con lo estipulado para los casos de robo o pérdida de este. En caso de daño, desperfecto por maltrato, descuido o negligencia, se realizará reporte de incumplimiento de políticas de seguridad al usuario que tenga a cargo el dispositivo.
- En caso de robo o extravió de algún elemento de cómputo se debe notificar inmediatamente al área de Tecnología Informática y Comunicaciones y a la subgerencia administrativa, para tomar las medidas correspondientes.
- Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.
- Se debe garantizar los equipos de protección contra incendios, inundaciones y fluctuaciones eléctricas (UPS).

3.5 Políticas para el uso de software

Partiendo de la importancia de cumplir con las normas legales sobre los derechos de autor, copyright, derechos de uso y divulgación e instalación de software se presentan algunas normas prioritarias para el cumplimiento de estas.

- En los equipos de cómputo que pertenezcan a “FORVIS MAZARS”, solo se deberá instalar y usar software que tenga las respectivas licencias, acuerdos de uso o que sean en su totalidad software libre, evitando al máximo la instalación de software demo o de prueba.
- Solo el personal del área de Tecnología Informática y Comunicaciones está autorizado para la instalación desinstalación, actualización y administración de software en los equipos que pertenecen a FORVIS MAZARS.
- Todas las Licencias de software adquiridas por “FORVIS MAZARS” a través de compra, donación o cesión son propiedad y de uso exclusivo de FORVIS MAZARS.
- El software adquirido e instalado en los equipos de la firma debe ser usado exclusivamente para uso relacionado con las actividades propias del ejercicio de “FORVIS MAZARS”.
- En el caso de hallar software ilegal instalado en los equipos de la firma, se hará responsable al usuario que tenga el equipo a cargo para toda responsabilidad civil, económica y penal cuando se le haya comprobado su falta.
- El control, manejo de las licencias y el inventario de los Medios, paquete de CD´s será responsabilidad del área de Tecnología Informática y Comunicaciones.
- El área de tecnología se hará responsable del inventario físico de cada equipo con sus respectivas licencias del software instalado.
- Si se requiere la instalación de algún software debe solicitarlo por escrito, por correo electrónico por GLPI al área de Tecnología Informática y Comunicaciones, indicando la justificación, equipo donde se deberá realizar dicha instalación y contar con la autorización de la subgerencia administrativa.
- El software y aplicaciones que están permitidas varían de acuerdo con el área y las necesidades de cada usuario, pero en general los únicos programas y aplicaciones permitidos según la cantidad de licencias adquiridas son:
    - Microsoft Windows
    - Microsoft Office
    - Adobe PDF
    - Helisa NIIF
    - Helisa Nomina
    - Antivirus ESET-Kaspersky

  El software tipo gratuito (freeware) permitido en los equipos de FORVIS MAZARS es el siguiente:

    - PDF24
    - Gliffy
    - Agente Fushion Inventory
    - Cliente KIMAI
    - Cliente GLPI
    - Fillezilla Client
    - WinSCP
    - Notepad++

- Veracript
- 7-Zip
- KeePass
- VLC Media Player

El uso de otro tipo de software open source debe ser evaluado y aprobado por el área de Tecnología Informática y Comunicaciones.

- Se prohíbe el uso de tecnologías de virtualización de pago o gratuitas dentro de los equipos de cómputo, excepto en casos que sean autorizados por el área de Tecnología Informática y Comunicaciones, y en las cuales se garantice el correcto licenciamiento de estas.
- El área de Tecnología Informática y Comunicaciones deberá llevar un inventario de las licencias de software de la firma en la que se relacione como mínimo el tipo de software, la clave de licencia y el equipo en el que fue instalada.

3.6 Políticas para el uso de Correo Electrónico Office 365 y Microsoft Teams

El correo electrónico Office 365 y Microsoft Teams es el medio formal y oficial de comunicaciones de Mazars Colombia S.A.S. y una herramienta de trabajo que ha dispuesto la firma con el fin de facilitar las labores propias de los cargos de cada uno de sus empleados y/o colaboradores, es primordial establecer los lineamientos que se deben tener presente de acuerdo con las obligaciones, prohibiciones que cada empleado debe tener presente.

