POLÍTICA DE SEGURIDAD INFORMÁTICA

MR-IT-001

01 de diciembre de 2022

Yesid Moncada T.

Realizado Por: **Jefe de Sistemas**
Fecha de Revisión: 01/12/2022

Aprobado Por: **Gerente**
Fecha de Aprobación: 01/12/2022

Revisado Por: **Directora S.I.G.**
Fecha de Revisión: 01/12/2022

TABLA DE CONTENIDO

PROPÓSITO

El presente documento tiene como finalidad dar a conocer las Políticas de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de COOPEVIAN.

INTRODUCCIÓN

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de Políticas de Seguridad Informática adecuadas.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de COOPEVIAN en materia de seguridad.

Este documento se encuentra estructurado en varias políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que se detallan en el presente documento.

OBJETIVO

Estas Políticas de Seguridad Informática se encuentran alineadas con el estándar ISO/IEC: 27002.

Establecer y difundir las Políticas de Seguridad Informática a todo el personal de COOPEVIAN, para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados.

ALCANCE

El documento define las Políticas de Seguridad Informática que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos de COOPEVIAN.

JUSTIFICACIÓN

El área de sistemas de COOPEVIAN, está facultada para definir las Políticas de Seguridad en materia informática.

SANCIONES POR INCUMPLIMIENTO

El incumplimiento al presente documento podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

BENEFICIOS

Las Políticas de Seguridad Informática establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información de COOPEVIAN.

1. POLÍTICA GENERAL

1.1. Política de Seguridad Informática

Las prácticas de seguridad informática de COOPEVIAN, deben garantizar un nivel apropiado de protección, confidencialidad (privacidad), integridad y disponibilidad de la información corporativa y todos los recursos tecnológicos, con base en directrices administrativas y las posibilidades que brinde la tecnología disponible.

Todo usuario que tenga asignado un activo o acceso informático se compromete a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de COOPEVIAN, así como el estricto apego al documento de las Políticas de Seguridad Informática para usuarios.

1.2. Responsabilidades del Área de Sistemas

a) Definir, implantar, divulgar y supervisar las políticas de seguridad informática y promover la incorporación de prácticas seguras en todas las áreas de COOPEVIAN, incluyendo la interacción con entes externos.

b) Evaluar permanentemente los riesgos, interpretar las directrices administrativas y analizar las condiciones de COOPEVIAN en relación con la seguridad informática.

c) Establecer tareas de monitoreo, que verifiquen la observación de las políticas de seguridad informática y permitan ejecutar acciones correctivas sobre las vulnerabilidades encontradas.

d) Velar por el correcto funcionamiento de la tecnología informática que se utilice en las diferentes áreas o procesos de la organización.

e) Definir estrategias y objetivos a corto, mediano y largo plazo.

f) Mantener la arquitectura tecnológica siempre actualizada y segura.

g) Controlar la calidad del servicio brindado.

h) Mantener el Inventario actualizado de los recursos informáticos.

i) Velar por el cumplimiento de las Políticas y Procedimientos establecidos.

j) Desarrollar, someter a revisión y divulgar a todo el personal por medio de (intranet, email, otros medios de comunicación) la Políticas de Seguridad Informática.

k) Programar y realizar capacitaciones al personal sobre el uso y manejo de las herramientas informáticas activas, con el ámbito de promover el mejoramiento continuo de la cooperativa.

1.3. Responsabilidades de los Usuarios

Es responsabilidad de los usuarios de COOPEVIAN quienes tengan asignados equipos, accesorios y aplicativos, cumplir a cabalidad la Política de Seguridad Informática establecida por el proceso de Sistemas de la organización.

a) Conocer y cumplir las políticas de seguridad informática establecidas dentro de la red local de COOPEVIAN.

b) Proteger y usar apropiadamente la información sobre la cual tienen acceso y los equipos informáticos entregados como dotación para el desempeño de las labores asignadas.

c) Asistir y aplicar las capacitaciones recibidas bien sean presenciales, escritas o virtuales, dictadas por el personal interno o externo con conocimientos informáticos.

d) Informar al personal de Sistemas de COOPEVIAN, cualquier exposición o riesgo que involucre la seguridad de la información, ya sea real o potencial.

1.4 Acuerdos de Uso y Confidencialidad

Todos los usuarios de equipos y servicios informáticos de COOPEVIAN deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información de COOPEVIAN, así como comprometerse a cumplir con lo establecido en el documento de Política de Seguridad Informática.

1.5 Entrenamiento en Seguridad Informática

Todo Asociado o Empleado activo de COOPEVIAN, sea antiguo o nuevo, deberá:

Leer el documento de Política de Seguridad Informática de COOPEVIAN, el cual se encontrará disponible en la Intranet, enviado por correo electrónico o divulgado por cualquier otro mecanismo de comunicación, donde se darán a conocer las obligaciones para los usuarios y las sanciones que pueden aplicar en caso de incumplimiento.

1.6 Medidas Disciplinarias

Cuando el personal de Sistemas de COOPEVIAN identifique el incumplimiento al presente documento remitirá el reporte o denuncia al líder de cada proceso con copia al líder de Gestión Humana, para los efectos de su competencia y atribuciones.

2. POLITICAS ESPECÍFICAS

2.1.1. Acceso a la Información

a) Las autorizaciones para el uso de una aplicación y los datos relacionados son responsabilidad exclusiva del líder del proceso. Por lo anterior el obligatorio el Requerimiento por escrito en la plataforma definida como mesa de ayuda.

b) Las situaciones especiales, que impliquen intervenir los archivos de producción de una aplicación, serán coordinadas con el líder de cada proceso e información correspondiente. Requerimiento por escrito en la plataforma definida como mesa de ayuda.

c) Los servidores de datos y los equipos serán protegidos de acceso no autorizado, mediante el establecimiento de derechos sobre discos y directorios. El personal de Sistemas de COOPEVIAN establecerá las políticas de seguridad correspondientes.

d) Se implementará el doble factor de autenticación (MFA) a los servidores, aplicativos o plataformas que dispongan de esta segunda capa de seguridad, para evitar el acceso no autorizado.

