Política de seguridad de la información

POL-TIN-18

Versión:01

Versión autorizada

Vigencia: Noviembre 2024.
Revisión: Noviembre 2025.

Autorizaciones

Dirección General	**Dirección Ejecutiva de Finanzas**

II. TABLA DE CONTENIDO

III. CONTROL DE CAMBIOS

Control de cambios			
Sección	Fecha de Vigencia	Modificación realizada	Responsable

IV. DEFINICIONES

Para efectos de la presente política, los términos y siglas del cuadro siguiente se deberán entender y aplicar como se definen a continuación:

Concepto	Definición
Acceso no autorizado	Consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de información
Base de datos	Serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.
Claves de acceso	Combinación de letras, números y signos para obtener acceso a un programa determinado.
Clasificación de Información	La información de Operbus se divide y clasifica en 5 rubros: Secreta, Confidencial, Interna y Pública, a continuación, su definición: - PÚBLICA. Información de dominio público, cuya divulgación no conlleva riesgos legales ni operativos, y puede ser compartida libremente por cualquier Colaborador. - USO INTERNO. Información generada por la operación de Operbus y sus subsidiarias, accesible para Directivos y Colaboradores y personas externas debidamente autorizadas. La divulgación o uso no autorizada de esta información puede acarrear riesgos o pérdidas leves para Operbus. - CONFIDENCIAL. Información estratégica, incluyendo sin limitar, listas de clientes de Operbus y sus Subsidiarias, sus métodos de negocios, sus métodos de relaciones públicas, de organización, de procedimientos operativos, de información financiera, “know-how”, de asistencia técnica, de secretos industriales de métodos y controles internos, planeación de negocios, proyecciones financieras, estrategias de mercado, y marketing, sea que esta haya sido marcada o no con la leyenda de “Información Confidencial” o que se encuentre o no en un soporte material, y la cual sólo puede ser conocida y utilizada por un grupo de Colaboradores o personas autorizadas, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a Operbus. - RESTRINGIDA. Información altamente sensible que debe ser protegida para evitar divulgaciones, alteraciones o destrucciones que pudieran resultar en incumplimientos legales. Su acceso está limitado a un grupo selecto de Directivos, y cualquier divulgación no autorizada puede acarrear graves consecuencias a Operbus.

Concepto	Definición
Clasificación de Información (Continuación)	- SECRETA. Información crítica, cuya divulgación o uso no autorizados podría ocasionar pérdidas graves a Operbus. Su acceso está restringido a un número muy limitado de Directivos. Cada Dirección funcional de la Empresa es responsable de clasificar y gestionar su información de acuerdo con estas categorías, determinando los niveles de acceso y los permisos de uso correspondientes, en cumplimiento con las leyes y regulaciones aplicables
Colaboradores	Es el personal de Operbus, S.A. de C.V. y Filiales que presta sus servicios internamente, independientemente de su condición contractual laboral.
Correo Basura o SPAM	Correo Electrónico que se envía en forma masiva con la finalidad de divulgar, establecer cadenas, promover o vender alguna idea, concepto o producto diferente a los propósitos de Operbus.
Correo Electrónico	Herramienta utilizada para realizar transferencias de información (Archivos de texto, imágenes, hojas de cálculo, etc.); es decir, envío y/o recepción de mensajes a través de los sistemas electrónicos bajo los cuales opera una red (Internet e Intranet).
DBA	Profesional responsable de la administración, mantenimiento y seguridad de bases de datos. Sus funciones principales incluyen la instalación y configuración de sistemas de gestión de bases de datos, la supervisión del rendimiento, la realización de copias de seguridad y restauraciones, la implementación de políticas de seguridad y acceso, así como la optimización de consultas y el diseño de esquemas de bases de datos. El DBA garantiza que los datos sean accesibles, seguros y estén organizados de manera eficiente para satisfacer las necesidades de Operbus.
Directivos	Director General, Director Ejecutivo de Finanzas, Director Ejecutivo de Ventas y Desarrollo de Producto y el personal con categoría laboral de Director y de Gerente de área conforme a la estructura vigente y autorizada de Operbus, S.A. de C.V. y Filiales.
Información	Conjunto de datos organizados y procesados que tienen significado y relevancia para el receptor. Puede presentarse en diversas formas, como texto, números, imágenes o sonidos, y su valor radica en su capacidad para proporcionar conocimiento, facilitar la toma de decisiones y mejorar la comprensión de un tema o situación.
Internet	Red global de computadoras interconectadas que permite la transmisión de datos y la comunicación entre dispositivos en todo el mundo. Funciona mediante un conjunto de protocolos estándar, conocidos como TCP/IP, que facilitan el intercambio de información.
ITIL	Acrónimo de Biblioteca de Infraestructura de Tecnologías de Información (Por sus siglas en inglés).

