POLITICA DE TECNOLOGIAS Y SISTEMAS DE INFORMACION CORPORATIVO

TERMINOS Y DEFINICIONES

Para cualquier duda sobre los términos que se mencionan en este documento y sobre recomendaciones adicionales de seguridad, favor de revisar los documentos complementarios "**Anexo B Definiciones**", "**Anexo A Sobre las sanciones**", "**Anexo C Recomendaciones de Seguridad Adicionales**".

ALCANCE

El presente manual de Lineamientos de Tecnologías y Sistemas de Información del Grupo Industrial Mexicano, S. A. de C.V. (Grupo GIM) aplica a todas las subsidiarias de este grupo industrial, así como, al propio GIM Corporativo (Matriz); además de que lo deberán de observar de manera inmediata cada una de las nuevas subsidiarias que sean adquiridas por GIM.

OBJETIVO

El objetivo de este manual, es estandarizar los lineamientos para las Tecnologías y Sistemas de Información y los formatos para la gestión de la misma, que aplicarán para el uso de recursos de Hardware, Software, Comunicaciones, nombre de usuario de red, así como cualquier servicio y recurso externo relacionado al mismo, que coadyuven a la seguridad e integridad de la información creada, recibida y trasmitida a través de colaboradores, proveedores y clientes del Grupo GIM, las subsidiarias de este grupo industrial, y las nuevas subsidiarias que sean adquiridas por Grupo GIM.

1.- DISPOSICIONES GENERALES DE TSI

1.1.- Los lineamientos internos de cada subsidiaria no podrán contraponerse a la Política y Lineamientos del grupo GIM corporativo.

1.2.- Es responsabilidad de los directores de las subsidiarias de Grupo GIM el proporcionar los recursos tecnológicos requeridos y necesarios al área de TSI corporativo de Hardware, Software, Comunicaciones, nombre de usuario(a) de red, así como cualquier servicio externo, que coadyuve a mantener y salvaguardar la información creada, recibida y transmitida en la red de datos GIM.

1.3.- Se define a la generación de información con recursos tecnológicos propiedad de Grupo GIM cómo el activo más importante de las subsidiarias pertenecientes a éste, y es prioridad del área de TSI corporativo el salvaguardarla con los medios y alcance presentes y futuros que le han sido y serán asignados.

1.4.- Es responsabilidad del área de TSI de las subsidiarias catalogar la información y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer las medidas de seguridad a aplicar con TSI Corporativo.

1.5.- Se define al aplicativo “Sistema de Inventario” desarrollado para el área de T.I. y utilizado por ésta, como medio de administración, registro y gestión de Hardware, Software, Comunicaciones, nombre de usuario de red, así como cualquier servicio y recurso externo utilizados en el grupo GIM y subsidiarias durante su período de vigencia.

1.6.- Es responsabilidad de TSI corporativo la definición, capacitación y operación de las actividades del personal de TSI asignado a cada una de las subsidiarias de Grupo GIM de acuerdo al perfil solicitado y requerido por el área de Recursos Humanos del Grupo GIM Matriz y/o las subsidiarias.

1.7.- Es responsabilidad del área de TSI de las subsidiarias, apoyar, revisar, difundir, actualizar, mejorar y aplicar los lineamientos establecidos en este grupo GIM.

1.8.- La definición de Hardware, Software y Comunicaciones, así como cualquier

servicio externo relacionado al mismo, será responsabilidad de TSI corporativo definirlo para todas las subsidiarias de Grupo GIM con la debida autorización.

1.9.- Todo requerimiento al área de TSI deberá ser realizado a través de la creación de una solicitud de soporte (ticket) ubicado en el menú de aplicaciones en la intranet, de acuerdo al alcance definido en el documento complementario "**Manual de Soporte**".

1.10.- Es responsabilidad del Comité de vigilancia interna el designar a un tercero capacitado y certificado, para revisar y auditar los procedimientos y actividades que se realizan por el área de TSI de grupo GIM y subsidiarias al menos una vez al año, con el fin de detectar vulnerabilidades que puedan atentar contra la seguridad de la información.

1.11.- Es responsabilidad del área de TSI el investigar, definir, adquirir y aplicar el surgimiento de nuevas tecnologías que coadyuven a la mejora de los procesos tecnológicos en la red de datos GIM, con la debida autorización.

