1. OBJETIVO

Constituir los procedimientos y políticas para el uso, control y administración de las Tecnología de Información y Comunicaciones que deben conocer y cumplir las todas las áreas de la empresa Global de Seguridad Zomac Ltda y sus colaboradores.

2. ALCANCE

Las políticas aquí definidas son aplicables para todos los funcionarios y contratistas de la empresa de Global de Seguridad Zomac Ltda, bien sea en calidad de usuarios o administradores de servicios e infraestructura de tecnología y comunicaciones.

Los dispositivos regulados y atendidos por estas políticas son:

- Aquellos que hacen parte de los activos fijos de la empresa Global de Seguridad Zomac Ltda.
- Aquellos de propiedad de terceros que usan servicios o la infraestructura de la empresa Global de Seguridad Zomac Ltda.

3. DEFINICIONES

3.1. TIC: Tecnologías de la Información y Comunicaciones.
3.2. Servidor: equipo de cómputo que, formando parte de una red, provee servicios a otras computadoras o dispositivos denominados clientes.
3.3. Dispositivo: para el presente manual se considera una denominación genérica para todo equipo electrónico como computadoras, tabletas, etc, que son utilizados para almacenamiento, procesamiento y comunicación de datos.

4. POLITÍCAS

4.1. Políticas Generales

- Bajo ninguna circunstancia los colaboradores de la empresa pueden utilizar los recursos informáticos para realizar actividades ajenas a los procesos corporativos de Global de Seguridad Zomac Ltda.
- Todos los equipos de cómputo (escritorio, portátiles) de propiedad de la empresa deben ser vinculados al dominio corporativo local (cuando sea aplicable) y se rigen bajo los parámetros y normas de seguridad definidas en

el servidor de dominio, se exceptúan aquellos equipos que físicamente se encuentran de manera permanente fuera de las instalaciones principales de la empresa o fuera del alcance de red del directorio activo.

- Todos los dispositivos propiedad de la empresa o de Terceros que usan o comparten servicios o recursos de infraestructura se acogen a los parámetros y normas de seguridad definidos en este manual.
- Los equipos propiedad de la empresa, solo pueden ser intervenidos por el departamento de Sistemas (o ha quien se le ha delegado este rol); este personal es el único autorizado para realizar las actividades de soporte técnico y cambios de configuración en el equipo de cómputo. En el caso de labores de mantenimiento efectuadas por terceros éstas deben ser previamente aprobadas el responsable Sistemas.
- El área de Sistemas no tiene ningún alcance y responsabilidad de soporte frente a equipos de terceros, salvo la supervisión de las condiciones mínimas de seguridad para la vinculación a sus servicios o infraestructura, en todo caso se requiere la autorización del responsable de Sistemas.
- El presente manual es de cumplimiento general, cada organización puede desarrollar controles adicionales para aspectos de seguridad y cumplimiento legal asociado a TI.

4.2. Adquisición de hardware, software y tecnología

4.2.1. Compras de infraestructura, licenciamiento o por volumen

Todos los requerimientos deben ser evaluados gestionando el mayor beneficio económico y poder de negociación para Global de Seguridad Zomac Ltda bajo la responsabilidad del encargado del área de Sistemas; los requerimientos o necesidades de la empresa serán formalizados como conducto regular a través de requisición con el fin de evaluar cada necesidad y determinar la viabilidad técnica, teniendo en cuenta los siguientes puntos:

- *Compras masivas o por volumen*: todo proceso de renovación tecnológica, compra masiva de dispositivos de cómputo o licenciamiento (sistemas operativos, suite de ofimática o aplicativos).
- *Adquisición de servidores e infraestructura*: procesos de renovación tecnológica e infraestructura, compra de servidores, sistemas de almacenamiento, switches, routers, firewalls, telefonía, sistemas de refrigeración, UPS y licenciamiento asociado.
- *Contratos alquiler tecnológico y de servicios*: cualquier tipo de alquiler de equipos o infraestructura y contratos de servicios (dominios, hosting, canales de internet, contratos de soporte, soluciones de impresión, aplicaciones, etc..).

- *Otras compras:* Los procesos de adquisición de periféricos de equipos de cómputo, relacionados con las necesidades de su operación (sustituciones, partes o repuestos).

En todo caso los procesos de compra para más de 2 equipos de cómputo por mes deben solicitarse cotización alterna con el área de compras haciendo evaluación de ofertas.

4.3. Asignación y devolución de equipos de cómputo

- La empresa debe garantizar los controles para el registro de inventario, entrega y devolución de equipos de cómputo.
- Cada organización debe garantizar los controles para el cumplimiento legal respecto a licenciamiento de software de uso autorizado.
- Se debe regularizar el inventario de equipos de cómputo con base a los parámetros establecidos en el formato de inventario.