2.1.2. Acceso a los equipos

Para prevenir el acceso remoto a su equipo, el usuario debe realizar permanentemente prácticas seguras, tales como:

a) Eliminar las opciones de compartir recursos. (Archivos, Carpetas, entre otros).

b) Compartir sus directorios o carpetas, cuando sea necesario, utilizando claves y solo a usuarios específicos.

c) Asegurar la confidencialidad de sus contraseñas, está prohibido la divulgación de la contraseña de acceso a la red o aplicativos a los demás compañeros de trabajo o terceros, sin autorización del líder del proceso o del personal de sistemas.

d) Cerrar la sesión del equipo asignado o acceso a Escritorio Remoto.

e) Bloquear la sesión de Windows en el momento que se ausente del equipo asignado.

2.1.3. Cuentas de Usuario y Contraseñas

a) Toda novedad de ingreso de personal nuevo o modificación al personal administrativo antiguo, que requiera la asignación de equipos y acceso a aplicativos, debe ser reportada por el líder del proceso al personal de Sistemas; justificando los servicios y herramientas que el nuevo usuario necesitará para el desempeño de sus funciones. Esta solicitud debe de ser realizada por medio de la aplicación SISMAC y se debe de adjuntar el formato (**MR- FT-009 FORMATO CREACION DE USUARIO.docx**) totalmente diligenciado.

b) Toda novedad de retiro de personal de COOPEVIAN, debe ser reportada por el mismo líder del proceso o por la dirección del proceso de Gestión Humana al personal de Sistemas; a más tardar el día de retiro. El personal de Sistemas se encargará de eliminar o deshabilitar las cuentas y accesos a la red, correo y demás aplicativos internos y externos, así como de dar destino a los equipos de cómputo que se liberen, de común acuerdo con el líder de proceso. Esta solicitud debe de ser realizada por medio de la aplicación SISMAC y se debe de adjuntar el formato (**MR- FT-009 FORMATO CREACION DE USUARIO.docx**) totalmente diligenciado.

c) Todo usuario debe tener una identificación única en la red, con su respectiva contraseña, la cual no puede ser transferida a otra persona sin previa autorización del área de Sistemas.

d) Toda aplicación debe tener un sistema de registro y autenticación que asegure el acceso autorizado a la información.

e) La contraseña es personal e intransferible y no debe ser compartida, escrita, ni revelada. Las actividades que se realicen con su identificación son responsabilidad del propietario de la cuenta.

f) En caso de que algún compañero necesite acceder a un equipo tecnológico no asignado y no tenga conocimiento previo de la contraseña, debe de solicitar la debida autorización escrita al líder del proceso para que esta persona comparta la contraseña de ingreso a la red y/o aplicativos o solicitar al personal de Sistemas por medio de un ticket, el cambio de contraseña.

g) La contraseña debe tener un tamaño mínimo de 14 caracteres, y de preferencia que combine letras en mayúscula y minúscula, números y caracteres especiales. Debe evitar al máximo que sean adivinadas por la simplicidad de la contraseña y que no incluyan palabras o frases obvias, tales como, nombres y apellidos propios del usuario, meses del año o fechas especiales.

h) Si el sistema no obliga al cambio de contraseñas a los 120 días como se especifica en la matriz en el campo periodicidad, es responsabilidad del usuario realizar este cambio periódicamente.

i) Una vez digitada la contraseña, no se debe dejar la estación de trabajo sola y desbloqueada, si va a ausentarse bloquee la pantalla **(CTRL + ALT + SUPR + BLOQUEAR EQUIPO)** o con la combinación de teclas (**Windows + L**).

j) Los usuarios no deben intentar acceder ilegalmente o sin autorización a los sistemas de información de COOPEVIAN, ni a los servidores, ni equipos de comunicaciones, de lo contrario estaría vulnerando la seguridad de estos, lo que se cataloga como delito informático y lo cual conlleva a ser sancionado disciplinariamente.

2.1.4. Comunicación de políticas y procedimientos de uso y manejo de cuentas de usuario, contraseñas y aplicativos internos

Mediante el proceso de capacitación e inducción al personal administrativo (Asociados y Empleados), se informa de las políticas, procedimientos de uso y manejo de los diferentes aplicativos y acceso a los mismos, por medio de envío de TIPS de seguridad informática por correo electrónico, capacitaciones presenciales, virtuales, publicación en la Intranet o envío de SMS.

2.1.5. Sanciones disciplinarias por mal manejo de políticas y procedimientos informáticos

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo con el reglamento emitido por COOPEVIAN.

Las sanciones pueden ser desde una llamada de atención hasta la terminación del contrato laboral dependiendo de la gravedad de la falta, malicia o perversidad que ésta manifiesta.

Corresponderá al área de Gestión Humana con autorización de la Gerencia y el Consejo de Administración, hacer las propuestas finales sobre las sanciones a quienes violen las políticas de seguridad informática de la Cooperativa.

Todas las acciones en las que se comprometa la seguridad de la infraestructura física y lógica de los sistemas de información de COOPEVIAN y que no estén previstas en esta política, deberán ser revisadas por el área de Sistemas y ejecutar una acción de mejora sobre la Política de Seguridad Informática y posterior a esto publicar y divulgar a todo el personal de la Cooperativa.

En cuanto a los daños a la infraestructura tecnológica y de información, Interceptación ilegítima de sistemas informáticos o red de telecomunicaciones, suplantación de sitios Web para capturar datos personales, acceso abusivo a un sistema informático y demás delitos informáticos, se aplicará la **Ley 1273 de 2009**, incurriendo a las sanciones que con ella conlleva en cada uno de sus artículos que la componen.

