VISAN®
Seguridad Privada

POLITICA DE SEGURIDAD INFORMATICA

INFORMACÍON DE CONTROL DOCUMENTAL

Área / Departamento:	Medios Tecnológicos y Sistemas	**Clasificación**	Documento interno
Tipo de documento:	Documento de consulta	**Aplica a:**	Toda la organización

CONTROL DE CAMBIOS

No. de Versión	DESCRIPCIÓN DE CAMBIOS	ELABORADO POR	FECHA	REVISADO POR	APROBADO POR
1	Creación de documento	Fernando Vargas Jefe MT&S	1/08/2018	Viviana Villamil Jefe G&D	Juan Carlos Rojas medina Gerente General
2	Se realiza actualización de la política incluyendo los controles actuales	Maicol Forero Jefe sistemas	7/11/2023	Betty Pereira	Jhon Jairo Munera Estupiñán Gerente General
3	Se realiza actualización incluyendo el numeral 16.2 redes Privada VPN	Maicol Forero Jefe sistemas	17/04/2024	Constanza Rodriguez Gerente financiera	Jhon Jairo Munera Estupiñán Gerente General

ELABORADO POR:	REVISADO POR:	APROBADO POR:
MAICOL FORERO JEFE SISTEMAS	CONSTANZA RODRIGUEZ GERENTE FINANCIER	JHON JAIRO MUNERA ESTUPIÑÁN GERENTE GENERAL
FECHA: 16/07/2025	FECHA: 16/07/2025	FECHA: 16/07/2025

TABLA DE CONTENIDO

La política de seguridad informática tiene por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de la organización.

1. ALCANCE

Este documento de políticas de seguridad es elaborado de acuerdo con el análisis de riesgos y de vulnerabilidades en la compañía (VIGILACIA SANTAFEREÑAY CIA), por consiguiente, el alcance de estas políticas se encuentra sujeto a las mismas.

Esta política es aplicable a todos los empleados, contratistas y otros empleados de la compañía, incluyendo a todo el personal externo que cuenten con un equipo conectado a la Red. Así mismo es aplicable también a todos los equipos y servicios propietarios o arrendados que de alguna manera tengan que utilizar local o remotamente el uso de la Red o recursos tecnológicos de Visan, así como de los servicios e intercambio de archivos y programas.

La elaboración de las presentes Políticas de Seguridad está basada en el análisis interno y han sido planteadas, analizadas y revisadas con el fin de no contravenir con las garantías básicas de los usuarios, y no pretende vulnerar el derecho a la privacidad sin dejar a un lado la seguridad de la información de la organización, respetando en todo momento estatutos y reglamentos internos de Visan.

- Control de acceso (aplicaciones, base de datos, área de medios tecnológicos y sistemas).
- Resguardo de la Información.
- Clasificación y control de activos.
- Gestión de las redes.
- Gestión de la continuidad del negocio.
- Seguridad de la Información en los puestos de trabajo.
- Controles de Cambios.
- Protección contra intrusión en software en los sistemas de información.
- Monitoreo de la seguridad.
- Identificación y autenticación.
- Utilización de recursos de seguridad.
- Comunicaciones.
- Privacidad.

2. OBJETIVOS

- Dotar de la información necesaria a los usuarios y empleados, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software, así como la información que es procesada y almacenada en estos.
- Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de Visan.

3. VIGENCIA

La documentación presentada como Políticas de Seguridad entrará en vigor desde el momento en que sean aprobadas por la Gerencia. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de Visan o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

4. NOTIFICACIONES DE VIOLACIONES DE SEGURIDAD

Es de carácter obligatorio para todo el personal (Fijo, Contratado), la notificación inmediata de algún problema o violación de la seguridad, del cual fuere testigo; esta notificación debe realizarse vía correo electrónico a la Jefatura de Sistemas Jefe.Sistemas@visan.net.co , quien está en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente.