Concepto	Definición
Intranet	Red privada que utiliza tecnologías de Internet para compartir información, recursos y servicios dentro de una organización. A diferencia de Internet, que es accesible públicamente, la intranet está restringida a los empleados o miembros de la organización y se utiliza principalmente para mejorar la comunicación interna, la colaboración y la gestión del conocimiento.
Mensajería instantánea	Servicio de comunicación que permite a los Usuarios enviar y recibir mensajes en tiempo real a través de internet. Esta forma de comunicación se caracteriza por su inmediatez y facilidad de uso, permitiendo conversaciones en texto, audio o video
Operbus / Empresa / Organización	Operbus S.A de C.V. y Filiales.
Personal externo	Personas distintas a Directivos y Colaboradores que por motivos de negocio colaboran con Operbus entre los que se encuentran clientes, proveedores, consultores, etc.
Proveedor de bienes	Entidad o empresa que suministra productos o mercancías a otras empresas o consumidores. Su función principal es abastecer a sus clientes con los artículos necesarios para sus operaciones, ya sea para la venta al por menor, el uso interno o la producción de otros bienes.
Proveedor de servicios	Entidad o empresa que ofrece servicios a otras empresas o consumidores. Estos servicios pueden abarcar una amplia variedad de sectores y actividades, incluyendo, pero no limitándose a: • **Tecnología de la información** (Consultoría, desarrollo de software, soporte técnico) • **Telecomunicaciones** (Servicios de internet, telefonía) • **Logística** (Transporte, almacenamiento) • **Marketing** (Publicidad, relaciones públicas) • **Financieros** (Contabilidad, asesoría fiscal) • **Servicios profesionales** (Consultoría, asesoría legal)
Responsable de la información (Continuación)	Persona o entidad designada para gestionar, proteger y supervisar el uso de la información dentro de Operbus. Sus funciones principales incluyen: 1. **Clasificación y organización**: Determinar cómo se clasifica y organiza la información, asegurando que sea accesible y esté adecuadamente protegida. 2. **Seguridad**: Implementar políticas y procedimientos para salvaguardar la información contra accesos no autorizados, pérdida o daño. 3. **Cumplimiento legal**: Asegurar que el manejo de la información cumpla con las leyes y regulaciones pertinentes, como las de protección de datos 4. **Capacitación**: Proporcionar formación a los empleados sobre las mejores prácticas para el manejo de la información y la importancia de la seguridad. 5. **Supervisión**: Monitorear el uso de la información dentro de la organización y tomar medidas correctivas cuando sea necesario.

Concepto	Definición
Seguridad TI	Conjunto de políticas, procedimientos, herramientas y prácticas diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas informáticos de Operbus.
Usuario	Persona que utiliza un sistema, servicio o producto, especialmente en el contexto de tecnologías de la información y comunicación. Los Usuarios pueden interactuar con software, hardware, aplicaciones web, plataformas de redes sociales y otros recursos digitales

V. ANTECEDENTES

Es un hecho irrefutable que la información en conjunto con los procesos y sistemas que hacen uso de la misma, se han constituido con el paso de las décadas en activos importantes para cualquier organización sin importar, su giro, naturaleza, tamaño, capital, número de personal, etc.; es por ello por lo que su confidencialidad, integridad y disponibilidad, principalmente de aquella catalogada como sensible y/o confidencial resulta generalmente esencial para garantizar la continuidad operativa y funcional y con ello mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos a corto, mediano y largo plazo.

Con base en la premisa anterior y considerando que los niveles de terrorismo tecnológico y ataques que los sistemas sufren diariamente a nivel internacional, todas las organizaciones independientemente de su giro o fines, así como de sus sistemas de información, están expuestas a un elevado número de amenazas que aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a sus activos críticos de información a diversas formas de fraude, espionaje, sabotaje, vandalismo, etc. Los virus informáticos, el hacking o los ataques de denegación de servicio son algunos de los ejemplos más comunes y conocidos; sobre el particular, resulta de capital importancia que las organizaciones consideren la ocurrencia de riesgos y de incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización, así como aquellos provocados accidentalmente por catástrofes naturales o fallos técnicos.

Adicionalmente, el cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno y la protección adecuada de los objetivos del negocio para asegurar su cumplimiento, son algunos de los aspectos fundamentales en los que un sistema de gestión de seguridad de la información debe tener en cuenta para la adecuada gestión de las organizaciones.