- Los usuarios son responsables de todas las actividades que se realicen desde su cuenta de correo electrónico Office 365 y Microsoft Teams.
- El uso de las cuentas de correo electrónico Office 365 y Microsoft Teams de FORVIS MAZARS asignadas a cada usuario es y debe ser de uso razonable, no se debe utilizar para registrarse a páginas para uso personal como redes sociales, eventos, almacenes de cadena, etc.
- Todos los usuarios deben utilizar para el manejo de correos electrónicos office 365 la herramienta Microsoft Outlook y para Microsoft Teams la herramienta de Microsoft Teams, la cual esta licenciada por FORVIS MAZARS, para lo cual cuando se le asigne la cuenta de correo se debe configurar en el equipo asignado.
- Las cuentas de correo electrónico Office 365 y Microsoft Teams son creadas para el uso exclusivo de las funciones propias del usuario, por lo tanto, el usuario debe hacer uso de este servicio implementando criterios de racionalidad, respeto, responsabilidad, integridad y seguridad de la información.
- Todos los usuarios deben manejar los mensajes instantáneos de Microsoft Teams tanto de recepción y envió, el correo electrónico office 365 entrantes y salientes y archivos adjuntos como información propiedad de FORVIS MAZARS. y destinada exclusivamente al ejercicio estricto de sus funciones y responsabilidades.
- Queda prohibido y de falta grave falsificar, esconder, suprimir o sustituir la firma de un usuario de correo electrónico office 365 y Microsoft Teams.

- Los usuarios no deben utilizar cuentas de correos electrónicos office 365 y cuentas de Microsft Teams asignadas a otros usuarios. En caso de ser necesario la utilización o lectura de correos o mensajes enviados de Microsoft Teams de otra persona ya sea porque el propietario de la cuenta se encuentre de vacaciones, permisos, incapacitado o porque es un funcionario retirado de FORVIS MAZARS, se debe contar con autorización del funcionario ausente o con autorización del jefe de área por escrito o por correo o por GLPI al área de Tecnología Informática y Comunicaciones.
- Para el redireccionamiento de correos a otra cuenta se debe enviar autorización por escrito o por correo o a GLPI al área de Tecnología Informática y Comunicaciones, evitando el redireccionamiento a una cuenta de correo externa para efectos de resguardar la información de FORVIS MAZARS.
- FORVIS MAZARS podrá revisar los buzones de correo electrónico de office 365 y conversaciones realizadas por Microsoft Teams cuando lo estime conveniente para verificar el cumplimiento de la política o por otras razones acordes a los intereses legítimos de la compañía. Enviando autorización por escrito o por correo o por GLPI al área de Tecnología Informática y Comunicaciones por parte de la gerencia general.
- FORVIS MAZARS no se hace responsable del uso inapropiado que los usuarios hagan de sus cuentas de correo electrónico office 365 y Microsoft Teams.
- Los funcionarios y contratistas podrán únicamente hacer uso del correo corporativo office 365 y de la cuenta de Microsoft Teams durante la vigencia del respectivo contrato.
- El uso de listas de correos y reenvíos masivos serán únicamente para comunicaciones estrictamente laborales con información de interés general y formal.
- Según lo establecido en la **Ley 527 de 1999 art 10 y 11**, los mensajes de correo electrónico revisten la misma fuerza probatoria que tienen los documentos físicos.
- El envío de correos electrónicos office 365 implica el consumo de recursos tecnológicos y demanda tiempo a la persona receptora, por tal razón se debe evitar el envío de correos innecesarios y que no guarden relación con el desempeño de las funciones asignadas.
- Todo correo de procedencia desconocida, correo basura, SPAM, correo no deseado, phishing, etc. que sea recibido en los buzones de correo electrónico de FORVIS MAZARS, debe ser reportado de inmediato al área de Tecnología Informática y Comunicaciones con el fin de evaluar y tomar las medidas pertinentes para evitar posibles infecciones y/o hacking de un tercero por código malicioso o virus.
- El área de Tecnología Informática y Comunicaciones es la autorizada para el envío de correos masivos, comunicados, etc., en caso de que alguna área, departamento o persona requiera enviar algún correo masivo, deberá solicitarlo al área de Tecnología Informática y Comunicaciones, quienes evaluarán la pertinencia o no de dicha solicitud y realizará las actividades pertinentes.
- El envío masivo de correos electrónicos puede hacer que los correos electrónicos del remitente se marquen como correo no deseado, además de arruinar potencialmente la capacidad de la organización para comunicarse por correo electrónico, el envío masivo de correos electrónicos desde el dominio FORVIS MAZARS puede provocar el bloqueo del dominio, por lo que está prohibido.