Es responsabilidad de todo empleado que maneje datos o información a través de accesos debidamente autorizados, el cumplimiento de las políticas de control de acceso, su incumplimiento puede incurrir en alguna violación en materia de seguridad informática acarreando sanciones al reglamento interno de trabajo. Es por ello que las personas relacionadas de cualquier forma con los procesos tecnológicos deben ser conscientes y asumir que la seguridad es asunto de todos y, por tanto, deben conocer y respetar las Políticas de Seguridad.

5. LINEAMIENTOS PARA LA ADQUISICIÓN DE BIENES INFORMÁTICOS

Toda adquisición de tecnología informática se efectuará a través de una requisición autorizada por la gerencia administrativa y la jefatura de sistemas, al planear las operaciones relativas a la adquisición de bienes informáticos, establecerán prioridades y en su selección deberá tomar en cuenta el procedimiento **LGT-PRO-01 PROCEDIMIENTO DE COMPRAS Y LOGISTICA**, así mismo se evaluará el desarrollo Tecnológico, el grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

6. ESTÁNDARES

Toda adquisición se basa en los estándares, es decir la arquitectura de la compañía establecida por el área de medios tecnológicos y sistemas.

7. CAPACIDADES

Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área. Para la adquisición de Hardware se tendrá en cuenta lo siguiente:

- El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores de este y dentro de los estándares tecnológicos según actualidad
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente.

- Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
- Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y a la contratación establecida en Visan.
- Juntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste
- En lo que se refiere a los servidores, equipos de comunicaciones, concentradores, switches y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, se registrarán en el programa de mantenimiento preventivo y correctivo.
- Todo proyecto de adquisición de bienes de tecnología debe sujetarse al análisis, aprobación y autorización del área de medios tecnológicos y sistemas

8. SOFTWARE

- En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente.
- Para la adquisición de Software base y utilitarios, el Área de medios tecnológicos y sistemas dará a conocer periódicamente las tendencias con tecnología
- 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.
- El área de medios tecnológicos y sistemas promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

9. BASES DE DATOS

Para la operación del software de red en caso de manejar los datos empresariales mediante sistemas de información, se deberá tener en consideración lo siguiente:

- Toda la información 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.
- El acceso a los sistemas de información deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información de Visan. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.
- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.
- Los datos de los sistemas de información deben ser respaldados de acuerdo con la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente.
- En cuanto a la información de los equipos de cómputo, se recomienda a los usuarios que realicen sus propios respaldos en la (Carpeta segura) ya que esta reposa en un servidor de la compañía

- Los sistemas de información deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoría y Control).
- Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.
-

10. FRECUENCIA DE EVALUACIÓN DE LAS POLÍTICAS.

Se evaluarán las políticas del presente documento, con una frecuencia anual por el Área de medios tecnológicos y sistemas, gestión y desarrollo.

11. POLITICAS DE SEGURIDAD FISICA

11.1. ACCESO FÍSICO

Visan destinará un área que servirá como centro de telecomunicaciones donde ubicarán los sistemas de telecomunicaciones y servidores.
Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.
El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso.
Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de medios tecnológicos y sistemas.

12. PROTECCIÓN FÍSICA

12.1. DATA CENTER

El Data Center deberá:

- Tener una puerta de acceso de vidrio templado transparente, para favorecer el control del uso de los recursos de cómputo.
- Ser un área restringida que garantice la entrada solo al personal autorizado por la jefatura de sistemas
- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo
- Estar libre de contactos e instalaciones eléctricas en mal estado
- Aire acondicionado. Mantener la temperatura a 17 grados centígrados.
- El analista de sistemas realizara un control diario temperatura y aires acondicionados y llevar un registro de estos controles.
- Respaldo de energía redundante.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- El ingreso al centro de datos será registrado en un formato este con el fin de llevar un control de ingreso
- Contar con algún esquema que asegure la continuidad del servicio.

- Prevención y/o detección de incendios
- Contar con un extintor de incendio adecuado y cercano al DataCenter.

12.2. INFRAESTRUCTURA

Las dependencias deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.
El resguardo de los equipos de cómputo deberá quedar bajo el área de medios tecnológicos y sistemas contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.