Por lo expuesto, Operbus emite la presente política misma que tiene carácter obligatorio para los Directivos, Colaboradores y terceros externos a quienes resulte aplicable.

VI. OBJETIVO

Establecer un marco sólido para la gestión de la seguridad de la información en Operbus, garantizando que se sigan las mejores prácticas en la protección de datos, alineadas con **ITIL en su versión vigente** como un marco de buenas prácticas para la gestión de servicios de tecnología de la información y comunicaciones (TIC´s), para mitigar riesgos y asegurar la continuidad del negocio, de tal manera que:

a. Sea debidamente protegida la confidencialidad, integridad, disponibilidad, eficiencia, efectividad y confiabilidad de la información de Operbus de cualquiera de sus clientes, socios de negocio, Directivos, Colaboradores y cuando sea procedente del Personal externo en general.

b. Se desarrolle y se mantenga vigente una cultura empresarial de seguridad informática y de la información orientada a la identificación y análisis de riesgos, y

c. Se establezcan con claridad los roles y responsabilidades de los Directivos, Colaboradores y terceros relacionados en materia de seguridad de la información.

VII. ALCANCE

La presente política aplica a los procesos de definición, formalización implementación y operación relacionados con la seguridad de la información de Operbus, sistemas, aplicaciones y procesos que manejan datos.

La presente política dejará sin efecto cualquier disposición verbal o escrita que en la materia objeto de la misma se hubiese aplicado en forma previa a su entrada en vigor.

Su observancia es obligatoria para Directivos y Colaboradores, así como para contratistas y terceros que manejen o accedan a información crítica, así como para todas las áreas e Operbus que intervengan en forma directa o indirecta en dichos procesos.

VIII. NORMATIVIDAD RELACIONADA

Normativa relacionada (Documentos, políticas, procedimientos)	
Nombre del documento	**Área emisora**
Código de Ética y Conducta.	Dirección General
Reglamento Interior de Trabajo	Gerencia de Recursos Humanos

IX. LINEAMIENTOS

Son políticas de Operbus, las siguientes:

A. Disposiciones de carácter general

El presente apartado contiene las disposiciones de carácter general que se deben observar en materia de seguridad de la información.

1) Se encuentra estrictamente prohibido el uso de toda información que:

   a. Viole o infrinja los derechos de cualquier persona, incluidos los derechos de autor.
   b. Pueda ser percibida por un receptor como difamatorio, engañoso, abusivo u ofensivo.
   c. Constituya una amenaza, acoso o riesgo.
   d. Afecte de forma adversa el desempeño o disponibilidad de los servicios establecidos en la presente política.

e. Contenga cualquier virus, componente dañino o datos contaminados.
f. Contenga cualquier publicidad, promoción u ofrecimiento de productos o servicios para fines comerciales distintos a los de Operbus.
g. Consista en Correo basura.
h. Contenga pornografía, temas religiosos, bélicos, Torrents y descargas ilegales, apuestas, extremistas, anonimato o proxy, aplicaciones y software no oficiales.
i. Difame u hostigue

2) La creación de una cuenta de Usuario deberá ser solicitada por el personal adscrito a la Gerencia de Recursos Humanos, jefe Inmediato o bien, el propio Usuario; ¥ las aplicaciones o servicios a utilizar deberán ser autorizados por el Gerente o Director del área y considerando el Vo. Bo. del Director Ejecutivo de Finanzas, siguiendo para el efecto el procedimiento vigente en la materia.

3) Para las aplicaciones de internet abierto y de Mensajería instantánea, cada Usuario deberá justificar el uso de este servicio en el desarrollo de sus actividades y en pleno apego a política o procedimiento que corresponda.

4) Por defecto todos los perfiles de Internet que tenga Operbus deberán buscar bloquear los sitios conocidos como maliciosos, de spam o con Malware.

5) Por solicitud de la Gerencia de Recursos Humanos, se deberán cancelar inmediatamente los privilegios de acceso de aquellos Usuarios que dejen de laborar en Operbus.

6) Toda la información generada en las aplicaciones y servicios que se regulan en la presente política por Directivos y Colaboradores de la Empresa y Personal externo son propiedad de Operbus

7) Los servicios que se regulan en la presente política son de uso estrictamente laboral, razón por la cual el Usuario no deberá utilizarlos para el desarrollo de ningún proceso o negocio diferente al de la Empresa, para atender asuntos personales, diversión, ni para actividades que estén prohibidas por cualquier ley o reglamento aplicable.

8) Para tener acceso a los servicios de Correo Electrónico, Internet, Intranet y Mensajería Instantánea, equipo de telecomunicaciones, equipo de cómputo y celular, el Directivo o Colaborador deberá seguir los procedimientos que se determinen para su asignación, así como aceptar y firmar el formato de responsiva que determine Operbus.

