IVC CONTRATISTAS GENERALES S.A.

POLÍTICA DE SEGURIDAD DIGITAL

	NOMBRE	FIRMA	FECHA
REVISADO:	Ing. Francisco Argumedo Gerente TI		13/12/2024
APROBADO:	Ing. Ytalo Valle Pachas Gerente General		16/12/2024

Esta copia controlada es para uso interno de IVC CONTRATISTAS GENERALES S.A.

CONTENIDO

POLÍTICAS PARA EL USO DE EQUIPOS Y SEGURIDAD DE LA INFORMACIÓN

Las políticas expresadas en el presente documento tienen por finalidad dar a conocer los lineamientos para el buen uso, manejo, control y administración de los equipos y recursos informáticos de IVC CONTRATISTAS GENERALES S.A, de ahora en adelante IVC.

Los equipos y recursos informáticos son proporcionados por la empresa con el objeto de facilitar y optimizar su desempeño diario con otros miembros de la empresa, con los proveedores y con los clientes.

La asignación de equipos y acceso a los recursos informáticos de IVC. está condicionada a la aceptación de la presente política de uso:

I. GENERALES

1. El área de TI es responsable de la administración de los equipos y recursos informáticos de IVC, así también de dar a conocer los compromisos, normas y procedimientos que han adquirido al tener acceso a la información y a los sistemas utilizados por la empresa.
2. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO son los encargados de implementar y mantener las conexiones de las redes de datos internas y externas de la empresa.
3. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO brindarán mantenimiento y asesoramiento en el uso de los equipos y recursos informáticos de la empresa.
4. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO en coordinación con el área de TI, se encargarán de establecer los controles de datos fuente, los controles de operación y los controles de seguridad, con el objeto de asegurar la integridad y adecuado uso de la información que se genere en la empresa.
5. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO en coordinación con el área de TI y la administración, se encargarán de autorizar la adquisición y uso de equipos diseñados para el procesamiento, almacenamiento y transporte de la información (como: grabadoras de CDROM, DVD, discos duros externos, memorias USB, entre otros).
6. El área de TI con apoyo de EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE

SOPORTE TECNOLÓGICO establecerán un Plan Anual de Mantenimiento Preventivo y Correctivo de los equipos informáticos.

7. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO en coordinación con el área de TI de IVC, ubicarán las computadoras debiendo considerar lo siguiente:
   a. La zona debe ser la adecuada para un equipo de cómputo.
   b. Que no exista agua o goteras que puedan dañar el equipo de cómputo.
   c. La superficie sea de un escritorio ya sea de madera o de otro material, lejos de campos magnéticos para evitar que el equipo se recargue de iones.
   d. Prohibido colocar los equipos sobre lunas.
   e. Colocar los equipos lejos del calor o del fuego.
   f. Que sea de fácil acceso el encendido y apagado del equipo de cómputo.
   g. Estas consideraciones serán tomadas en cuenta por el usuario debiendo respetar estas normas de ubicación.

II. DEL USO Y CUIDADO DE LOS EQUIPOS INFORMATICOS

1. Los equipos informáticos son exclusivamente para uso en el ámbito laboral, bajo responsabilidad directa del usuario.
2. Los usuarios son responsables del adecuado uso y control de los componentes de los equipos informáticos que se le ha asignado y/o personales (propios) cuando se conecten a la red de IVC.
3. Los usuarios que instalen sin autorización software en sus equipos informáticos son responsables de los problemas técnicos y/o económicos que podrían ocasionar en el equipo instalado y en los demás equipos conectados a la red y de las licencias originales de software instalado.
4. El usuario, bajo ninguna circunstancia debe abrir los equipos informáticos y/o periféricos, retirar o cambiar componentes de los mismos, alterar o eliminar el software que se encuentra a su disposición, cambiar la configuración determinada a su entrega por el personal del área de Sistemas. En caso de incurrir el usuario en cualquiera de las situaciones señaladas será reportado por el área de RRHH y de Administración, solicitando una sanción correspondiente.
5. El usuario a quien se le haya asignado un equipo informático deberá seguir las pautas que se describen según componente:

2.1. El Teclado:

a. El usuario únicamente podrá efectuar Ia limpieza externa del teclado.
b. El usuario debe evitar manchar el teclado o el cable de este con cualquier clase de tinte.
c. El usuario debe evitar comer o beber sobre el teclado. Todo desperfecto que se origine por esta causa será de responsabilidad del usuario y su reposición será por cuenta del usuario responsable y determinada su correspondiente responsabilidad económica.
d. El usuario debe abstenerse de realizar maniobras sobre las partes internas del teclado. Las revisiones de los teclados son efectuadas por personal del área de Sistemas.
e. El usuario debe evitar tener cerca del teclado grapas y/o clips, que, de insertarse entre las teclas, pueden ocasionar cruces de función.
f. El usuario debe evitar colocar objetos sobre el teclado y apoyarse sobre este.
g. El usuario NO debe utilizar ningún tipo de material extraño para pulsar las teclas.

2.2. El CPU:

a. El área de Sistemas realizará periódicamente Ia limpieza del CPU y analizará y depurará los discos duros de los equipos mediante los procedimientos más convenientes.
b. El usuario deberá evitar materiales magnéticos cerca del CPU.
c. La parte posterior y los lados del CPU deben estar siempre libres para asegurar una ventilación mínima adecuada. El usuario NO debe apilar documentos, files de palanca, botellas o cajas sobre el CPU.

2.3. El Monitor

a. El usuario debe evitar colocar o pasar materiales magnéticos por Ia pantalla.
b. El usuario debe evitar manipular agresivamente los botones de graduación/ajuste del monitor.
c. Si el usuario va a limpiar la pantalla debe utilizar una franela seca para su limpieza.

2.4. El Mouse

a. El usuario NO deberá maniobrar ninguna de las partes internas del mouse, ni manipular incorrectamente el cable que sirve de conexión al CPU.
b. El usuario NO deberá golpear el mouse.

2.5. Las Impresoras:

a. El usuario NO debe limpiar las impresoras. Solo EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO hará la limpieza y mantenimiento de las impresoras.
b. El usuario debe evitar manipular las partes de las impresoras mientras se encuentra apagada y cuando este imprimiendo.
c. La colocación de las cintas, cartuchos de tinta y tóner se realizará de acuerdo a las instrucciones del Manual de usuario de la impresora.
d. La configuración de las impresoras a todo el personal de la empresa es responsabilidad de EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO.
e. La colocación de papel en los respectivos suministradores de hoja se realizará de acuerdo a Ia especificación de cada bandeja.

III. DE LA RED LAN

1. La Red LAN (Local Área Network – Red de Área Local) es el conjunto de componentes que permite la interconexión de los equipos informáticos a fin de que los usuarios puedan compartir y utilizar los recursos informáticos implementados.
2. Una red LAN, está compuesto por los servidores (donde se almacena toda Ia información de los sistemas y servicios informáticos), medios de conexión (cableado, tarjetas de red y distribuidores de conexiones), y las estaciones de trabajo (equipo de cómputo del usuario).
3. El área de Sistemas es la encargada de la administración de la Red LAN de la empresa.
4. El usuario podrá acceder a la red LAN de la empresa, desde su equipo de cómputo autorizado e instalado en la oficina principal.
5. Además de los recursos ofrecidos para el equipo de cómputo asignado a cada

usuario, estos contaran con los recursos que les ofrece la red, tales como: compartir impresoras, compartir archivos, almacenar archivos en los servidores, correo electrónico y acceder a Internet. Estos recursos deben ser usados racionalmente y sin perjudicar a la empresa y a otros usuarios.

6. Para el uso de los recursos de la Red en cada área de la empresa, se cuenta con diferentes equipos que llevan la señal hasta cada estación de trabajo (Switches, Router, cable de fibra óptica, cables UTP cat. 6, UTM, entre otros).
7. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO son responsables del mantenimiento de las cuentas del usuario de red (usuario de dominio) y el establecimiento de las normas de seguridad para Ia protección de Ia información almacenada en los servidores.
8. El usuario que haga mal uso de los recursos de Ia Red, será inhabilitado en su cuenta de dominio y en su cuenta de correo.

IV. DE LOS SERVICIOS INFORMATICOS

1. Los lideres de procesos solicitan Ia asignación de un usuario en Ia Red (usuario de dominio) y acceso a los servicios informáticos, administración aprobara el acceso.