3.7 Políticas para la generación de Backups

Como medidas de contingencia para aseguramiento y restablecimiento de la información es indispensable definir las políticas de generación de backups que permitan identificar el tipo de backup, procesos de restauración y los responsables de dicha actividad.

- La creación de copias de respaldo es una herramienta muy útil como medida de seguridad informática y contingencia en cualquier tipo de desastre o en caso de daño, perdida, borrado de la información o de los dispositivos de almacenamiento, por lo cual se debe realizar copias de respaldo o Backus periódicamente de toda la información digital de la firma el área de tecnología debe programar las tares necesarias.
- El área de Tecnología Informática y Comunicaciones de FORVIS MAZARS será responsable generar y desarrollar las tareas necesarias para realizar los backups internos de la información.
- Las copias de seguridad se deben realizar en Backups Cloud, medios magnéticos, discos duros o dispositivo de almacenamiento externo de forma organizada para garantizar su pronta recuperación.
- Las copias de seguridad o backups se deben realizar a diario y uno trimestral en cada Q (Q1 enero a marzo) de forma externa, registrando el cumplimiento de esta actividad en un formato de bitácora adecuado.
- Las copias de seguridad o backups se deben realizar a diario y uno trimestral en cada Q de forma externa así:
    - Q1: Enero, febrero y marzo.
    - Q2: Abril, mayo, junio.
    - Q3: Julio, agosto, septiembre.
    - Q4: Octubre, noviembre, diciembre
- Estas actividades deben estar registradas en la bitácora de backups; adicional cuando se entreguen los backups trimestral a la gerencia estos se deben entregar listando los archivos y con acta de entrega.
- Los usuarios que se encuentran fuera de las instalaciones de FORVIS MAZARS deben usar almacenamiento en la nube como OneDrive para salvaguardar la información.
- El usuario final será el responsable de pasar/copiar toda la data que tiene almacena en OneDrive al servidor donde está localizada la data en FORVIS MAZARS.

3.8 Políticas sobre el uso de Red y de Internet

Este servicio es suministrado por el FORVIS MAZARS, para los empleados, contratistas y proveedores, previamente autorizados para su uso, con el propósito de facilitar el cumplimiento de sus actividades laborales diarias por medio del acceso a fuentes de consulta de información científica, técnica, gubernamental y/o de cualquier índole, sobre temas de importancia para la firma. Como todo servicio, que basa su operación en el manejo de información, FORVIS MAZARS promueve el uso prudente y mesurado de este servicio para apoyar las operaciones y comunicaciones propias del negocio. Esta Política está basada en las buenas

prácticas y recomendaciones de seguridad, administración y privacidad de la información, identificadas para los servicios tecnológicos de las instituciones del sector público y privado.