9) Las cuentas y contraseñas asignadas al Usuario son personales e intransferibles, por lo que deberá manejarlas con carácter estrictamente confidencial y por ningún motivo dejarlas a la vista y/o compartirlas.

10) Se deberán establecer mecanismo(s) para que después de una inactividad de la computadora de 10 minutos se active automáticamente el protector de pantalla con contraseña de acceso. En caso de que el Usuario deje su equipo desatendido deberá bloquearlo previamente a que se separe del mismo.

11) Queda estrictamente prohibido el envío de información secreta, confidencial o de uso interno, por los medios que se regulan en la presente política hacia afuera de las

instalaciones la Empresa, o bien, a personal que no tenga privilegios para su uso, sin la autorización correspondiente de personal debidamente facultado conforme a lo que se establece en la presente Política.

12) Los Directivos, Colaboradores, contratistas y en general, Personal externo, no deberán tomar información clasificada como secreta, confidencial o interna sin que exista justificación válida para el uso de esta y ello se encuentre formalizado en documento con validez legal.

13) En caso de que se requiera entregar alguna información clasificada como secreta, confidencial o de uso interno a Personal externo, deberá estar plenamente justificado y contar con la aprobación de personal facultado así como suscribir contrato de confidencialidad previamente, debiendo el titular del área solicitante informar al área de TI respecto a la entrega de la información.

14) En los casos en los que por razones propias de los procesos de negocio de Operbus se requiera ejecutar trabajo remoto (actividades en casa o en un lugar ajeno a la organización) se deberán aplicar las disposiciones establecidas en la presente política.

15) Se encuentra estrictamente prohibido a cualquier persona tomar fotografías o grabar videos de las instalaciones y/o centros de cómputo de Operbus sin la autorización expresa del Director General, Director Ejecutivo de Finanzas o del Director de TI quienes se encuentran facultados para emitir la autorización correspondiente.

16) Toda persona que ingrese a las instalaciones de la Empresa (Clientes, proveedores, terceros, etc.) que porten equipo de cómputo o electrónico y que vayan a utilizar durante su estancia, deberán registrarlo previo a su ingreso en el área de Seguridad y Vigilancia, de lo contrario, el equipo se deberá quedar bajo resguardo en la misma.

B. <u>En materia de uso de Correo Electrónico</u>

El presente apartado contiene las disposiciones que se deben observar en materia de uso de Correo Electrónico.

1) No está permitido a los Usuarios que tengan asignada una cuenta de Correo Electrónico de Operbus o filiales, el envío de Correo basura o de programas de distribución libre (screen savers, juegos, cadenas, utilerías, ejecutables, fotos, presentaciones, música y videos o cualquier otro no relacionado con la actividad propia de cada puesto).

2) El Usuario es responsable de los mensajes que envía, así como de cuidar de los correos que reciba, el remitente y los documentos anexos y en su caso, deberá reportar al área de TI cualquier posible correo dudoso, toda vez que este podría contener un programa maligno.

3) La información enviada por este medio no debe contener de manera enunciativa más no limitativa las siguientes: referencias pornográficas, bromas, invitaciones a eventos no relacionados a las actividades de su responsabilidad de trabajo, suplantación de cualquier tipo o violaciones de derecho de autor.

4) Toda información que se genere a través de correo electrónico de Operbus por sus Directivos y/o Colaboradores, será considerada propiedad de la Empresa.

5) La capacidad máxima de envío de un correo electrónico y sus archivos adjuntos será determinada de acuerdo con la política que establezca el área de TI para este propósito

6) El Usuario será el responsable de validar la cuenta de correo destinataria, en especial cuando envíe información clasificada como Secreta, Confidencial o de Uso interno.

7) La información que se encuentre clasificada como Secreta o Confidencial que requiera ser transmitida por medios de comunicación públicos o correo electrónico deberá necesariamente utilizar un esquema de cifrado con el fin de proteger su confidencialidad e integridad.

8) Los Usuarios con derecho al servicio correo electrónico en los equipos de telefonía celular proporcionados por Operbus y por lo tanto de sincronía con los mensajes de este tipo son: Directores, Gerentes y personal autorizado, siendo responsabilidad de estos configurar una contraseña de acceso al dispositivo.

   Es necesario que en el caso de que sufran el robo o extravío del equipo de telefonía celular, lo reporten al área de TI, a su Jefe inmediato y a la Gerencia de Recursos Humanos y posteriormente entregar el mismo día del suceso, salvo que exista justificación, el acta de robo levantada en el Ministerio Público.