2. Los tipos de acceso que solicitarán podrán ser todos o algunos de lo que se detallan a continuación:
   - Acceso a los sistemas de la empresa.
   - Acceso a la información de la empresa.
   - Acceso al correo electrónico.
   - Acceso a Internet
3. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO, después de la aprobación de administración deberán resolver la solicitud de acceso para el nuevo usuario, en un plazo no mayor a 24 horas.
4. Los lideres de procesos solicitan ampliación o bloqueo de los accesos del usuario cuando sea necesario, cuando deje de laboral en la empresa, o ya no se requiera.
5. Los usuarios son responsables de las actividades que realicen con sus accesos y permisos, como su identificación de usuario de dominio y contraseña y a los servicios informáticos. En caso el usuario ceda su acceso a cualquier servicio informático a otra persona, sigue siendo responsable de las actividades que este tercero realice.

V. DEL SERVICIO TECNICO

1. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO brindarán el mantenimiento técnico preventivo y correctivo a los equipos y recursos informáticos de Ia empresa.
2. Los Usuarios que soliciten aI proveedor mantenimiento de los sistemas informáticos, Ia atención de un servicio técnico, deberán coordinar con el área de TI y una vez concluido el servicio técnico, el usuario y su jefe deben reportar la conformidad respectiva. El mantenimiento de los sistemas informáticos tiene como plazo máximo 48 horas después de recibida la orden de servicio técnico.

VI. DEL CORREO ELECTRONICO

1. El servicio de correo electrónico es para uso exclusivo de envío y recepción de información concerniente a las funciones que el usuario cumple para la empresa. Por lo tanto, esta información forma parte del Activo de Ia empresa.
2. El uso frecuente y continuo, exige tener sujetos estos programas a controles y revisiones técnicas y mantenimiento de forma periódica por el área de Sistemas.
3. La cuenta de correo electrónico es de uso exclusivo del usuario asignado, por tanto, bajo ninguna circunstancia este podrá usar Ia cuenta de otro usuario.
4. Al culminar la relación laboral del/la colaborador/a los mensajes tendrán una permanencia no mayor de 60 días desde Ia fecha de entrega o recepción de estos. Superada Ia fecha de permanencia, los mensajes serán respaldados y el dominio será eliminado, salvo que por razones de función amerite su almacenamiento en el servidor por más tiempo del establecido, lo que deberá ser coordinado previamente con el área de TI
5. Las consecuencias posibles, por el contenido de un correo, son de responsabilidad exclusiva del usuario de Ia cuenta de correo.
6. La administración y gestión de la clave de una cuenta de correo electrónico, es responsabilidad del área de TI.
7. El área de TI/ Administración permite el acceso al correo electrónico corporativo, mediante la coordinación con EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO desde su servidor de correo y como cliente el Outlook o a través de un navegador de Internet, para lo cual se utiliza el Outlook Web Access (OWA), que estará disponible para todos los usuarios de correo.
8. El tamaño máximo permitido para el envío de un correo electrónico lo determinara EL/LOS EL PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE

TECNOLÓGICO. No se aplicarán restricciones a la recepción de correo. En caso de que la función de algunos usuarios requiera de una mayor capacidad del máximo permitido, esto deberá ser coordinado previamente con el área de TI.

9. En caso el usuario reciba correos no deseados o de procedencia dudosa, deberá seguir el instructivo “Correos con posible Spam o Virus” o notificar del hecho al área de Sistemas.
10. Los mensajes de correo deberán tener un asunto (subject) que refleje o resuma su contenido.
11. Las notificaciones corporativas también podrán efectuarse mediante correo electrónico corporativo.

VII. DEL INTERNET

1. El Internet tiene por finalidad brindar información de carácter global y de interés múltiple; es una plataforma que permite obtener información a través de las diferentes redes de información.
2. Debido a la proliferación de virus informáticos y del consumo de ancho de banda, se restringe el uso del servicio de Internet para el acceso a servidores externos, redes sociales (Facebook, Instagram, TikTok, YouTube), videos, música, páginas de descarga de archivos no relacionadas a las funciones laborales.
3. El área de Sistemas está facultada para la Implementación de Sistemas de Información, auditoria de Sistemas, diseño y gestión de páginas Web, y de servicios utilizados por los usuarios.