1.12.- Es responsabilidad de T.I. Corporativo el **diseñar, configurar y administrar** la red de datos GIM que proporcione el mayor tiempo posible de forma continua la disponibilidad y seguridad del flujo de información y aplicativos existentes para la operación del Grupo Gim y Subsidiarias.

1.13.- Es responsabilidad de TSI corporativo el elaborar un directorio del personal de TSI de las subsidiarias pertenecientes a este grupo, así como del propio GIM Corporativo (Matriz).

1.14.- Es responsabilidad de TSI corporativo el elaborar un directorio de los proveedores de TSI de las subsidiarias pertenecientes a este grupo, así como del propio GIM Corporativo (Matriz), el personal de TSI de las subsidiarias deberá de proporcionar los datos necesarios para realizar la captura de los mismos en el Sistema de inventario.

1.15.- Todo equipo que tenga la capacidad de ser administrado bajo un usuario y contraseña que la contenga por default, deberá de ser actualizado con un nuevo usuario y contraseña que sustituya al original con los mismos privilegios para evitar riesgos de seguridad.

1.16.- Todo proveedor externo que requiera ingresar a los servidores de Grupo GIM y subsidiaras deberá de realizarlo mediante la herramienta de soporte remoto TEAMVIEWER y regirse a lo mencionado en el documento "**Lineamiento de**

seguridad de Información de GIM”, y que deberá estipularse en el contrato de servicios acordado.

1.17.- El no cumplimiento de los lineamientos y documentos complementarios, por parte de los usuarios de Grupo GIM será sancionado por el comité de vigilancia interna.

1.18.- Todas las actividades específicas definidas para el cumplimiento de esta política se realizarán en base a los lineamientos que se mencionan en la misma.

2.- SOBRE SEGURIDAD DE INFORMACIÓN Y EL ACCESO A LOS RECURSOS DE INFORMACIÓN

2.1.-Es responsabilidad de RH informar y solicitar al área de T.I. el alta, cambio o baja de usuario de acuerdo al llenado del documento "**Formato de creación y uso de nombre de usuario en red de datos GIM**" bajo el alcance definido en los documentos complementarios "**Lineamiento de creación y uso de nombre de usuario en red de datos GIM**" y **"Lineamiento de baja de nombre de usuario de red de datos GIM, ERP, Correo y aplicativos**" de acuerdo al perfil designado.

2.2.- Toda información generada, modificada o eliminada por medio de los recursos tecnológicos asignados por Grupo GIM es propiedad del mismo grupo y su alcance está definido en el documentos complementarios "**Lineamiento de recursos tecnológicos de la red de datos GIM**" y "**Lineamiento de Seguridad de Información GIM".**

2.3.-Los usuarios que eliminen y/o modifiquen información propiedad de Grupo GIM tal como archivos de trabajo de cualquier aplicativo, bases de datos, xml y pdf de facturación y contabilidad electrónica, buzón tributario, de forma tendenciosa ó de beneficio propio, será causa de rescisión de contrato laboral.

2.4.- Los accesos a áreas restringidas denominadas cómo SITE's sólo será realizado por el personal autorizado por el área de T.I. corporativo y de acuerdo con el alcance definido en el documento complementario "**Lineamiento de Acceso a los Centros de Datos GIM**".

2.5.- Los usuarios que sean separados de sus funciones y les haya sido asignado algún recurso de Hardware, Software, Comunicaciones, nombre de usuario(a) de red, así como cualquier servicio externo relacionado al mismo, deberán de entregar a Recursos Humanos un documento de no adeudo de(l)/los recurso(s) asignado(s), autorizado por el área de T.I. y obtenido del Sistema de Inventario realizando las acciones mencionadas en el documento complementario "**Lineamiento de baja de nombre de usuario de red de datos GIM, ERP, Correo y aplicativos**".

2.6.- Los permisos especiales para algún usuario cómo compras, contabilidad y

solicitudes de pago, será responsabilidad de la dirección de la entidad el definir el nivel jerárquico para asignar a la persona de soporte que realizará dichas actividades, se deberá recibir la solicitud por parte de dirección de la entidad con el llenado del documento complementario "**Formato de creación y uso de nombre de usuario en red de datos GIM**".