C. <u>En materia de acceso a Internet e Intranet</u>

El presente apartado contiene las disposiciones que se deben observar en materia de acceso a Internet e Intranet.

1) Los Usuarios con acceso autorizado a Internet e Intranet serán responsables de revisar la seguridad y veracidad de cada sitio en el acceso a páginas bancarias de Internet que requieran datos bancarios, número de tarjetas, claves confidenciales, números de cuentas bancarias o cualquier tipo de referencia bancaria.

2) Sin excepción, la información obtenida a través de fuentes de Internet deberá ser verificada por el Usuario antes de ser utilizada para fines del negocio.

3) Se encuentra estrictamente prohibido que con un equipo propiedad de Operbus se tenga acceso a Internet por medio de dispositivos, software o conexiones no autorizados por la Dirección y/o Gerencia de TI dentro de sus instalaciones de Operbus o sus oficinas

4) Se encuentran estrictamente restringidos a los Usuarios de manera enunciativa más no limitativa, los sitios de contenido o descarga de:

   a. Software
   b. Redes sociales de acuerdo con su perfil
   c. Servicios de radio y/o televisión (Servicios en demanda)
   d. Programas "peer to peer" o alguna otra tecnología que permita el intercambio de archivos en volumen

e. Música y/o video
f. Material Pornográfico
g. Drogas
h. Trata de personas
i. Apuestas
j. Religión

5) En materia de Intranet, cada área de la Empresa deberá determinar qué tipo de información se deberá publicar, misma que deberá contar invariablemente con la autorización del Director correspondiente y de ser necesario con el Vo. Bo. de la Dirección General y/o de la Dirección Ejecutiva de Finanzas.

   Lo anterior bajo la premisa de que la información contenida en la Intranet o cualquier sistema interno autorizado es propiedad de Operbus.

D. <u>En materia de Contraseñas</u>

El presente apartado contiene las disposiciones que se deben observar en materia de Contraseñas.

1) Cada Usuario es responsable del resguardo de las contraseñas que utilice para accesar a los sistemas y/o los dispositivos que la Empresa le ha asignado, por lo que deberá cambiarla de manera inmediata si tiene algún indicio de que ha sido conocida por otra persona.

2) Los Usuarios deberán cambiar cada 90 (Noventa) días las contraseñas para el acceso al equipo de cómputo asignado, así como a las aplicaciones a las que estén autorizados; en el caso de que la aplicación lo permita, el área de TI deberá realizar los ajustes técnicos necesarios con el objeto de que estas emitan un recordatorio respecto a la necesidad de cambiar la contraseña.

3) Las contraseñas deberán ser robustas para evitar que sean vulneradas por lo que se deberán observar los siguientes puntos:

   No deberán:

   - ✓ Estar basadas en palabras de un diccionario, no importando el idioma.
   - ✓ Contener datos personales, como nombres, apellidos, fechas de nacimiento, números de teléfono, división donde se labora, etc.
   - ✓ Utilizar parte de la misma cuenta de Usuario (User Id).
   - ✓ Crearse a partir de una palabra, con el cambio de caracteres por símbolos o números.

     Ejemplo:
     - Cuenta de Usuario: jcarlosmartinez
     - Contraseña: jc4rl0sm4rt1n3z
   - ✓ Utilizar una secuencia de letras o números, por ejemplo12345, abcde.
   - ✓ Contener el mismo carácter de manera secuencial, por ejemplo: 2222 ó aabbcc.

   Una manera correcta de crear una contraseña es de la siguiente manera:
   - ✓ Longitud mínima de 8 caracteres.

- ✓ Contener al menos una letra MAYÚSCULA, una minúscula y un número.
- ✓ Diferente de las 3 últimas contraseñas.

E. <u>En materia de uso de dispositivos USB /DVD y Encriptación</u>

El presente apartado contiene las lineamientos para el uso de dispositivos USB/DVD.

1) Se encuentra restringida la conexión no autorizada de cualquier dispositivo o elemento de almacenamiento sin una autorización expresa y previa del Director General y/o Director Ejecutivo de Finanzas con comunicación al área de TI.

2) Los medios removibles de almacenamiento para que puedan ser utilizados por Directivos, Colaboradores y Personal externo (Contratistas y demás terceros) facultados en los sistemas de información y en plataforma tecnológica, deberán ser autorizados por el Especialista de Seguridad y el Director de TI de acuerdo con la política de autorización vigente en la Empresa.

3) Los medios de almacenamiento removibles como cintas, discos duros removibles y dispositivos USB, entre otros, que contengan información de la Empresa, deberán ser controlados y físicamente protegidos por el Usuario Responsable de la información que contengan.