4.4. Uso de equipos de computo

- Todo dispositivo de cómputo, propiedad de la empresa, deberá ser utilizado únicamente para actividades relacionadas a la operación y las responsabilidades asignadas de acuerdo con el rol del colaborador.
- El área de Sistemas debe implementar las acciones necesarias para el correcto funcionamiento de los equipos de cómputo entre ellas actividades preventivas y correctivas consideradas en el plan de mantenimiento.
- La solicitud de suministros, componentes, periféricos y/o accesorios de equipo de cómputo debe ser tramitados a través del departamento de Compras, con la asesoría del responsable de Sistema de mesa de ayuda.
- Se deben garantizar controles que logren aislar cualquier dispositivo de cómputo que no se encuentre bajo la intervención administrativa de la empresa (computadoras privadas del personal, computadoras de proveedores, contratistas o terceros en general, las cuales no están sujetas a las políticas de seguridad de la empresa y por ende constituyen un riesgo).
- De llegase a existir algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa los dispositivos de cómputo de la empresa, deberá ser notificado con la mayor brevedad al área de Sistemas o su responsable.
- Sólo el personal autorizado por el área Sistemas está facultado intervenir físicamente los equipos de cómputo propiedad de la empresa.

- Todos los equipos de cómputo bajo la supervisión de la empresa deben contar con un software antivirus actualizado, con el objetivo de proteger el equipo de programas maliciosos.
- Se debe gestionar que todas las computadoras de la compañía reflejen una imagen corporativa estandarizada, mediante un fondo o tapiz definido por las políticas de dominio y establecidas por el área de Sistemas.

4.5. Propiedad de la Información

Se deben instaurar los controles necesarios para garantizar que:

- Los datos que los funcionarios procesen y/o manipulan en las diversas aplicaciones y cualquier medio de procesamiento electrónico en Global de Seguridad Zomac Ltda, durante el desarrollo normal de sus actividades laborales, son propiedad de esta.
- Toda copia de seguridad o Backup que contenga información de la empresa, realizada bajo responsabilidad del usuario, debe ser entregada al momento de la finalización de la relación laboral.
- Todo funcionario que tenga relación con la información de la organización en cualquier formato o con cualquier servicio de procesamiento de información, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad de esta, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial.

4.6. Actividades prohibidas

- Violar los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.
- La distribución o instalación de software sin la licencia de uso adquirida por la empresa.
- Difundir información identificada como confidencial a través de medios que involucren el uso de la Tecnología de Información.
- Introducir software malicioso en la red o en los servidores (virus, malware, envío masivo de correo electrónico, etc.)
- Utilizar los medios tecnológicos suministrados por Global de Seguridad Zomac Ltda para conseguir o transmitir material con ánimo de lucro, algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.
- Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen

sean los recursos o servicios propios de la empresa.

- Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.
- Monitorear puertos o realizar análisis del tráfico de la red de telecomunicaciones. El personal del área de Sistemas, es responsable de la Seguridad Informática y puede realizar estas actividades siempre y cuando sean previamente autorizadas por la Gerencia.
- Burlar mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
- Usar comandos o programas para el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet).
- Instalar cualquier tipo de software en los equipos de cómputo de la empresa sin la previa autorización del área de Sistemas.
- Modificar la configuración de sistemas operativos, aplicativos institucionales softwares antivirus, o políticas de seguridad en general definidas en los equipos de cómputo.
- Descargar archivos de gran tamaño que puedan afectar los canales de datos y comunicación.

4.7. Administración de Contraseñas

Se deben establecer los controles para el uso de contraseñas que permitan a sus colaboradores acceder a los recursos actuales de manera segura e idónea, a su vez constituyan la primera línea de defensa para garantizar que la información sólo sea accedida por el personal autorizado.

- Todos los usuarios de Global de Seguridad Zomac Ltda requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo asignado y acceder a los servicios de redes y aplicaciones de la compañía.
- Las contraseñas deben cumplir los siguientes requisitos de seguridad: un mínimo de ocho (8) caracteres alfanuméricos, contener una letra mayúscula, un número y/o un carácter especial.
- Las contraseñas son personales, intransferibles y conocidas únicamente por usuario el cual será responsable de toda la actividad que se realice con su cuenta.
- En caso de identificar algún tipo de riesgo, el área de Sistemas tiene atribuciones para restablecer en cualquier momento la contraseña de cualquiera de los usuarios, con previo aviso para no afectar de ninguna manera la continuidad de su trabajo.
- Se debe habilitar el bloqueo de todas las computadoras de escritorio y portátiles después de 5 minutos de inactividad, el equipo es nuevamente disponible tras el ingreso de la clave del usuario.