12.3. INSTALACIONES DE EQUIPOS DE CÓMPUTO

La instalación del equipo de cómputo quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- El Área de medios tecnológicos y sistemas deberá contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

12.4. CONTROL

- Los Activos de Sistemas deben llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.
- Los encargados del área de medios tecnológicos y sistemas son los responsables de organizar el cronograma para el mantenimiento preventivo y correctivo de los equipos de cómputo.
- El Área de Recursos Humanos deberá reportar a medios tecnológicos y sistemas cuando un usuario deje de laborar este con el fin de retirarle las credenciales de ingreso a los recursos y supervisar la correcta devolución de los equipos y recursos asignados al usuario.
- El usuario, en caso de retiro, deberá tramitar ante el área de medios tecnológicos y sistemas el paz y salvo correspondiente.

12.5. RESPALDOS

- las Bases de Datos de Visan serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.
- Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro que permita tener contingencia y continuidad de negocio.

- Los demás respaldos (una copia completa) deberán ser almacenados en un lugar seguro y distante del sitio de trabajo
- Para reforzar la seguridad de la información, en cada equipo de la compañía se dejará un acceso directo a una carpeta llamada (carpeta segura) esta estará alojada en un servidor la cual se realizará backup de la información diariamente en forma incremental la información que no se encuentre en esta carpeta serán responsabilidad absoluta de los usuarios

12.6. RECURSOS DE LOS USUARIOS

- Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y Red de la compañía, de acuerdo con las políticas que en este documento se mencionan.
- Los usuarios deberán solicitar apoyo al área de medios tecnológicos y sistemas ante cualquier duda en el manejo de los recursos de cómputo de Visan.
- El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la Compañía, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera).

12.7. DERECHOS DE AUTOR

- Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor.
- Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de Visan en ninguna circunstancia sin la autorización escrita de la jefatura de medios tecnológicos y sistemas o la gerencia administrativa.
- No está permitido instalar ningún programa en su computadora sin dicha autorización o la clara verificación de que Visan posee una licencia que cubre dicha instalación.
- No está autorizada la descarga de Internet de programas informáticos no autorizados por la jefa tura de medios tecnológicos y sistemas o la gerencia administrativa.
- No se tolerará que un empleado realice copias no autorizadas de programas informáticos.
- No se tolerará un empleado realice intercambios o descargas de archivos digitales de música (MP3, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución de este.
- Si se descubre que un empleado ha copiado programas informáticos o música en forma ilegal, este puede ser sancionado, suspendido o despedido.
- Si se descubre que un empleado ha copiado programas informáticos en forma ilegal para dárselos a un tercero, también puede ser sancionado, suspendido o despedido.
- Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.
- Los usuarios no descargarán ni cargarán programas informáticos no autorizados a través de Internet.
- Los usuarios no realizarán intercambios o descargas de archivos digitales de música (MP3, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución de este.

- Los usuarios que se enteren de cualquier uso inadecuado que se haga en Visan de los programas informáticos o la documentación vinculada a estos, deberán notificar a la jefatura de medios tecnológicos y sistemas
- Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.
- Los empleados que realicen adquieran o utilicen copias no autorizadas de programas informáticos estarán sujetos a sanciones disciplinarias internas de acuerdo con las circunstancias. Dichas sanciones pueden incluir suspensiones y despidos justificados.

13. POLITICAS DE SEGURIDAD LOGICA

RED

Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de las empresas entre usuarios, departamentos, oficinas y hacia afuera a través de conexiones con otras redes.

- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.
- No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de Visan.
- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la compañía y se usarán exclusivamente para actividades relacionadas con labor asignada.
- Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.
- El uso de analizadores de red es permitido única y exclusivamente por el área de medios tecnológicos y sistemas para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad bajo las Políticas de Seguridad.
- No se permitirá el uso de analizadores para monitorear o censar redes ajenas a Visan y no se deberán realizar análisis de la Red desde equipos externos a la entidad.
- Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

SERVIDORES.