4) Los discos duros de los equipos de cómputo deberán ser encriptados de acuerdo con el formato o esquema que para el efecto establezca la Dirección de TI con el objeto de evitar fuga de información en caso de robo o perdida.

5) Toda la información clasificada como Confidencial o Crítica deberá ser encriptada para su almacenamiento en las bases de datos con el objeto de evitar su mal uso.

F. <u>En materia de participación de Proveedores</u>

El presente apartado contiene las lineamientos para regular la participación de proveedores en los procesos relacionados con la seguridad de información de Operbus.

1) Los Proveedores podrán tener acceso a la información de Operbus previa firma del Acuerdo de Confidencialidad y No Divulgación donde se regulen los estatutos de Seguridad de la Información que deben cumplir y se encuentren debidamente contratados de conformidad con lo establecido en la Política General de Compras de la Empresa.

2) Los Proveedores que tengan acceso a la red y/o servicios Operbus, estarán sujetos a lo establecido en la presente política, y en el Acuerdo de Confidencialidad y No Divulgación y respetar cada uno de los lineamientos que le sean indicados por la Empresa.

3) Todos los contratos de servicio que se suscriban entre Operbus y Proveedores deberán incluir por lo menos los siguientes términos de seguridad:

   a. Especificación de los niveles de servicio aceptables e inaceptables.

b. Responsabilidades legales de ambas partes respecto a la protección de la información.
c. Roles y responsabilidades relacionadas, entre otros, con:
   Protección contra malware o (Programa Maligno).
   Respaldos.
   Controles criptográficos.
   Gestión de la Vulnerabilidad.
   Gestión de Incidentes.
   Verificación de cumplimiento técnico.
   Pruebas de seguridad.
   Auditoría.
   Controles de autenticación y acceso.
   Gestión de identidad y acceso.

d. Acuerdos para la transferencia de personal cuando sea apropiado.
e. Convenio de Confidencialidad.
f. Proceso de escalamiento y resolución de problemas.
g. Causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información y penalizaciones

G. <u>En materia de Equipos de Cómputo</u>

El presente apartado contiene las lineamientos para regular los aspectos específicos de los Equipos de Cómputo propiedad o bajo la administración de Operbus.

1) El área de TI será la encargada de generar el resguardo y recabar la firma del Usuario informático como responsable de los activos informáticos que se le sean asignados por Operbus para el desarrollo de sus actividades, mismos que deberá de conservar en la ubicación autorizada por la misma.

2) Los Usuarios tienen estrictamente prohibido instalar o desinstalar dispositivos y/o retirar las etiquetas de identificación de los Equipos de Cómputo sin la autorización expresa de la Dirección de TI, por lo que deberán solicitarlo a la misma en caso de requerir servicios como los referidos.

3) Es de suma importancia que el Usuario observe los siguientes puntos mientras opera el Equipo de Cómputo:

   a. No consumir alimentos o ingerir líquidos.
   b. Evitar colocar objetos encima del equipo o cubrir los orificios de ventilación
   c. Mantener el equipo informático en un entorno limpio y sin humedad.
   d. Asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

4) Se encuentra estrictamente prohibido que el Usuario abra o desarme los Equipos de Cómputo, exclusivamente el personal adscrito al área de TI tiene autorizado realizar esta función cuando se requiera.

5) Los Usuarios no deberán usar Equipos de Cómputo asignados a otras personas; si fuera necesario acceder al equipo de otro Usuario (mientras se encuentra fuera o

ausente), el Usuario que lo requiera deberá solicitar a través de correo electrónico al Área de TI previamente autorizado por la Dirección de su adscripción, la autorización correspondiente.

6) Los Usuarios deberán asegurarse de respaldar la información (OneDrive) que consideren relevante en los casos en que el Equipo de Cómputo sea enviado a reparación; posteriormente deberá solicitar un borrado seguro por parte del área de TI de aquella información sensible que se encuentre en el Equipo de Cómputo previendo la pérdida involuntaria de información derivada de proceso de reparación; invariablemente deberán solicitar la asesoría del personal del Área de TI quien deberá llevar un control de los eventos de borrado seguro en dicho equipo.

7) En el caso de eventos de mantenimiento de emergencia por fallo del Equipo de Cómputo, el Usuario deberá en primer lugar dar aviso al Área de TI para el resguardo de la información para que posteriormente se realicen las gestiones necesarias para hacer valida la garantía correspondiente.

H. <u>En materia de Usuarios</u>

El presente apartado contiene las lineamientos relacionados con las responsabilidades de los Usuarios de Equipos de Cómputo, cuentas de Correo Electrónico y cualquier dispositivo o cuenta asignada por la Empresa.