- No revelar la contraseña personal o permitir su uso a terceros para actividades ajenas a la misión de la empresa, la prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario, cuando la conexión a la red corporativa se realice desde el hogar.
- No exponer las credenciales de acceso sobre recordatorios visibles en Monitores o libretas, Se recomienda que la contraseña sea aprendida de memoria y no apuntarla en ningún medio físico

4.8. Correo electrónico

- El Correo Electrónico es un medio de comunicación privada entre el emisor y el destinatario, por lo tanto, no podrá divulgarse a través de Internet información considerada como de uso confidencial hacia personal no autorizado, salvo la información considerada como parte de la gestión operativa y comercial.

- El usuario es responsable del contenido de los correos enviados esto incluye entre otros: Contenido de material ofensivo u obsceno, cualquier quebrantamiento de propiedad intelectual, copyright o cualquier información ilegal o criminal.

- Son actividades prohibidas la transmisión de mensajes que puedan establecer un medio hostil sobre la raza, edad, sexo, religión, política, nacionalidad, origen, incapacidad u orientaciones personales; comentarios despectivos, noticias informales o mal intencionadas, cadenas de cartas, mensajes masivos de índole personal, y en general cualquier tipo de información que cause congestión en la red o interfiera con el trabajo de otros.

- El área de Sistemas es responsable de analizar y bloquear la recepción de correos electrónicos desde aquellas direcciones que se han identificado como spam, virus, código malicioso, catalogadas en lista negra o con mala reputación. En caso de requerir la recepción de correo electrónico desde alguna de las direcciones identificadas como ofensivas deberá solicitarse al área de Sistemas quien revisará su posible viabilidad dado que los recursos de almacenamiento y redes son limitados se debe establecer el procedimiento para el uso, control de los recursos y garantizar la custodia de la información.

4.9. Internet

- El área de Sistemas establecerá los controles que garanticen el uso adecuado del recurso en relación con las actividades y funciones de los colaboradores

- El acceso a contenido web debe ser restringido y controlado a contenidos pertinentes al normal desarrollo de las funciones administrativas y servicios operativos que demande la compañía, los funcionarios son responsables de mantener su imagen profesional dentro de Internet, así como proteger la imagen y reputación de la empresa, el acceso a páginas no autorizadas podrá ser observadas y de inmediato serán informadas.

- No se debe de utilizar el acceso a Internet como un medio de participación, acceso y distribución de actividades o materiales que vayan en contra de la Ley o las políticas de la compañía.

- No se faculta acceder, ver o descargar desde sitios de Internet: gráficos, imágenes o cualquier otro material que pueda ser observado como obsceno, abusivo o que contenga humor inapropiado, lenguaje amenazante u otra forma de lenguaje objetable dirigido a un individuo o grupo.

4.10. Almacenamiento y Copias de Seguridad

- La información obtenida de cualquiera de los servicios internos deberá ser almacenada localmente en el equipo de cómputo del usuario y no puede ser distribuida o transmitida por la red institucional, sin la autorización respectiva.

- Las áreas de almacenamiento compartidas como recursos de red deben ser tratadas como almacenamientos temporales y su uso está restringido a documentos. El área de Sistemas debe garantizar el aprovechamiento óptimo de los recursos compartidos para mantener la integridad y para asegurar que los usuarios utilicen los recursos de manera responsable.

- Las unidades de red de usuario deben mantener estrictamente la información requerida para el trabajo diario; cualquier dato con antigüedad superior de 12 meses debe ser considerado información histórica sujeta a respaldo.

- Los recursos compartidos se encuentran almacenados en la nube de One Drive administrado por el Responsable de Sistemas, en caso de que se produzca una falla en el disco duro, se podrán restaurar los documentos a través de copia de seguridad.

- El área de Sistemas, realizará copia periódicas de seguridad de los servidores donde se encuentras las aplicaciones y recursos compartidos como segunda medida de recuperación.

- Los recursos y aplicaciones alojados en el One Drive tendrán tareas de mantenimiento y Backup cada 15 días además de contar con Respaldos de Copias de Seguridad en Disco Duro Sólido.

4.11. Conducta del usuario

- El usuario es responsable de transmisiones de cualquier tipo a través su cuenta y servicios asociados.
- El usuario no debe usar los servicios de tecnología para propósitos ilegales o de entretenimiento.
- El usuario debe cumplir con todas las regulaciones, políticas y procedimientos internos.

- La comunicación de los usuarios se debe conducir con respeto y consideración, evitando los abusos y el uso del lenguaje inapropiado.
- Se prohíbe el acceso a cualquier fuente de información cuyo contenido no se encuentre relacionado con las actividades propias del trabajo y funciones del colaborador (Redes Sociales Facebook, Instagram, YouTube, entre otras).