VIII. DE LA SEGURIDAD DE LA INFORMACION

1. La información generada y almacenada en los equipos de cómputo y servidores de la Red, son de propiedad de la empresa.
2. Para información de los Proyectos de la empresa, el responsable de autorizar el acceso a los usuarios es de la gerencia. Para otro tipo de información el responsable de autorizar el acceso es los lideres de áreas, las cuales corresponde dicha la información.
3. El usuario que encuentre alguna irregularidad en los equipos de cómputo y/o con los servicios informáticos, deberá comunicarlo inmediatamente al área de Sistemas, a fin de que tome las medidas correctivas.
4. Cada usuario que utilice una estación de trabajo cuenta con una contraseña para el acceso a la red LAN y una cuenta de correo electrónico, estos servicios

son considerados confidenciales y de uso exclusivo del usuario asignado; las contraseñas serán gestionadas por el área de TI de IVC. Esta contraseña es de carácter personal e intransferible, cuya vigencia y/o caducidad serán gestionadas por los lideres de área, bajo responsabilidad y aprobación del área de TI y administración.

5. Todo usuario que haga uso de los Sistemas que utiliza la empresa a los que se ha dado acceso y permisos, se hará responsable de Ia información que manipule durante su uso.
6. Los lideres de las áreas, deberán informar al área de TI el personal que ingresa y deja de laborar en su área. Asimismo, en un plazo no mayor de 48 horas, el área del de TI deberá coordinar se brinde o restringa los accesos y servicios informáticos asignados a dicho personal, según corresponda.
7. Dependiendo el área las copias de respaldo de Ia información se realizan en el NAS.
8. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO gestionarán y coordinarán el almacenamiento y custodia de los discos duros de respaldo de los servidores principales de Ia empresa.
9. EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO podrán desinstalar cualquier producto de uso no oficial, personal y/o software que no cuente con Ia licencia correspondiente.
10. Todos los equipos de cómputo contarán con un antivirus corporativo que se mantendrá actualizado permanentemente.

IX. DE LAS RESPONSABILIDAD DE LOS USUARIOS

1. AI inicio de las labores, el usuario debe verificar que los cables y los componentes estén completos y conectados en forma correcta, caso contrario informara aI área de Sistemas inmediatamente.
2. Evitar desconectar bruscamente el equipo de cómputo o mover el equipo de cómputo más allá de Ia distancia permitida por los cables o apagar el estabilizador (si aplica) sin antes haber apagado Ia máquina.
3. En caso de interrupción de fluido eléctrico, se debe: Apagar todos los equipos de cómputo: monitor, CPU e impresora.
4. Restablecido el fluido esperar aproximadamente 15 minutos para encender los equipos de cómputo.
5. No se debe dejar los monitores encendidos por más de 12 horas.

6. No abrir por ningún motivo el case del CPU.
7. No abrir por ningún motivo las cubiertas de las impresoras.
8. No golpear el teclado ni el mouse del equipo de cómputo.
9. Respetar los equipos asignados a otras personas, incluyendo los que están fuera de la empresa.
10. Corresponde a todo usuario, garantizar la confidencialidad e integridad de la información generada y obtenida, tomando las precauciones debidas.
11. El usuario solo podrá utilizar la cuenta del usuario y contraseña que se le ha asignado para tener acceso a sistemas y recursos de la red.
12. Los usuarios deben proteger la seguridad de acceso a los Sistemas de Información y a la red de la empresa.
13. Los usuarios deben proteger la confidencialidad e integridad de la información almacenada.
14. Los usuarios deben mantener su clave de acceso en un lugar confiable a fin de que otros usuarios no puedan utilizarla.

X. DE LAS PROHIBICIONES Y RESTRICCIONES DE LOS USUARIOS

1. Queda prohibido utilizar los equipos y recursos informáticos de la empresa para beneficios personales.
2. Queda prohibido instalar en los equipos informáticos de la empresa, software no licenciado o no autorizado por el área de Sistemas.
3. Queda prohibido almacenar en los equipos informáticos de la empresa, instaladores de software ilegal.
4. Queda prohibido almacenar en los equipos informáticos de la empresa, información de otro usuario sin el consentimiento expreso del propietario.
5. Queda prohibido el uso de equipos informáticos de la empresa a personal ajeno a la empresa.
6. Queda prohibido ejecutar programas ya sean propios u obtenidos a través de Internet o correo electrónico u otro medio.
7. Queda prohibido Instalar servidores web, servidores de correo y clientes de correo electrónico.
8. Queda prohibido la manipulación de los equipos de comunicación de la empresa como router, firewall, switchs, antenas Wifi, cableado, etc. por parte de los usuarios.
9. Queda prohibido ingresar y utilizar a páginas Web con contenido obsceno,

vulgar, para adultos o pornográfico, a servicios P2P, a servicios de correos gratis, a servicios de apuestas en línea, a páginas que no tengan que ver nada con las labores desempeñadas dentro de la empresa.