2.7.- T.I. Corporativo tiene el derecho de inspeccionar cuando considere necesario, sin previo aviso, toda la información almacenada en los recursos tecnológicos de la red de datos GIM de acuerdo al alcance definido en el documentos complementarios "**Lineamiento de archivos y carpetas compartidos en red de datos GIM"** y "**Lineamiento de Seguridad de Información GIM"**.

2.8.- Los empleados que requieran realizar sus actividades laborales de forma remota deberán de conectarse a través de una VPN asignada por el área de T.I. y que fue previamente solicitada mediante un requerimiento de soporte (ticket) y autorizada por el mismo medio y/o correo anexo al mismo, realizándolo únicamente del recurso de hardware y software que se le haya asignado, así como, el nombre de usuario(a) y contraseña de red de datos asignada.

2.9.- No está permitido habilitar una conexión VPN desde un equipo personal o de terceros, ya que el área de T.I. no tiene injerencia en el mismo y tampoco tiene el conocimiento de que cumpla con los requisitos de seguridad necesarios para la seguridad e integridad de la información del Grupo GIM y sus subsidiarias.

2.10.-El acceso a consolas de administración de servicios de proveedores, deberán de ser actualizados con una contraseña segura, de acuerdo a los requerimientos del **Lineamiento de creación y uso de nombre de usuario en red de datos GIM**, así como la habilitación de la doble autenticación en caso de que aplique.

2.11.- El acceso a los servidores y equipos de datos de Grupo GIM y subsidiarias deberá de realizarse a través de la herramienta de acceso remoto TEAMVIEWER con la licencia respectiva ya sea por administración interna y/o por proveedores externos que requieran el acceso por alguna actividad pactada de soporte, configuración, instalación y/o desarrollo, asimismo, es responsabilidad del proveedor el tener la licencia respectiva para poder ingresar y apegándose a lo mencionado en el documento "**Lineamiento de seguridad de Información de GIM"**.

3.- SOBRE NOMBRES DE USUARIO(A)S Y CONTRASEÑAS

3.1.- Es responsabilidad de T.I. corporativo la creación, eliminación, cambio y administración de nombres de usuario y contraseña asignados al empleado para el acceso a la red de datos GIM de acuerdo con el procedimiento definido en el documento complementario "**Lineamiento de definición de Nombre de usuario**", que deberán ser utilizados de acuerdo al alcance definido en el documento complementario "**lineamiento de creación y uso de nombre de usuario en red de datos GIM**"

3.2.- Los nombres de usuarios y sus respectivas contraseñas no pueden ser transferidas, prestadas o reveladas a terceros salvo ocasiones especiales siempre y cuando sea autorizado por quien corresponda. El transferir el nombre de usuario y la revelación de su contraseña sin previa autorización será sancionado según las acciones disciplinarias establecidas por el comité de vigilancia interna.

3.3.- El uso de contraseñas para obtener acceso a los recursos tecnológicos en la red de datos GIM o para codificar cualquier archivo o mensaje no implica que los usuarios deban tener una expectativa de privacidad en la información que estos hayan creado o recibido, alineándose a lo mencionado en el documento complementario **"Lineamiento de Seguridad de la información GIM".**

3.4.- Para mantener la seguridad de los nombres de usuario(a) y contraseñas, éstos están obligados a bloquear o cerrar la sesión de trabajo en la red en todo momento en que se encuentren fuera de su lugar de trabajo.

3.5.- La información estará segmentada por accesos explícitamente otorgados y autorizados por la persona propietaria de la información y aplicados por el personal de TSI, con la utilización del Nombre de usuario(a) y contraseña asignada apegándose a lo mencionado en el documento "**Lineamiento de seguridad de Información de GIM"**.

4.- SOBRE LA UTILIZACIÓN DEL CORREO ELECTRÓNICO (E-MAIL):

4.1.- La definición, creación y administración de las cuentas de correo electrónico es responsabilidad de TSI Corporativo bajo el alcance definido en el documento complementario "**Lineamiento de creación y uso de cuenta de correo electrónico**".

4.2.- La utilización para fines personales de la cuenta de correo electrónico no está permitido.

4.3.- Está prohibido facilitar y/o permitir el uso de la cuenta de correo electrónico a cualquier otra persona distinta del propio usuario al que fue asignada.