4.12. Administración de Software

El área de Sistemas, es la única área autorizada para llevar a cabo la administración del software de la empresa, por lo que se encuentra dentro del alcance de sus responsabilidades:

- Mantener bajo resguardo las licencias de uso de software.
- Llevar un control de las licencias en operación y el equipo en el cual se encuentra en uso.
- Planificar la inspección de equipos de cómputo en intervalos regulares.

- Difundir a los empleados las Políticas de Uso de Software con el fin de que conozcan la normatividad en este concepto.

4.13. Instalación y soporte de Software

- El área de Sistemas es la única autorizada para realizar la instalación de software y proporcionar soporte del mismo en todos los equipos de cómputo.

- Se prohíbe la instalación de copias ilegales de cualquier programa descargado de Internet, software adquirido para uso personal del usuario o software de esparcimiento.

4.14. Proveedores de servicio técnico (acuerdo de nivel de servicio)

- El área de Sistemas debe identificar los servicios y equipos críticos de su responsabilidad.
- La empresa debe contar con proveedor de soporte técnico para servicios y equipos críticos con personal competente para eventos críticos.

4.15. Ventanas de mantenimiento con afectación de servicios

- Todo evento de mantenimiento o intervención preventiva o correctiva que impacte en la continuidad de los servicios de correo electrónico, canales de internet o aplicaciones internas debe ser programado con anticipación procurando el menor impacto en la operación.
- Las emergencias, imprevistos o no controlables por el personal del área de Sistemas serán atendidas con el criterio de urgencia por el Técnico en Sistemas, de igual manera se activarán los escalamientos con los proveedores que corresponda para solucionar los incidentes en el menor tiempo posible.

4.16. Retiro de equipos oficinas

- El área de Sistemas deberá elaborar el acta de salida, cuando algún bien informático de (computadores, portátiles y periféricos) requiera ser trasladados fuera de las instalaciones, por motivo de garantía, reparación o evento.

- Si algún equipo informático de cómputo escritorio, portátil o periférico es trasladado por el usuario a oficinas distintas al lugar asignado, oficinas externas o foráneas para realizar sus labores, dicho bien estará bajo resguardo del responsable que retira el equipo y el pase de salida quedará a consideración del área de sistemas para su autorización u visto bueno.

- El usuario que ingrese equipos de su propiedad a las instalaciones de Global de Seguridad Zomac Ltda, es responsable de la información almacenada en el mismo, y deberá mantener la privacidad, integridad y respaldos de la misma sin ser esto responsabilidad del área de sistemas.

5. RESPONSABILIDADES

5.1. El área de Sistemas es la responsable de:

- El seguimiento y administración de las políticas de Tecnología de Información y Comunicaciones.
- La asignación y distribución de los equipos de cómputo.
- La administración y asignación de los servicios informáticos de la compañía.
- Elaboración y ejecución anual del plan de mantenimiento preventivo para los equipos de cómputo.

5.2. Son responsabilidades del usuario:

- Cumplir los procedimientos internos y las políticas de control y seguridad.
- Administrar las cuentas y claves de acceso hacia los diferentes servicios y sistemas internos.

- Notificar inmediatamente al área de Sistemas cualquier uso no autorizado de su cuenta, o cualquier intrusión de seguridad conocida.
- Usar los servicios con fines institucionales.
- Analizar cualquier archivo o programa obtenido a través de Internet o Correo Electrónico con software antivirus.
- No utilizar el Correo Electrónico corporativo en suscripciones a listas que saturen la capacidad de almacenamiento del buzón o para fines personales.
- Cambiar las contraseñas para ingreso a los sistemas cada 45 días, cuando éstos no exijan el cambio de manera automática.
- No abrir mensajes ni links de correos para los cuales se desconozca remitente.

6. CLÁUSULA DE CUMPLIMIENTO.

El área de Sistemas realizará acciones de verificación del cumplimiento de las políticas corporativa y estándares de seguridad informática.

Podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procedan. El mal uso de los recursos informáticos será reportados y se tomaran las acciones disciplinarias correspondientes.

Los líderes y responsables de los procesos establecidos en Global de Seguridad Zomac Ltda, deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares definidos y cualquier otro requerimiento de seguridad

JOHN FABIO PEÑA BERMEO
REPRESENTANTE LEGAL
Fecha: 04/03/2025

CONTROL DE CAMBIOS

VERSIÓN	PÁGINA	DESCRIPCIÓN DEL CAMBIO	FECHA
1	Todas	Creación del documento	04/03/2024
2	Todas	Creación del documento	04/03/2025
Elaboró: Responsable del SIG		**Revisó y aprobó:** Gerente General	