- Cada colaborador es responsable por conocer, adoptar y acatar esta política cada vez que haga uso de este servicio.
- Toda información o contenido consultado, copiado o descargado queda bajo responsabilidad del dueño de la cuenta del computador asignado. Se recomienda citar la fuente (página web) en los documentos o informes generados con información obtenida por este servicio.
- Toda responsabilidad derivada del uso de un nombre de usuario distinto al propio recaerá sobre aquel usuario al que corresponda el nombre indebidamente utilizado.
- Es indispensable que todos los funcionarios de FORVIS MAZARS. demuestren un comportamiento profesional y ético al tener acceso a Internet para proteger la imagen de la firma. Son muy importantes igualmente la protección de la información su gestión y la seguridad aplicada a toda la información que se obtenga o comparta por este medio.
- El área de Tecnología Informática y Comunicaciones puede monitorear el uso del servicio de Internet o revisar el contenido de las páginas visitadas por cualquier usuario al igual que los contenidos o archivos descargados en cualquier momento con el fin de asegurar el buen uso de este sistema.
- Si se determina que alguna de las páginas previamente restringidas por el área de Tecnología Informática y Comunicaciones es requerida para el desempeño de funciones de algún colaborador esta será habilitada únicamente con el consentimiento y solicitud de su jefe directo.
- El uso de la red inalámbrica de **FORVIS MAZARS** es para uso exclusivo de usuarios que requieran su uso como parte de sus funciones o actividades propias del negocio. El uso de los recursos de las redes es utilizado como medio de comunicación para la conexión del total de equipos e impresora y dispositivos/activos que los requieran y que sean de FORVIS MAZARS, por lo tanto, debemos garantizar un uso considerable por parte de los usuarios para contar con el ancho de banda suficiente para las labores importantes que se realizan día a día.
- El acceso a internet con que cuenta la firma es para las actividades relacionadas de acuerdo con el cargo y funciones desempeñadas, por favor sea razonable con el uso de internet para fines personales.
- Los usuarios deben reportar al área de Tecnología Informática y Comunicaciones cualquier incidente que se presente en el servicio de internet.
- Está prohibido la descarga de software de internet sin la autorización de la gerencia o del área de Tecnología Informática y Comunicaciones.
- Se prohíbe la administración remota de equipos conectados a Internet, salvo que se cuente con autorización gerencia general y/o área de Tecnología Informática y Comunicaciones y con un mecanismo de control de acceso seguro.
- Para gestionar la vulnerabilidad técnica en **FORVIS MAZARS** se emplea un servicio externo llamado BITSIGHT, con el cual se reduce e identifica el riesgo cibernético, reduciendo así las brechasde seguridad y vulnerabilidades.

3.9 Políticas sobre la Red Física de Datos y la Red Eléctrica

La presente política contiene los lineamientos necesarios para garantizar el buen uso del cableado estructurado FORVIS MAZARS.

- El sistema de cableado estructurado debe contar en todo su recorrido con la protección de ductos (canaletas, rieles, tubo) adecuada necesaria para evitar daños en su parte física, durante todo su recorrido.
- El sistema de cableado estructurado debe ser documentado mediante planos y archivos que ilustren su recorrido y los diferentes tipos de cableado, ductos y nomenclatura de identificación utilizada para cada punto de red.
- Se debe contar con un sistema de cableado que cumpla las normas de cableado estructurado EIA/TIA 568, para este propósito se debe tener en la infraestructura de red cableado estandarizado en categoría 6A.
- El centro de cableado y de servidores de FORVIS MAZARS debe contar con una seguridad minina de acceso físico, en la que se controle mediante puerta con seguro el ingreso al personal no autorizado y mediante formato de ingreso a centro de cómputo registrar los ingresos del personal de mantenimiento.
- El sistema de cableado estructurado debe contar en todos sus elementos con el correspondiente maquillaje de identificación.
- Cualquier cambio que se realice en el sistema de cableado estructurado y en el centro de cómputo deben ser bajo la supervisión del área de Tecnología Informática y Comunicaciones y debe quedar documentado.
- Los usuarios de FORVIS MAZARS deben cuidar el sistema de cableado dando una correcta utilización, no se debe maltratar de ningún modo, se debe enchufar y desenchufar las conexiones de manera correcta y con cuidado.
- A la red regulada de la firma solo se debe conectar los equipos y dispositivos propios de FORVIS MAZARS que pertenezcan al área de tecnología y que sean indispensables para el manejo de la información, como computadores, portátiles, servidores, unidades de almacenamiento entre otros. Dispositivos personales no se deben conectar a la red regulada ni equipos que representen riesgo al adecuado funcionamiento de la red regulado como cafeteras, ventiladores, aspiradoras, etc.

3.10 Política para la protección contra virus informáticos

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen necesarios para lograr los objetivos de la organización y asegurar el cumplimiento de objetivos misionales.

FORVIS MAZARS y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o

vandalismo a través de virus informáticos, hacking o ataques de denegación de servicio; por tal motivo se pautan las siguientes políticas con el fin de mitigar estas amenazas.

- El área de Tecnología Informática y Comunicaciones será la responsable por mantener vigente las licencias y actualizado los antivirus con que cuenta FORVIS MAZARS.
- Todo equipo de cómputo perteneciente a FORVIS MAZARS. debe tener instalado un antivirus para la protección de infecciones informáticas.
- Los usuarios deben seguir las recomendaciones y directrices establecidas con el fin de prevenir la infección con virus informáticos.
- Todos los correos, archivos adjuntos, memorias USB y cualquier dispositivo de almacenamiento deberán ser analizados por el antivirus con el fin de prevenir la infección y propagación de virus informático.
- Periódicamente se hará el rastreo en los equipos de cómputo de FORVIS MAZARS, y se realizarán las siguientes acciones: Actualización automática de las firmas antivirus proporcionadas por el fabricante de la Solución Antivirus.