4.4.- TSI Corporativo se reserva el derecho de monitorear que la utilización de la cuenta de correo electrónico sirva para propósitos legítimos. TSI Corporativo utilizará diferentes herramientas de monitoreo (Hacking ético) para asegurarse de que todos los usuarios cumplan con las política establecida. La utilización inapropiada de la cuenta de correo electrónico será sancionada según las acciones disciplinarias establecidas por el comité de vigilancia interna.

4.5.- La configuración de la cuenta de correo electrónico en el celular personal se realizará únicamente cuando ya se haya aplicado la doble autenticación (MFA).

4.6.- Los usuarios que utilicen la cuenta de correo electrónico para acosar, difamar, discriminar o intimidar a un usuario interno ó externo, enviar bromas, propagandas, material obsceno, pornografía, cadenas de mensajes, solicitudes de productos, servicios de índole personal, delitos cibernéticos y virus, así como correos masivos que se consideran SPAM, ó robo de identidad, serán sancionados de acuerdo a las acciones disciplinarias definidas por el comité de vigilancia interna.

5.- SOBRE LA UTILIZACIÓN DE RECURSOS DE RED, INTERNET Y ARCHIVOS EXTERNOS

5.1.- Es responsabilidad de TSI corporativo el **estandarizar** los recursos tecnológicos a integrar en la red de datos GIM para mejorar la eficiencia de la misma.

5.2.- El acceso a internet a los usuarios será autorizado por la gerencia de la entidad y será monitoreado por T.I. corporativo de acuerdo al alcance mencionado en el documento complementario "**Lineamiento de acceso y uso de internet**", y auditado por el comité de vigilancia interna.

5.3.- La administración de las páginas web, videoconferencia, streaming y dominios de correo de internet, son responsabilidad del área de T.I. corporativo, ésta podrá apoyarse y/o delegar las funciones, sin que ello implique la pérdida de control de las mismas.

5.4.- Toda información que sea trasmitida por la red de datos GIM de acuerdo al alcance mencionado en el documento complementario "**Política de uso de archivos y carpetas en la red de datos GIM**", que pueda poner en riesgo su transmisión, por saturación a causa de sus volúmenes, sus protocolos, sus horarios, tendrán que ser solicitado y autorizado por T.I.

5.5.- El personal de T.I. tiene la autorización para aplicar el alcance mencionado en el documento complementario "**Lineamiento de uso de recursos de la red de datos GIM**", en el momento que detecte alguna falla que deteriore la eficiencia de la red de datos GIM.

5.6.- El área de T.I. realizará el respaldo de información contenida en los recursos tecnológicos de la red de datos GIM de acuerdo al alcance definido en el documento complementario "**Lineamiento de respaldo de servidores de la red de datos GIM**" para los equipos definidos como "CRITICOS" en el sistema de inventario de equipo de cómputo.

5.7.- Las conexiones externas a la red de datos GIM de los empleados deberán de realizarse a través de una VPN otorgada por GIM y equipos asignados por el mismo.

5.8.- El usuario deberá de evitar el conectarse a cualquier red pública con acceso a internet en la medida de sus posibilidades, para disminuir la probabilidad de robo de información e intentos de ciber ataques.

5.- SOBRE EL USO DE SOFTWARE y HARDWARE

1.- Todo usuario está obligado a firmar y respetar el documento anexo "**Acuerdo entre empresa y Usuario sobre el uso de software**"

2.- Todo software que se requiere para la realización de las funciones laborales de un usuario(a), deberá de ser requerido a través de una solicitud de soporte (ticket) al área de T.I. y autorizado por el Gerente directo para su adquisición.

3.- No esta permitido la utilización de software sin licenciamiento y gratuito que pueden poner en riesgo la información contenida en los equipos definidos como críticos en el sistema de inventario de equipo de cómputo.

4.- A los usuarios que se les sorprenda utilizando cualquier programa no permitido, sin la autorización expresa del gerente de la entidad y/o responsable designado por él, serán sancionados por el comité de vigilancia interna.

5.- Es responsabilidad del usuario informar al área de T.I. si se presenta algún aviso de actualización de sistema operativo o software en sus equipos asignados, para que se evalué la factibilidad de llevar a cabo su realización, o realización por requerimiento de proveedor.

6.- La asignación de Equipos (tipo y modelo) se realizará bajo solicitud y autorización del Director(a) de la entidad o responsable designado por él(ella), por la vía definida en el punto 1.6 de la sección "**Disposiciones generales de TSI**" al área de T.I.