Configuración e instalación

El área de medios tecnológicos y sistemas tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

- La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de Sistemas.
- Durante la configuración de los servidores el jefe del área de medios tecnológicos y sistemas debe generar las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

- Los servidores que proporcionen servicios a través de la red e Internet deberán funcionar 24 horas del día los 365 días del año.
- Recibir mantenimiento preventivo mínimo dos veces al año
- Recibir mantenimiento semestral que incluya depuración de logs.
- Recibir mantenimiento anual que incluya la revisión de su configuración.
- Ser monitoreados por el Jefe de medios tecnológicos y sistemas el analista de medios tecnológicos y sistemas.
- Los servicios de Internet sólo podrán proveerse a través de los servidores autorizados por Sistemas.

CORREO ELECTRÓNICO

- El área de medios tecnológicos y sistemas se encargarán de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
- La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres.
- Los correos recibidos a las cuentas del dominio **visan.net.co,** catalogados como Phishing, Spear phishing o Whaling estos serán loqueados puntualmente en la consola de administración de correos por la jefatura del área de medios tecnológicos y sistemas

13.1. BASES DE DATOS

- 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.
- El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso.
- 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.
- 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.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

13.2. RECURSOS DE CÓMPUTO

Seguridad de cómputo

- El Área de medios tecnológicos y sistemas es la encargada de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo.
- El Área de medios tecnológicos y sistemas deben mantener informados a los usuarios y poner a disposición de estos el software que refuerce la seguridad de los sistemas de cómputo.

- El Área de medios tecnológicos y sistemas son los únicos autorizados para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

13.3. RESPONSABILIDADES Y AUTORIDADES

El Jefe de medios tecnológicos y sistemas y el analista medios tecnológicos y sistemas tendrán las siguientes responsabilidades y autoridades:

- Podrán ingresar de forma remota a los equipos excepto las gerencias exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.
- Deberán utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.
- Deberán realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.
- Deben actualizar la información de los recursos de cómputo, cada vez que adquiera e instale equipos o software.
- Deben registrar cada máquina en el inventario de control de equipos de cómputo y red de Visan.
- Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.
- Reportar a la jefatura de medios tecnológicos y sistemas los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

13.4. INCUMPLIMIENTO POLITICA

El incumplimiento de las responsabilidades personales establecidas en la sección 13.9.2 de la Política de Seguridad Informática MT&S-DOC-01, especialmente en lo referente a la gestión de accesos autorizados, el uso adecuado de contraseñas, la protección de datos personales y el manejo de información sensible, será considerado una falta grave. Cualquier uso indebido o no autorizado del sistema de información, así como la suplantación de accesos, constituirá una violación grave de la Política de Seguridad Informática. Estas acciones podrán acarrear sanciones disciplinarias que van desde amonestaciones hasta la terminación del contrato laboral, dependiendo de la gravedad y recurrencia de la infracción.

Además, si el incumplimiento ocasiona daños o perjuicios a la organización o a terceros, el trabajador podrá ser civil y penalmente responsable, de acuerdo con las normativas legales vigentes. Las sanciones también podrán incluir la suspensión del acceso al sistema y la aplicación de acciones legales pertinentes, según corresponda.

13.5. RENOVACIÓN DE EQUIPOS

- Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.
- Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al área de medios tecnológicos y sistemas a fin de que se seleccione el equipo adecuado. Sin el visto bueno de medios tecnológicos y sistemas no podrá liberarse una orden de compra.

13.6. USO DE SERVICIOS DE RED

Gerencias y Sedes

- El área de medios tecnológicos y sistemas son los responsables de la administración de contraseñas y deberán guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.
- El jefe de medios tecnológicos y sistemas y el analista de medios tecnológicos y sistemas tienen las siguientes responsabilidades en los servidores de Visan.
  - Respaldo de información conforme a los procedimientos establecidos.
  - Revisión de logs y reporte de cualquier eventualidad.
  - Implementar de forma inmediata las recomendaciones de seguridad y reportar posibles faltas a las políticas de seguridad en cómputo.
  - Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
  - Organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores.
- La jefatura y el analista son los únicos autorizado para asignar las cuentas a los usuarios.
- La jefatura y el analista podrán aislar cualquier servidor de red, notificando a las Gerencias y áreas de la entidad, en las condiciones siguientes:
  - Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la Red.
  - Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
  - Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
  - Si se detectan accesos no autorizados que comprometan la integridad de la información.
  - Si se viola las políticas de uso de los servidores.
  - Si se reporta un tráfico adicional que comprometa a la red de Visan.