A continuación, se enlista algunas de las acciones **no autorizadas** por la Política de Seguridad Informática y las cuales conducen a impartir Sanciones Disciplinarias:

a) Hacer copia de la información de COOPEVIAN en dispositivos de almacenamiento externos personales tales como: (Correo electrónico, almacenamiento en la nube, memorias USB, celulares, discos duros externos, entre otros), sin previa autorización escrita del jefe inmediato y del personal de Sistemas.

b) Instalar Software sin autorización. De ser necesario instalar algún software en los equipos de cómputo de COOPEVIAN, se debe de realizar el requerimiento solicitando la debida autorización al personal de Sistemas con copia al líder del proceso. (Este requerimiento debe de realizarse por el aplicativo SISMAC).

c) No se debe de acceder a los equipos de cómputo no asignados y sin previa autorización por la persona encargada del mismo, líder del proceso o del personal de Sistemas.

d) Los equipos asignados como herramientas de trabajo se deben de mantener y/o devolver completos y en óptimas condiciones tal cual como fueron entregados por el personal de Sistemas de COOPEVIAN.

e) No se permite destapar, manipular o cambiar los componentes de los equipos asignados, sólo el personal de Sistemas de COOPEVIAN son los autorizados para realizar cambios, mantenimientos o reparaciones a los equipos asignados para actividades propias del cargo.

f) Se debe informar con anticipación al proceso de Sistemas el ingreso y retiro de Asociados y/o Empleados para actualizar el estado de los usuarios de validación en la red y demás aplicativos de COOPEVIAN.

g) Propagar virus en la red de COOPEVIAN y no tomar las precauciones de analizar los dispositivos de almacenamiento externos (Correo electrónico, almacenamiento en la nube, memorias USB, celulares, discos duros externos, entre otros).

h) Suplantar los usuarios y contraseñas de acceso a la red y aplicativos internos sin previa autorización por el personal de Sistemas.

i) Eliminar información de los equipos de cómputo clientes, servidores de datos, almacenamiento en la nube y unidades compartidas de red destinadas para el trabajo colaborativo en red de la organización.

j) Dejar máquinas o equipos tecnológicos encendidos o conectados al toma corriente de energía después de terminar la jornada laboral y fines de semana, de ser necesario se debe de solicitar la autorización al líder del proceso con copia al personal del proceso de Sistemas.

k) Autorizar a terceros o extraños el uso y manejo de los equipos clientes, servidores o software sin previa autorización por parte del líder del proceso o personal del proceso de Sistemas.

l) Compartir o divulgar contraseñas de acceso a las redes de Internet Wi-Fi de las sedes de COOPEVIAN sin previa autorización del personal del proceso de Sistemas.

2.2. Política de Compra y Licenciamiento de Software

a) Sólo la Gerencia y el área de Sistemas puede autorizar la adquisición e instalación de software en los equipos de COOPEVIAN. Se exceptúa de la anterior disposición, el software de los equipos, que se adquieren con los proyectos de circuitos cerrados de televisión (CCTV). Estas compras se harán siguiendo lo establecido en el Procedimiento de Compras.

b) Todo el software instalado en COOPEVIAN debe estar respaldado por una licencia que garantice que fue adquirido legalmente. Esta licencia debe estar a nombre de COOPEVIAN, no se permiten licencias a título personal, sólo se exceptúa el software cuya licencia es de libre distribución e instalación.

c) Todos los productos de software que se utilicen deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

d) El proceso de Sistemas promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

e) Las licencias de software deben estar bajo custodia del proceso de Sistemas, quien garantizará su adecuada protección, control y administración.

f) Se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario y/o el software gratuito.

g) Está prohibido hacer copias o usar los diferentes aplicativos, plataformas o datos de COOPEVIAN para fines personales.

h) Está prohibido el uso de los equipos de cómputo de COOPEVIAN para fines personales, estos están configurados y designados únicamente para el uso de actividades propias de la organización.

2.2.1 Desarrollo de Software Interno

a) Los aplicativos desarrollados por personal interno o externo, que sea parte del proceso de Sistemas, o sea liderado por ésta, son propiedad intelectual de COOPEVIAN.

b) Está prohibido hacer copia del código fuente de los aplicativos de COOPEVIAN para el uso personal.

2.2.2 Derechos de Propiedad Intelectual

Está prohibido por las leyes de derechos de autor y por COOPEVIAN, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por COOPEVIAN y ser publicados y divulgados en Internet u otros medios de comunicación para fines personales.

2.3. Política de Hardware

2.3.1. Compra e instalación de equipos de cómputo

Solo la Gerencia o representante legal suplente, puede autorizar la adquisición o compra de computadores, equipos de red y periféricos para el uso en COOPEVIAN.

2.3.2. Equipos de Terceros

a) El ingreso de equipos tecnológicos, tales como, (Portátiles, Tablet, entre otros) de terceros debe ser coordinado por el responsable de la visita y reportar al Jefe de Seguridad y Porterías para su registro y control de activos.

b) El ingreso y salida de estos equipos debe reportarse al personal de las Porterías de la sede en que se encuentre.

c) El uso de estos equipos tecnológicos se debe de involucrar en todas las políticas de seguridad informática de COOPEVIAN, incluyendo todas las condiciones de seguridad, confidencialidad y protección de la información de COOPEVIAN.

d) La conexión de equipos de terceros a la red de COOPEVIAN (Cableada o Inalámbrica) debe hacerse con autorización y supervisión de personal del proceso de Sistemas.

2.3.3. Renovación de equipos tecnológicos

a) Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación tecnológica.

b) La recomendación por parte del proceso de Sistemas es que estas renovaciones se realicen entre 3 y 5 años de uso de los equipos, basándose en las recomendaciones del fabricante.

c) Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para mejorar el desempeño de sus actividades, estas deberán realizar una consulta al personal de Sistemas a fin de que se seleccione el equipo adecuado. Sin el visto bueno del personal de Sistemas y la Gerencia no podrá autorizarse una orden de compra.