1) Las cuentas de Usuario y cuentas de Correo Electrónico son personales e intransferibles. Las contraseñas utilizadas son responsabilidad exclusiva de cada Usuario, lo que incluye cualquier acceso que involucre su cuenta, así como su confidencialidad y resguardo. En caso de que un Usuario tenga la sospecha de que su contraseña pudiera estar comprometida, deberá notificar inmediatamente dicho hecho al área de TI.

2) Cada Usuario tiene la responsabilidad de revisar los mensajes electrónicos que reciba y no abrir ningún Correo Electrónico cuyo remitente sea de dudosa procedencia. En caso de tener sospecha de un Correo Electrónico malicioso deberá notificarlo al área de TI para su revisión y atención.

3) Los Usuarios no deberán comprometer a Operbus mediante la utilización de los servicios que se regulan en la presente Política de manera enunciativa más no limitativa con actos de difamación, hostigamiento, suplantación de identidad, reenvío de cadenas de correo y compras.

4) En los casos de Usuarios que tienen a su cargo o responsabilidad a Personal externo, deberán establecer los mecanismos necesarios para garantizar el cumplimiento de la presente Política; asimismo, deberán informar al área de TI cuando el Personal externo deje de laborar para la Empresa.

5) En el caso de que se autorice a un Usuario el uso de cualquier dispositivo de almacenamiento de datos, deberá solicitar al área de TI realice el respaldo y/o el borrado seguro de la información almacenada en dicho dispositivo.

6) Todos los documentos que un Usuario envíe a impresión deberá recogerlos

inmediatamente; asimismo, ningún caso deberá dejar documentos internos, confidenciales o sensibles sin atender.

7) Los Usuarios deberán resguardar adecuadamente los documentos o medios de almacenamiento de datos que contengan información clasificada como Confidencial, Secreta o Sensible.

8) Cada Usuario será Responsable de la información que contenga en el Equipo de Cómputo asignado por la Empresa, así como de la que se genere con su uso.

9) Cada Usuario será responsable del cuidado y buen uso del o los equipos que tenga asignados(s) (PC o laptop, teléfono, tableta, etc.) y por lo tanto, responsable de los daños del activo que dicho equipo sufra por uso mal intencionado o negligente.

10) El Equipo de Cómputo o cualquier recurso de TI que sufra alguna descompostura por maltrato, descuido o negligencia por parte de un Usuario, éste deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

11) Los Usuarios no deberán realizar descargas o instalaciones de software no autorizadas o sin licencia. El área de TI es la única autorizada para su instalación y mantenimiento.

12) Los Usuarios deberán solicitar la instalación de aplicaciones o software al área de TI siguiendo el procedimiento en vigor correspondiente, para lo cual deberán contar con la autorización del Director del área en la que se encuentran adscritos.

13) Cada Usuario deberá solicitar al área de TI los respaldos que requiera sobre su información y la frecuencia con que dicho proceso se debe realizar.

I. <u>En materia de funciones de las áreas de TI</u>

El presente apartado contiene las lineamientos relacionados con las funciones que tienen bajo su responsabilidad las áreas que integran la Dirección de TI.

1) Las áreas que integran la Dirección de TI son las únicas que puede habilitar los accesos que hayan sido solicitados y autorizados para los servicios electrónicos de Operbus de conformidad con el procedimiento establecido para tal efecto.

2) Las áreas que integran la Dirección de TI son las responsables de monitorear el uso de los servicios de correo electrónico, Internet, Intranet, así como de reportar las fallas o afectaciones del servicio a sus Usuarios y Directivos correspondientes.

3) La eliminación de medios informáticos de almacenamiento que contengan Información clasificada como Confidencial, Crítica, Sensible o de Uso Interno, deberá ser llevada a cabo exclusivamente por personal autorizado adscrito a la Dirección de TI, y en estricto cumplimiento con los procedimientos documentados y aprobados por la Empresa para tales efectos.

4) TI es el área encargada de instalar el software necesario para la ejecución de los accesos solicitados por el Usuario y que le fueron autorizados de acuerdo con el número de licencias aprobadas.

5) Las áreas que integran la Dirección de TI son las responsables de mantener el antivirus actualizado para que toda información y software sean verificados y en caso de detección de virus, este sea eliminado.

6) Las áreas que integran la Dirección de TI son las responsables de activar el Firewall de cada equipo o el que traiga integrado el Antivirus a fin de disminuir los puertos abiertos que no sean utilizados por los Usuarios.