10. Queda prohibido ingresar y utilizar páginas Web que permitan obtener contraseñas de software o sistemas informáticos.
11. Queda prohibido ingresar y utilizar páginas Web a fin de descargar software Ilegal o no licenciado.
12. Queda prohibido almacenar en los equipos de cómputo en cualquier formato digital (videos, imágenes, documentos) información que atenten contra Ia moral en perjuicio de terceros.
13. Queda prohibido el uso de Internet para cualquier actividad que sea lucrativa o comercial de carácter individual, así como el uso del servicio de correo corporativo para propósitos fraudulentos, publicitarios o para Ia propagación de mensajes no relacionados con Ia actividad Laboral.
14. Queda prohibido acceder mediante el servicio de Internet asignado a contenidos que puedan estar relacionados con servidores generadores de SPAM o VIRUS, o que puedan contener programas que permitan romper las claves de acceso, u otros que puedan utilizarse con fines no lícitos o no autorizados y dañinos tanto para Ia empresa como para terceros.
15. Queda prohibido utilizar equipos y recursos informáticos (hardware y software) a fin de obtener las claves de acceso de otro usuario o recurso que no se le ha dado acceso, esto ameritará una sanción de acuerdo con el grado de responsabilidad, Ia misma que se elevará aI área de Administración.
16. Queda prohibido utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro de Ia empresa.
17. Queda prohibido utilizar los equipos y recursos informáticos de Ia empresa para ganar acceso no autorizado a redes y sistemas remotos.
18. Queda prohibido provocar deliberadamente el mal funcionamiento de los equipos y servicios informáticos, esto ameritara una sanción de acuerdo con el grado de responsabilidad.
19. Queda prohibido la suplantación o uso no autorizado de Ia cuenta de correo de otra persona, esta ocurrencia será considerada como falta grave y esto ameritará una sanción de acuerdo al grado de responsabilidad, Ia misma que se elevará aI área de RRHH/ Administración.

20. Queda prohibido ingresar a la cuenta de correo de otro usuario y leer los correos de ese usuario, esta ocurrencia será considerada como falta grave y esto ameritará una sanción de acuerdo con el grado de responsabilidad, la misma que se elevará al área de RRHH/ Administración.
21. Queda prohibido iniciar o continuar cadenas de mensajes que innecesariamente aumenten el espacio en los buzones electrónicos y el tráfico en la red.
22. Queda prohibido suscribirse a las listas de interés que no guardan relación con la actividad laboral asignada.
23. Queda prohibido, dejar botellas, tazas, vasos con agua u otro líquido, cerca de los equipos informáticos que pueden ocasionar un cortocircuito y mucho más grave un incendio.
24. Queda prohibido, dejar botellas con agua, papeles, documentos, files de palanca, cajas, cartones, al costado del CPU que pueden ocasionar un cortocircuito y mucho más grave un incendio.

XI. DE LOS SERVIDORES

1. Solo el personal de EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO están autorizados a entrar en la sala de servidores.
2. Todos los servidores tendrán un mantenimiento preventivo periódico.
3. La manipulación y el traslado de los servidores es responsabilidad del área de TI, se debe tener mucha precaución al transportar los equipos.
4. Todos los servidores contaran con un antivirus corporativo que se mantendrá actualizado permanentemente.
5. No se debe golpear ni dejarla caer los servidores, ni dejar bebidas u otro líquido cerca de los servidores.
6. Si se va el fluido eléctrico, de inmediato las baterías de respaldo conectado a los servidores entraran en funcionamiento. Si el fluido eléctrico se va en días y horas laborales, el personal de EL/LOS PROVEEDOR/ES DE LOS SERVICIOS DE SOPORTE TECNOLÓGICO apagarán todos los servidores de manera correcta.