2.3.4 Daño de equipos

El equipo de cómputo o cualquier recurso de tecnología de información que sufra algún daño por maltrato, descuido o negligencia por parte del usuario, este deberá ser gestionado con el jefe directo y la Gerencia y regirse a lo que indique los estatutos o reglamento interno de trabajo, para definir si el asociado o empleado debe de asumir el valor de la reparación o reposición del recurso tecnológico dañado.

2.4. Sistemas de comunicación y cómputo

a) La red de datos, Internet, correo electrónico y equipos de cómputo, están destinados para las actividades laborales y como tal deben utilizarse de manera productiva. Debe evitarse la utilización de estos sistemas de comunicación con propósitos de entretenimiento o diversión.

b) Está prohibido el uso de los sistemas y herramientas mencionados para propósitos ilegales que atenten contra los intereses de COOPEVIAN, sus clientes, proveedores, empleados y/o asociados.

2.5. Seguridad de Redes

a) Solo el personal de Sistemas está autorizado para la instalación, configuración, y traslado de los equipos tecnológicos y redes de comunicaciones.

b) Todo usuario que tenga acceso a los equipos de comunicación de red y/o servidores, debe estar autorizado por el personal del proceso de Sistemas.

2.6. Acceso Remoto

a) No está permitido el uso de módems personales (3G, 4G o 5G) en computadores que estén conectados a la red local (LAN) de la organización; a menos que sea debidamente autorizado por el personal de Sistemas. Todas las comunicaciones de datos deben efectuarse a través de la red local de COOPEVIAN.

b) Para tener acceso remoto a (Servidores, Conexión VPN, Team Viewer, AnyDesk, entre otros) a las aplicaciones y servicios de red de COOPEVIAN, se debe tramitar la correspondiente autorización del proceso de Sistemas.

c) Las personas que tiene acceso remoto a (Servidores, Conexión VPN, Team Viewer, AnyDesk, entre otros) a la información de COOPEVIAN, son responsables por la seguridad de la información con los mismos niveles de control requeridos dentro de la red local de COOPEVIAN.

d) No está permitido proveer o suministrar a terceros no autorizados, las cuentas de usuario o recursos informáticos de COOPEVIAN, como lo son (Usuarios de inicio de sesión y contraseñas).

2.7. Suite de Correo Electrónico

El derecho a tener y utilizar una cuenta de correo electrónico de COOPEVIAN, debe ser solicitado al proceso de Sistemas, con la correspondiente solicitud en la plataforma de mesa de ayuda SISMAC.

El usuario que disponga de una cuenta de correo de COOPEVIAN deberá de acatar los siguientes ítems:

a) La contraseña debe tener un tamaño mínimo de 14 caracteres, y de preferencia que combine letras en mayúscula y minúscula, números y caracteres especiales. Debe evitar al máximo que sean adivinadas por la simplicidad de la contraseña y que no incluyan palabras o frases obvias, tales como, nombres y apellidos propios del usuario, meses del año o fechas especiales.

b) Todas las cuentas de la suite de correo electrónico tendrán habilitado y configurado el doble factor de autenticación (MFA), esto para controlar el acceso no autorizado a las cuentas de correo.

c) El correo electrónico es una herramienta de trabajo por lo que NO está permitido utilizar el correo como aplicativo personal con fines políticos, religiosos, sentimentales, comerciales, juegos, redes sociales, ni ninguna clase de actividad mercantil.

d) Las comunicaciones deben ser breves, estilo telegráficas para evitar el congestionamiento de la red y el mal uso del tiempo del personal. Si es imprescindible enviar bastante información, porque el tema lo justifica se recomienda insertarlo como documento, ejemplo: Word, Excel, PowerPoint.

e) Solo se deben marcar como urgente los documentos que realmente los son.

f) Los correos deben ser correctamente dirigidos a las personas que requieran la información. Por ningún concepto se deben enviar correos generales que no son de interés general, como, por ejemplo: despedidas, agradecimientos, etc.

g) Se debe hacer buen uso de los contactos y grupos que contiene la libreta de direcciones de la suite de correo electrónico.

h) Hacer uso del remitente secreto con copia oculta de los contactos. "**CCO**". De esta forma evitamos que los correos de nuestros remitentes sean observados por terceras personas. Por ejemplo, el listado de correos de los clientes o asociados de la organización.

i) La información que se recibe de manera personal y confidencial por correo electrónico, no se puede rutear a otra persona, sin la autorización del remitente.

j) El uso de las cuentas de correo es privado y sus contraseñas confidenciales. Por ningún concepto se puede entrar a revisar la información dirigida a otra persona.

k) En forma general tratar de no imprimir los mensajes de correo, ya que esta herramienta fue creada para tener un archivo electrónico, agilizar las comunicaciones, descartar en la medida de lo posible el archivo tradicional y lograr un ahorro en papelería.

l) La persona que envía el mensaje de correo es responsable del contenido de este, debiendo considerar que la información vertida es irreversible.

m) El envío del mensaje de correo no libera al remitente de la responsabilidad de hacer seguimiento de las disposiciones impartidas.

n) Los correos no deben de sobrepasar el límite de tamaño permitido de recepción y envío cuando se adjunta algún elemento, el tamaño del correo se informará a través de correos electrónicos a todo el personal que maneje una cuenta de correo corporativo, ya que los tamaños pueden variar según la herramienta de correo que se maneje. Se deben de seguir las recomendaciones que indique el proceso de Sistemas por medio de TIPS en correo electrónico o en capacitaciones presenciales o virtuales.

o) Los usuarios deben de utilizar las herramientas de almacenamiento en la nube asignadas, según la suite que disponga la organización para dicha actividad, Por ejemplo, OneDrive.

p) Los usuarios deberán de utilizar la herramienta de comunicación "chat" organizacional destinada para la comunicación interna y trabajo colaborativo. Las herramientas de chat no organizacionales, tales como, WhatsApp, Telegram, Messenger, Signal, entre

otros, no serán soportadas o administradas por el personal de Sistemas de COOPEVIAN.