7) Las áreas que integran la Dirección de TI son las responsables de suspender / cancelar los accesos de los Usuarios que hayan sido reportados por la Gerencia de Recursos Humanos o de Seguridad de TI, como por ejemplo, el personal que dejó de laborar en la Empresa, respecto a los sistemas que tenga bajo su resguardo.

8) Encriptar los discos duros de los equipos de cómputo de acuerdo con la herramienta o esquema que designe cada empresa para este propósito

J. <u>En materia de funciones de la Dirección de TI</u>

El presente apartado contiene las lineamientos relacionados con las funciones que tiene bajo su responsabilidad la Dirección de TI.

1) La Dirección de TI, tendrá las siguientes responsabilidades:

   a. Coordinar el análisis de vulnerabilidades a los servicios de Correo Electrónico, Internet, PC's de manera periódica al menos 1 vez por año.

   b. Coordinar un respaldo de información cuando sea solicitado por el Director de las áreas funcionales de la Empresa.

   c. Mantener un registro de incidencias de seguridad a fin de contar con estadísticas de éstas, de prevenir y en su caso, corregir eventuales vulnerabilidades.

   d. Promover y vigilar el cumplimiento de los lineamientos y el uso adecuado de los servicios conforme a lo establecido en esta Política y en los documentos normativos específicos de la Empresa.

   e. Establecer los mecanismos de seguridad necesarios para mantener la seguridad en caso de trabajo remoto, teletrabajo o home office de acuerdo con los controles especificados.

   f. El acceso a la administración de las bases de datos está limitada a la Dirección y Gerencia de TI o administrador de bases de datos (DBA) por lo que la configuración de dicha Base de datos estará bajo su responsabilidad.

   g. El respaldo de la información, las bases de datos y las aplicaciones operativas, así como la frecuencia con la cual debe realizarse es responsabilidad de la Dirección y Gerencia de TI, debiendo llevarse por lo menos 1 vez a la semana o con la frecuencia que se determine en cumplimiento de la normativa que aplique en cada caso.

K. <u>En materia de manejo de Incidentes de Seguridad</u>

El presente apartado contiene las lineamientos relacionados con el manejo de Incidentes de Seguridad por parte de la Dirección de TI.

1) La Dirección de TI, deberá implementar las acciones que a continuación se enlistan para el manejo de Incidentes de Seguridad.

Detección y respuesta: Establecer un proceso para la identificación y notificación de Incidentes de Seguridad. Utilizar un sistema de gestión de incidentes (basado en ITIL) para documentar y resolver incidentes.

Análisis post-incidente: Realizar análisis de causa raíz y aplicar lecciones aprendidas para mejorar la respuesta y prevenir futuros incidentes.

Capacitación y Concienciación

Programas de formación: Implementar un programa de capacitación anual en seguridad de la información para todos los Directivos y Colaboradores.

Simulaciones de ataques: Realizar ejercicios de simulación de incidentes para evaluar la preparación y respuesta del personal.

Concienciación continua: Utilizar boletines y campañas informativas para mantener a los Directivos y Colaboradores informados sobre las mejores prácticas de seguridad.

Cumplimiento Legal y Normativo

Normativas aplicables: Cumplir con leyes y regulaciones locales e internacionales, como el Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) y la Ley de Protección de Datos Personales en Posesión de Particulares.

Auditorías regulares: Realizar auditorías de cumplimiento para asegurar que se sigan las políticas y se aborden las brechas.

Actualización continua: Establecer un proceso para incorporar mejoras basadas en nuevas amenazas, tecnologías y mejores prácticas.

X.- Cumplimiento y Supervisión

1) Los lineamientos contenidos en la presente política son de carácter obligatorio para los Directivos, Colaboradores y Trabajadores de Operbus a quienes resulten aplicables y la omisión o incumplimiento de éstos podrá ser objeto de las medidas disciplinarias que determine Operbus, mismas que podrán llegar incluso a la terminación de la relación laboral sin responsabilidad para la Empresa en términos de la fracción XI del artículo 47 de la Ley Federal del Trabajo; lo anterior, sin menoscabo de las acciones legales que en su caso, Operbus determine emprender.

2) La Gerencia de Auditoría Interna, cuenta con las facultades necesarias para verificar el cumplimiento de la presente política y proponer las recomendaciones para atender

los hallazgos que se deriven de las revisiones que realice, debiendo informar de ello a la Dirección General y a la Dirección Ejecutiva de Finanzas; todo lo anterior, de conformidad con lo que establecen las Normas de Auditoría Interna que regulan esta actividad profesional.

3) La Dirección de TI deberá mantener debidamente actualizada la presente política, de tal manera que su contenido se encuentre vigente y atienda al entorno y particularidades de Operbus en todo momento.

XI.- ANEXOS

Sin Anexos.