3.10 Política de acceso remoto

FORVIS MAZARS pretende conceder de manera segura y cumpliendo los tres pilares de la seguridad informantica (Confidencialidad – Integridad – Disponibilidad) a sus colaboradores, clientes, proveedores ETC, acceso a los sistemas de información de la firma, para que puedan llevar a cabo las labores que les correspondan.

- Entiéndase como acceso remoto el acto de conectarse a servicios, aplicaciones, datos y archivos desde una ubicación distinta a FORVIS MAZARS o una ubicación más cercana al centro de datos. Esta conexión permite a los usuarios acceder a una red o una computadora de forma remota a través de una conexión a Internet o telecomunicaciones.
- FORVIS MAZARS solo tiene autorizado el acceso remoto por conexión Virtual Private Network (VPN) y/o Escritorio Remoto (RDP).
- Sólo los usuarios previamente autorizados podrán utilizar los beneficios de acceso remoto (VPN y/o RDP), los que, además, serán los responsables del correcto uso de este servicio.
- Es de responsabilidad del usuario con privilegios de acceso remoto (VPN y/o RDP), asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.
- El uso del sistema de acceso remoto (VPN y/o RDP), debe ser controlado utilizando una contraseña de autenticación fuerte tal cual se mencionada en el numeral *3.2 Política de administración de perfiles y contraseñas*, manteniéndola siempre en secreto.
- Cuando esté conectado activamente a la red de FORVIS MAZARS, el sistema de acceso remoto VPN, permitirá el tráfico de acuerdo con el perfil del usuario hacia y desde el equipo a través del túnel VPN, por el protocolo el resto del tráfico pasará por la conexión respectiva.
- Cuando esté conectado activamente a la red de FORVIS MAZARS, el sistema de acceso remoto RDP, le permitirá visualizar la información de manera gráfica, todo el tráfico pasara por la red local de la firma.

- Es responsabilidad del área de Tecnología Informática y Comunicaciones asegurar el servidor de conexión RDP con la guía de hardening de la norma PCI DSS.
- Según el tipo de usuario se definen el máximo de sesiones simultáneas, que podrá generar cada usuario.
- Las puertas de enlace VPN y Conexión RDP serán configuradas y administradas por el área de Tecnología Informática y Comunicaciones.
- Todos los computadores conectados a las redes internas de FORVIS MAZARS mediante acceso remoto (VPN y/o RDP) deberán utilizar un software antivirus, este debe estar actualizado cuando se realice la conexión. Para los equipos personales es responsabilidad del usuario proveer este software antivirus a sus equipos.
- Los usuarios del sistema VPN serán automáticamente desconectados de la sesión, una vez que hayan transcurrido 5 minutos de inactividad. Los usuarios del sistema RDP serán automáticamente desconectados de la sesión, una vez que hayan transcurrido 10 minutos de inactividad de la sesión activa o 5 minutos para las sesiones desconectadas. El usuario deberá realizar el login nuevamente para volver a conectarse a la red de FORVIS MAZARS. Procesos artificiales informáticos como el “PING” no deben ser utilizados para mantener la sesión abierta.
- Para los usuarios finales que no cuentan con algún tipo de contrato con Mazars Colombia SAS, deberán cumplir todas las disposiciones establecidas en esta política y deberá firmar un acuerdo de confidencialidad de la información.
- Mediante el uso de la tecnología de mediante acceso remoto (VPN y/o RDP), los usuarios declaran conocer que sus computadores, ya sean asignados por el área de Tecnología Informática y Comunicaciones de FORVIS MAZARS o personales son una extensión de las redes de FORVIS MAZARS SAS y como tales, están sujetos a las mismas normas y reglamentos que se aplican a los equipos dentro de las dependencias de FORVIS MAZARS.
- La única manera segura de conexión a cualquier dispositivo dentro de la red local de Forvis Mazars-CO es a través de una conexión VPN y RDP.