2.8. Internet

Los usuarios con el servicio de navegación a Internet aceptan que:

a) Serán sujetos de monitoreo de las actividades que realizan en Internet.

b) Saben que existe la prohibición al acceso de páginas no autorizadas.

c) Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.

d) Saben que existe la prohibición de descarga e instalación de software sin la autorización del personal de sistemas.

e) El uso de Internet es para el desempeño de su función y puesto en COOPEVIAN y no para propósitos personales.

f) Está prohibido compartir o divulgar las contraseñas de las redes Wi-Fi de las sedes de COOPEVIAN, exceptuando las redes Wi-Fi de INVITADOS.

g) El derecho a usar Internet (Cableado o Inalámbrico), a través de los computadores o Router Inalámbricos de COOPEVIAN, debe ser solicitado al personal de Sistemas, con la correspondiente aprobación escrita del jefe inmediato. Se debe de tener en cuenta que esto incluye la conexión a dispositivos móviles, tales como: celulares, Tablet, entre otros.

2.9. Redes Privadas Virtuales (VPN)

a) Los usuarios móviles y remotos de COOPEVIAN podrán tener acceso a la red interna privada cuando se encuentren fuera de la empresa en cualquier ubicación con acceso a una conexión a Internet segura y evitando las conexiones públicas o gratuitas, utilizando las redes privadas VPN habilitadas por el proceso de sistemas.

b) El personal encargado del proceso de sistemas serán los únicos autorizados de configurar el software necesario y asignar las contraseñas a los usuarios que cuenten con la autorización de la conexión VPN.

2.10. Conectividad a Internet

a) La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los Asociados y/o Empleados de COOPEVIAN tienen las mismas

responsabilidades en cuanto al uso de Internet dentro o fuera de las instalaciones. Esto aplica para equipos (Portátiles, Escritorio, Celulares, Tablet, entre otros).

b) La autorización se debe de solicitar directamente al personal de Sistemas.

c) El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall y/o Antivirus incorporado en la misma.

d) No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem externo.

e) Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

f) Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

g) El personal que se conecte a internet dentro de las instalaciones debe de cumplir las políticas de seguridad sobre la navegación de páginas no autorizadas.

h) Se prohíbe el uso de herramientas, componentes, plugins o software que salten las políticas internas de navegación Web, por ejemplo, programas como proxys o VPN de terceros.

2.11. Seguridad internet y dispositivos inalámbricos

Con finalidad de fortalecer la seguridad del acceso a internet y configuración a los Router inalámbricos se aplicarán las siguientes actividades:

a) Actualización del Firmware de los dispositivos (Switch, Router, AP, Módems) para mejorar la seguridad y funcionamientos de estos.

b) Analizar las posibles mejoras en la configuración para un óptimo funcionamiento y así brindar y garantizar conexión a Internet, por ejemplo, la segmentación por VLAN’s.

c) Cambiar los nombres de SSID y contraseña de acceso a los AP’s inalámbricos para evitar que vulneren estos y accedan a red interna de COOPEVIAN, estos cambios se deben realizar como mínimo cada 6 meses.

d) La contraseña de acceso a la conexión de Internet inalámbrico debe de ser solicitada al personal encargado del área de Sistemas por medio del software SISMAC y con copia al jefe directo o la Gerencia para su respectiva aprobación. Esta no será divulgada o

compartida por otros medios por política de seguridad informática y así evitar la filtración de la contraseña.

2.12. Restricciones y/o Prohibiciones de acceso a internet

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

a) El uso de programas para compartir archivos (P2P).

b) El acceso a páginas con cualquier tipo de contenido explícito de pornografía, violencia, música, redes sociales, chats, emisoras, streaming, juegos, entre otros sin previa autorización.

c) Uso de JUEGOS "**On Line**" en la red.

Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea son:

NIVEL 1: Sin restricciones: Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea, excepto páginas de contenido pornográfico.
NIVEL 2: Internet restringido y mensajería instantánea: Los usuarios podrán hacer uso de internet y servicios de mensajería instantánea, aplicándose las políticas de seguridad y navegación.
NIVEL 3: Internet restringido y sin mensajería instantánea: Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación.
NIVEL 4: El usuario no tendrá acceso a Internet ni a servicios de mensajería instantánea.

Todos los niveles tendrán permisos totales a la página Web, Intranet y demás aplicaciones internas que dependan de un navegador Web, tales como: Google Chrome, Mozilla Firefox, Internet Explorer, entre otros.

2.13. Política de los equipos

a) La configuración de hardware y software establecida por el proceso de Sistemas debe respetarse y sólo puede ser modificada por personal de esta.

b) Los equipos no pueden moverse o reubicarse, sin la correspondiente autorización del personal de Sistemas. El traslado de equipos fuera de COOPEVIAN requiere autorización escrita del líder de proceso o Sistemas.

c) Restringir el uso de Discos Extraíbles (Memorias USB, Discos Duros Externos, Memorias SD, MicroSD, Celulares, Tablet, entre otros) y unidades lectoras de DVD-CD. Esto a

través de las GPO desde el Servidor principal o restricciones a través de la consola del Antivirus utilizado o software DLP.

d) Los líderes de cada proceso definirán que equipos de cómputo son necesarios desbloquear los puertos USB, dependiendo de la necesidad o actividad que se necesite mayor velocidad y almacenamiento de información. Por ejemplo, el proceso de Medios Tecnológicos, para la copia de extracción de videos de los CCTV de peticiones por los clientes o fiscalía.

e) El personal que necesite almacenar o compartir información y dependa de los puertos USB, se reemplazará por el almacenamiento en la nube definido por el proceso de Sistemas de la Cooperativa, teniendo como base las recomendaciones y buenas prácticas para almacenar y compartir la información en la nube. Para este caso, deberán tener presente la política de retención de datos.