7.- La asignación de equipos de cómputo y celulares será llevada a cabo por T.I. corporativo bajo solicitud y autorización del gerente de área de la subsidiaria o corporativo que corresponda y que por las labores del usuario se requiera, por medio de una solicitud de soporte (ticket) creado en la intranet.

8.- El equipo celular que finalice su contrato forzoso, pasará a ser propiedad del usuario asignado, en ningún momento lo devolverá a la entidad que presta sus servicios, siempre y cuando no sea separado de la misma.

9.- El usuario deberá de acatar las restricciones mencionadas en el documento "**Lineamiento de Seguridad de Información GIM**" referente al software contenido en el equipo y celular asignados.

10.- El numero de celular asignado al usuario, es propiedad del grupo GIM y subsidiarias y no cedera los derechos del mismo al usuario cuando este deje de prestar sus servicios en el grupo GIM y subsidiarias.

11.- Los usuarios no tienen permitido la utilización de dispositivos USB en sus equipos de cómputo asignado, podrán existir excepciones que deberán contar con la autorización del Gerente del área ya sea por las labores propias del puesto o por requerimientos de alguna autoridad gubernamental, solicitándolo mediante un ticket de soporte en la intranet, para tal caso, los dispositivos deberán de revisarse contra malware previamente.

12.- El Grupo GIM subsidiarias, repondrán al usuario el o los equipos de cómputo asignados en caso de robo, siempre y cuando sea autorizado por el director de la misma y el usuario haya presentado la denuncia correspondiente ante las autoridades competentes.

En tal situación las subsidiarias de grupo GIM se comprometen a pagar el arrendamiento del equipo robado y al final del mismo el 20% del valor de recuperación del equipo, así como el nuevo asignado.

13.- El Grupo GIM y subsidiarias tendrán la facultad de cobrar al usuario el equipo(s) de cómputo y celular asignado(s) en caso de daño por mal uso de acuerdo a revisión realizada por el área y proveedor de soporte según corresponda y por extravío, cubriendo el faltante del arrendamiento pendiente, más el 20% del valor de recuperación del mismo.

14.- A la finalización el equipo en arrendamiento éste se facturará a las subsidiarias en el mes siguiente, si las subsidiarias del grupo GIM no desean que se les facture, deberán de informarlo por correo electrónico al área de T.I. para iniciar el trámite de devolución y se comprometen a reponerlos en el mismo período para no dejar al usuario sin recurso laboral, éste equipo deberá de cumplir las especificaciones determinadas por T.I. para poder agregar el licenciamiento de software requerido.

15.- Los equipos devueltos a grupo GIM corporativo, deberán de estar en funcionamiento, con accesorios y eliminador de corriente en buen estado, solamente se aceptará el desgaste natural de uso, de otra forma se cobrará dicho equipo a la subsidiaria y será decisión de grupo GIM corporativo venderlos a su discreción, siempre y cuando el equipo no haya sido reportado con fallas por el usuario asignado y/o el área de soporte, teniendo como prioridad el usuario asignado y de acuerdo a las condiciones establecidas, revisar anexo D y ver referencia en intranet tickets de soporte nos. 2023-77QIX, 2025-5LS07.

16.- El equipo de cómputo considerado como activo en el inventario y tenga 4 años ó más y para servidores, switch, no-breaks, y equipo storewize tengan 8 años o más, se considerará como obsoleto y deberá ser dado de baja del inventario de activos siguiendo el procedimiento y completando los formatos que tenga definido el área responsable de ello, y en caso de ser necesario, éstos equipos deberán de ser cubiertos antes de que se de baja el activo.

<table>
<tr><th colspan="2">CÓDIGO DEL DOCUMENTO</th><th>ELABORA:</th></tr>
<tr><td colspan="2">GIM-SIST-PO-DG-01</td><td>MTI. Alejandro Zapata</td></tr>
<tr><th>FECHA DE REVISIÓN</th><th>NIVEL DE REVISION</th><th>Control Documental</th></tr>
<tr><td>27/12/2024</td><td>5</td><td>N.A.</td></tr>
<tr><th colspan="2">DUEÑO DEL PROCESO / DEPARTAMENTO.</th><th>Autoriza:</th></tr>
<tr><td colspan="2">TECNOLOGÍAS DE LA INFORMACIÓN</td><td>Dr. Enrique Autrique Ruiz</td></tr>
</table>