4. Compromisos y Principios de Seguridad de la Información

En Forvis Mazars, reconocemos la importancia de proteger la información como un activo valioso para nuestra organización y nuestros clientes. Esta política establece el marco de actuación de Forvis Mazars para gestionar la seguridad de la información, garantizando el cumplimiento de los requisitos legales y contractuales aplicables, así como el compromiso con la mejora continua de nuestro Sistema de Gestión de Seguridad de la Información (SGSI). A continuación, se presentan los compromisos y lineamientos de Forvis Mazars en relación con la seguridad de la información

- Compromiso de Cumplimiento: Forvis Mazars se compromete a cumplir con todos los requisitos legales, regulatorios y contractuales aplicables en materia de seguridad de la información, asegurando que nuestras prácticas y controles de seguridad estén alineados con las normas y obligaciones vigentes.

- Compromiso de Mejora Continua: Forvis Mazars asegura el compromiso de mejora continua de su Sistema de Gestión de Seguridad de la Información (SGSI), revisando y fortaleciendo de manera constante los controles y prácticas de seguridad de la información para adaptarse a los cambios en el entorno y las necesidades de la organización.

- Objetivos de Seguridad de la Información: Forvis Mazars establece objetivos claros y medibles en materia de seguridad de la información, orientados a proteger la confidencialidad, integridad y disponibilidad de la información, cumplir con los requisitos aplicables y fomentar una cultura de seguridad en toda la organización.

- Roles y Responsabilidades: La dirección de Forvis Mazars es responsable de la implementación y cumplimiento de esta política de seguridad de la información, asignando roles y responsabilidades específicas dentro de la organización para asegurar el cumplimiento de los compromisos de seguridad.

- Periodicidad de Revisión: Esta Política de Seguridad de la Información será revisada mínimo una vez al año, o en caso de cambios significativos en el entorno organizacional o normativo, para asegurar su continua adecuación y efectividad. La alta dirección de Forvis Mazars es responsable de esta revisión y actualización.

- La presente política satisface los requisitos aplicables relacionados con la seguridad de la información.

CONTROL DE VERSIONES

VERSIÓN	FECHA	PRÓXIMA REVISIÓN	AUTOR(ES)	DESCRIPCIÓN
1.0	30/05/2017		Juan Carlos Araque	Creación y aprobación de documento – Aprobación Gerencia General
2.0	28/06/2017		Carlos Guerrero	Se agrega cláusula de cumplimiento, se agrega listado de software freeware y restricción de uso de máquinas virtuales. Se modifica Política de backups para incluir proyecto de backup de datacenter alterno.
3.0	15/05/2018		Jhon Lopez	Cambio de formato, Modificación de todo el documento en las cláusulas en la política
3.1	22/08/2019		Jhon Lopez	Revisión, adición de nuevo permisos USB y actualización de contraseñas. Adición política acceso remoto.
4.0	15/11/2021		Fernando Malaver	Cambio de Formato para Iso27001 Codificación, control de versiones
4.1	3/03/2023		Fernando Malaver	Actualización punto 3.6 Correos masivos.
4.2	1/06/2024		Fernando Malaver	Actualización Razón Social y Logo.
4.3	05/12/2024		Julio Jiménez	Actualización de política, compromisos y principios de SI
5.0	15/07/2025		Julio Jiménez	Actualización documento según comentarios Audit interna/externa 2025, Ingreso de objetivos de SGSI actualizados según NC 4.

DISTRIBUCIÓN

ÁREA / PERSONA
Responsable de IT
Comité de Dirección

REVISIÓN

Redactado	Revisado	Aprobado
Julio Jiménez Gerente IT	Carlos Andrés Molano	Confirmo que todos los documentos y/o información e indicadores relevantes del SGSI han sido revisados y , alineándose con nuestros objetivos estratégicos y normativos. Reitero nuestro compromiso como organización en mantener y mejorar continuamente nuestro SGSI para garantizar la seguridad de la información y el cumplimiento de las normativas vigentes.
DIFUSIÓN	**IN1**	**CLASIFICACIÓN** **CL1**

(Tipo de difusión: **IN1**: interna; **IN2**: Grupo; **EXT**: al exterior) (Tipo de clasificación: **CL1**: público; **CL2**: confidencial; **CL3** in)