2.14. Política de equipos de impresión

La Cooperativa ha implementado un proyecto de arrendamiento de equipos de impresión, con el fin de promover el ahorro de papel y contribuir con el medio ambiente, iniciando una campaña y cultura con pensamientos más ecológicos y así minimizar al máximo la impresión innecesaria en COOPEVIAN. Para lograr dicho objetivo se deben de cumplir las siguientes normas:

a) El código de impresión es único e intransferible, esto quiere decir que no se debe de compartir o divulgar dicho código de impresión a compañeros de proceso o terceros.

b) Imprimir los documentos realmente necesarios para el proceso dentro de las funciones asignadas al cargo de cada usuario.

c) No se permite imprimir documentos personales en grandes cantidades (Más de 10 hojas por jornada laboral).

d) Se debe de cuidar los equipos de impresión adecuadamente, evitar daños en los mecanismos físicos y lógicos que los componen.

e) Cada usuario está sujeto a un análisis de la cantidad de documentos que imprimen y si es necesario deberá sustentar ante el jefe inmediato o la Gerencia la cantidad impresa en dicho periodo analizado.

f) Cada usuario tiene el derecho y el deber de solicitar el cambio de código de impresión en caso de sospechar que alguien esté utilizando dicho código sin previa autorización.

3. POLÍTICAS DE CUARTO DE SISTEMAS, SERVIDORES Y BASE DE DATOS

3.1. DataCenter (Centro de Datos)

Oficina con equipos de cómputo, telecomunicaciones y servidores que prestan servicios a todas las sedes de COOPEVIAN con las características físicas y ambientales adecuadas para que los equipos alojados funcionen sin problema y en óptimas condiciones.

El DataCenter deberá:

a) Tener una puerta de acceso de vidrio templado transparente, para favorecer el control del uso de los recursos de cómputo.

b) Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada sólo al personal autorizado del proceso de Sistemas.

c) En caso de ingresar personal externo, se debe de notificar un día antes y relacionar el número de identificación, nombre completo, fecha y hora y que acción va a realizar en el sitio.

d) Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.

e) Estar libre de contactos e instalaciones eléctricas en mal estado.

f) Aire acondicionado. Mantener la temperatura entre 17 y 22 grados centígrados.

g) Asignar un técnico para que realice un mantenimiento mensual de temperatura y aires acondicionados y llevar un registro de estos controles.

h) Respaldo de energía redundante (UPS) como mínimo para los equipos Servidores o planta eléctrica en su defecto para cada una de las sedes de COOPEVIAN.

i) Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

3.2. Infraestructura

a) Las dependencias deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

b) El resguardo de los equipos de cómputo deberá quedar bajo el proceso de Sistemas contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.

3.3. Servidores

a) El personal encargado del proceso de Sistemas tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

b) La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad del personal de Sistemas.

c) El personal de Sistemas definirá la tecnología, marca y recursos que tendrá cada Servidor para el correcto funcionamiento de estos.

d) Durante la configuración de los servidores el personal de Sistemas debe generar las normas para el uso de los recursos tecnológicos y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

   1. Los servidores que proporcionen servicios a través de la red e Internet deberán:

   2. Funcionar 24 horas del día los 365 días del año.

   3. Recibir mantenimiento preventivo al hardware mínimo dos veces al año.

   4. Recibir mantenimiento preventivo al software mínimo una vez al mes.

   5. Recibir mantenimiento preventivo anual que incluya la revisión de su configuración, licenciamiento de sistema operativo y software.

   6. Ser monitoreados por el personal encargado de Sistemas.

e) Los servicios hacia Internet o la nube solo podrán proveerse a través de los servidores autorizados por el personal de Sistemas.

3.4. Base de Datos

Para la operación del software de red que se utiliza en COOPEVIAN, se deberá tener en consideración lo siguiente:

a) Toda la información de los aplicativos de COOPEVIAN deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla. Se recomienda utilizar como motor de base de datos (SQL Server).

b) El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

c) El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso.

d) Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.

e) En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.

f) La longitud mínima de las contraseñas será igual o superior a siete caracteres, y estarán constituidas por combinación de caracteres alfanuméricos y especiales.

4. SEGURIDAD PERIMETRAL

La seguridad perimetral es uno de los métodos posibles de protección de la Red LAN, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

a) El personal del área de Sistemas implementará soluciones lógicas y físicas que garanticen la protección de la información de COOPEVIAN de posibles ataques cibernéticos internos o externos.

b) Rechazar conexiones a servicios de procedencia no autorizada o sospechosa.

c) Permitir solo ciertos tipos de tráfico (Ejemplo: Correo electrónico, http, https).

d) Proporcionar un único punto de interconexión con el exterior.

e) Redirigir el tráfico entrante a los sistemas adecuados dentro de la LAN (Red Interna).

f) Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.

g) Auditar el tráfico entre el exterior y el interior.

h) Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos.

i) Se recomienda implementar servidores WAF (Web Application Firewall), esto con el objetivo de proteger los servidores y aplicaciones Web de los diversos y posibles ataques a la capa de aplicación (XXS, Inyección de SQL, Envenenamiento de Cookies).

4.1. Firewall

a) La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (Físico) o Software (Lógico), que se encarga de controlar reglas y políticas de navegación, puertos de entrada y salida, enrutamiento y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos de los servidores o aplicativos expuestos a internet.

b) Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.

c) Se recomienda que la solución de Firewall disponga de sistema de respuesta automática y con inteligencia artificial, esto para actuar de forma autónoma las 24 horas en la prestación del servicio en la red local de la organización. Un ejemplo de soluciones, serían los DR o MDR.

d) El personal del proceso de Sistemas establecerá las reglas en el Firewall necesarias para bloquear, permitir o ignorar el flujo de datos entrantes y salientes de la Red LAN o WAN.

e) El Firewall debe bloquear las “conexiones extrañas o maliciosas” y no dejarlas pasar para que no causen vulnerabilidades o daños en la red interna.

f) El Firewall debe controlar los ataques de DDoS “Denegación de Servicio” y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.

g) El Firewall debe de permitir crear y gestionar reglas y políticas de navegación Web de usuarios y acceso de aplicaciones (P2P, Proxy’s, VPN’s, etc).

h) Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

5. ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, COOPEVIAN se reserva el derecho a modificar esta Política de Seguridad Informática cuando lo considere necesario. Los cambios realizados en esta Política serán divulgados a todos los usuarios de la Cooperativa por los diferentes canales de comunicación (Correo, SMS, Intranet, Inducción, Capacitaciones, etc.).

Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de la Política de Seguridad Informática más reciente, el no leer la Política de Seguridad Informática no exime a los usuarios de las responsabilidades, deberes y derechos que esta exige.

5.1. Disposiciones

a) Las disposiciones aquí enmarcadas, entrarán en acción a partir del día de su difusión.

b) Las normas y políticas objeto de este documento podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo del área de Sistemas con la revisión de la Dirección S.I.G y autorización de la Gerencia; una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su publicación.

c) La falta de conocimiento de las normas aquí descritas por parte de los usuarios no los libera de la aplicación de sanciones disciplinarias y/o penalidades por el incumplimiento de estas.

6. POLÍTICAS DE RESPALDO DE LA INFORMACIÓN

6.1. Planes de Contingencia

El área de Sistemas establecerá los planes de contingencia necesarios para respaldar y recuperar la información de COOPEVIAN y garantizar la continuidad de los diferentes servidores, aplicativos internos y toda la información corporativa en caso de siniestro.

Los procedimientos de Backup, transporte, restauración y verificación de la información de COOPEVIAN, deben estar debidamente documentados y actualizados. Su ejecución periódica son la garantía de la integridad y confiabilidad de la información.

Las acciones de emergencia a tomar en caso de un ciberataque serán las siguientes:

a) Cambio de contraseña de todos los servidores y cuenta administrador para evitar nuevos ingresos a estos.

b) Cambio de contraseña de los aplicativos para evitar acceso a la información de las bases de datos.

c) Restringir accesos por VPN, Escritorio Remoto, Team Viewer, AnyDesk y demás herramientas de conexión remota a la red local.

d) Solicitar cambio inmediato de contraseña a todos los usuarios de la red local y correo corporativo.

e) Restringir el uso de Discos Extraíbles (Memorias USB, discos duros externos, memorias SD, microSD, celulares, Tablet, entre otros), unidades lectoras de DVD-CD y acceso a Internet. Esto a través de las GPO desde el Servidor principal o restricciones a través de la consola del Antivirus utilizado o software DLP.

f) Bloqueo de la cuenta de usuario de inicio de sesión en el dominio de COOPEVIAN y acceso a correo electrónico (Local o Web) al personal que se considere de riesgo.

g) De acuerdo con la eventualidad implementar o modificar políticas de seguridad que refuercen el control y acceso a posibles vulnerabilidades en la seguridad informática de COOPEVIAN.

h) Cambiar contraseñas de las redes WI-FI periódicamente cada 6 meses, de esta manera controlar el acceso a Internet y red local del personal administrativo y visitantes.

i) Realizar cambio de permisos en el perfil de cada usuario, limitando permisos de Administrador a Usuario Avanzado o Usuario y de esta forma garantizar que los usuarios realicen posibles cambios en los equipos de cómputo los cuales no estén autorizados por el área de Sistemas.

j) Realizar capacitación de cómo convertir archivos de Excel y Word a formato PDF y cifrarlos y de esta manera enviarlos electrónicamente al destinatario y evitar la filtración y modificación de la información por terceros.

6.2. Copias de seguridad.

a) La información crítica del negocio debe ser respaldada periódicamente. El usuario es responsable de definir qué información debe ser respaldada y su frecuencia. La recomendación por parte del personal de Sistemas es que esta información se guarde en **la partición de disco duro "D:"** de cada computador de usuario o en la entrega del equipo de cómputo acompañada del acta de entrega se definirá una carpeta en la cual el usuario debe de mantener la información que considere importante para la copia de seguridad. El usuario está en la obligación de depurar continuamente la información allí

alojada y no guardar información que no sea necesaria para el cargo o área y no incluir: música, videos, fotos, programas, juegos, carpetas y demás documentos personales.

b) Es responsabilidad del área de Sistemas, el respaldo de la información que reside en los servidores de COOPEVIAN. Aquí se utilizarán varios medios o repositorios de almacenamiento para salvaguardar las copias de seguridad, sean locales o externos a la organización, estos serán, discos duros externos de gran volumen de almacenamiento, dispositivos NAS o SAN, almacenamiento en la nube pública o privada, así realizar una restauración de la información más ágil y segura.

c) De igual manera, es responsabilidad de cada usuario almacenar y controlar la información guardada en cada equipo de cómputo asignado y cumplir con la ruta definida para esta información. El personal de sistemas apoyará a los usuarios en la implementación de sus procedimientos de Backup con la aplicación para realizar determinada tarea programada y totalmente automática.

d) Los usuarios también tendrán asignado un tamaño de almacenamiento en la nube para guardar copias o carpetas y documentos que sean críticos del cargo o proceso, será responsabilidad de cada usuario hacer uso correcto de este almacenamiento como herramienta principal o alternativa.

e) Se recomienda disponer de una estrategia de copias de seguridad (3-2-1-1-0) 3 copias diferentes, 2 medios diferentes, 1 copia remota, 1 copia sin conexión separado o inmutable, 0 errores tras la verificación de la capacidad de recuperación de la copia.

CRONOGRAMA COPIAS DE SEGURIDAD SERVIDORES

SERVIDOR	TIPO BACKUP	PERIODICIDAD	RETENCIÓN DIAS
FILE SERVER	INCREMENTAL	Diario	15
	FULL	Semanal	3
	FULL	Mensual	2
	FULL	Anual	2
SERVIDORES CRÍTICOS	INCREMENTAL	Diario	15
	FULL	Semanal	3
	FULL	Mensual	2
	FULL	Anual	2
SERVIDORES CRÍTICOS	INCREMENTAL	Martes - Jueves	15
	FULL	Semanal	3
	FULL	Mensual	2
	FULL	Anual	2

6.3. Política Antivirus

a) En cada uno de los equipos de COOPEVIAN debe instalarse y activarse la herramienta de antivirus definida como solución corporativa. Esta debe mantenerse actualizada diariamente con la lista de los virus más actuales y así evitar su infección y propagación en la red local de COOPEVIAN.

b) Está prohibido desactivar el programa Antivirus, si el usuario detecta que ha sido deshabilitada debe informar inmediatamente al área de sistemas. El programa de Antivirus estará protegido por una contraseña de seguridad desde la consola administrativa, para evitar la desactivación en tiempo real del antivirus.

c) Si se detecta la presencia de virus u otro agente potencialmente peligroso, se debe informar de inmediato al personal de Sistemas para que realice el proceso adecuado para la desinfección o eliminación de la amenaza.

d) Es responsabilidad del usuario que ingrese archivos en medios magnéticos a COOPEVIAN (CD/DVD, discos duros externos, memorias USB, celulares, Tablet, entre otros), el antivirus realizará un escaneo automáticamente del dispositivo de almacenamiento para verificar que la información contenida allí sea segura, por ningún motivo se debe forzar la cancelación del escaneo y de ser cancelado la herramienta de Antivirus cuenta con una contraseña de seguridad desde la consola de administrativa para evitar la cancelación del mismo.

7. CIBERSEGURIDAD

La ciberseguridad, también conocida como seguridad digital, es la práctica de proteger la información digital, dispositivos y activos. Esto incluye información corporativa, cuentas de aplicativos, archivos, videos e incluso el dinero.

El acrónimo "CIA" se usa a menudo para representar los tres pilares de la ciberseguridad.

Confidencialidad: mantener los secretos y garantizar que solo los usuarios autorizados puedan obtener acceso a sus archivos y cuentas.

Integridad: garantizar que su información es la que debe ser y de que nadie ha insertado, modificado o eliminado cosas sin su permiso.

Acceso: garantizar que puede tener acceso a su información y sistemas cuando lo necesite. Un ejemplo de un problema de acceso sería una denegación de servicio, donde los atacantes desbordan el sistema con tráfico de red para hacer que el acceso sea casi imposible; o Ransomware que cifra el sistema e impide que lo use.

El personal de Sistemas definirá las herramientas, mecanismos y estrategias para disminuir los riesgos de ciberseguridad en la red corporativa, dentro de estos estarías los siguientes:

a) Crear contenido de formación para el personal.
b) Comunicar y divulgar constantemente sobre cambios o riesgos que se identifiquen en la red de la organización.
c) Generar campañas de Ransomware y Phishing.
d) Forzar el uso de contraseñas seguras.
e) Forzar el uso del doble factor de autenticación.
f) Enviar Tips sobre buenas prácticas del uso de las herramientas tecnológicas.
g) Utilizar herramientas de monitoreo de seguridad de red.
h) Implementar un plan de continuidad de TI.
i) Generar copias de seguridad de Servidores de datos y aplicaciones.
j) Disponer de un repositorio con inmutabilidad habilitada, para disminuir la afectación por ataques de Ransomware.
k) Realizar simulacros de restauración de copias de seguridad de servidores.
l) Aplicar herramientas de cifrado de datos.
m) Utilizar herramientas de análisis de vulnerabilidades web.
n) Herramientas inalámbricas de defensa de red.
o) Implementar software de antivirus.
p) Implementar una solución MDR (Detección y Respuesta Gestionada).
q) Disponer de un dispositivo de Firewall.
r) Implementar un sistema de prevención de intrusos (IPS)
s) Pruebas de penetración.
t) Usar certificados de cifrado en los servidores (SSL)
u) Utilizar conexión VPN con cifrado SSL

8. DIRECTIVA GLOBAL DIRECTORIO ACTIVO (GPO)

DIRECTIVAS DE CUENTAS Y CONTRASEÑAS	
DIRECTIVA	**CONFIGURACIÓN**
Exigir historial de contraseñas	24 contraseñas recordadas
Las contraseñas deben cumplir los requisitos de complejidad	Habilitado
Longitud mínima de la contraseña	14 caracteres
Vigencia máxima de la contraseña	120 días
Vigencia mínima de la contraseña	5 días
DIRECTIVAS DE BLOQUEO DE CUENTAS	
DIRECTIVA	**CONFIGURACIÓN**
Duración del bloqueo de cuenta	10 minutos
Restablecer recuentos de bloqueo de cuenta tras	10 minutos
Umbral de bloqueo de cuenta	3 intentos de inicio de sesión no válidos
DIRECTIVAS DE CUENTAS Y CONTRASEÑAS	
DIRECTIVA	**CONFIGURACIÓN**
Habilitar protector de pantalla	Habilitado
Proteger el protector de pantalla mediante contraseña	Habilitado
Tiempo de espera del protector de pantalla	Habilitado
Número de segundos de espera hasta que se active el protector de pantalla	600 segundos