13.7. USUARIOS

Identificación de Usuarios y contraseñas

- Todos los usuarios con acceso a un sistema de información o a la Red, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

- El usuario deberá definir su contraseña de acuerdo con lo establecido, para tal efecto y será responsable de la confidencialidad de esta.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recurso que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por La Jefatura de medios tecnológicos y sistemas.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud del área de medios tecnológicos y sistemas, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:
  - Cuando ésta sea una contraseña débil o de fácil acceso.
  - Cuando crea que ha sido violada la contraseña de alguna manera.
- El usuario deberá notificar al área de medios tecnológicos y sistemas en los siguientes casos:
  - Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
  - Si tiene problemas en el acceso a los servicios proporcionados por el servidor.
- Si un usuario viola las políticas de uso de los servidores, la jefatura de medios tecnológicos y sistemas podrá cancelar totalmente su cuenta de acceso a los servidores, notificando a La Gerencia correspondiente.

Responsabilidades Personales

- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar a la jefatura de medios tecnológicos y sistemas.
- El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.
- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.
- En caso de que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar a la jefatura de medios tecnológicos y sistemas una nueva clave.

- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.
- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.
- Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.
- Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.
- Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco del equipo de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

Uso Apropiado de los Recursos

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

Queda Prohibido

- Hacer uso de discos duros externos o memorias USB, el área de te medios tecnológicos y sistemas tiene bloqueado los puertos externos con el fin de prevenir perdida de información e infección
- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de Visan.
- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos Informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
- Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus.

14. ANTIVIRUS

Antivirus de la Red

- Todos los equipos de cómputo de Visan deberán tener instalada una Solución Antivirus.
- Periódicamente se hará el rastreo en los equipos de cómputo de Visan, y se realizará la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

14.1. Responsabilidad Área de medios tecnológicos y sistemas

El área de medios tecnológicos y sistemas responsables de:

- Implementar la Solución Antivirus en las computadoras de Visan.
- Solucionar contingencias presentadas ante el surgimiento de virus que la solución no se haya detectado automáticamente.
- Configurar el analizador de red para la detección de virus.
- El área de medios tecnológicos y sistemas aislarán el equipo o red, notificando a la Gerencia correspondiente, en las condiciones siguientes:
  - Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otros equipos y redes.
  - Si el usuario viola las políticas antivirus.
- La solución corporativa de seguridad de antivirus es Bit defender, Esta solución integra herramientas Antivirus, antispyware, firewall y prevención contra intrusiones, además de control de dispositivos y aplicaciones usando un único agente multiplataforma (Windows, Mac, Linux)

14.2. COBERTURA

Con Bit defender se da cobertura a los siguientes sistemas operativos:

Clientes

- Microsoft: Windows 8 / 10 / 11 en versiones 32 y 64 bits.
- Apple: Mac OS X 10.4 / 10.5 / 10.6 / 10.7 / 10.8

Servidores

- Microsoft: Windows 2013 Standard /Enterprise Edition, Windows 2022 R2 / Standard/ Enterprise Edition en distribution 32 y 64 Bits.
- Apple: Mac OS X Server 10.7 64 Bits

Para simplificar la instalación del agente Bitdefender , se pondrá a disposición del equipo de soporte los agentes de instalación clasificados como "Desktop, Portátiles y Servers" en versiones:

- Windows: Instalador interactivo y Silencioso en versiones 32 y 64 bits.
- Mac OS X (instalador único válido para Mac OSX 10.5 o superior)

15. POLÍTICAS ANTIVIRUS

Todos los equipos de cómputo conectados a la red corporativa deben tener instalado y debidamente actualizado Bit defender, con el fin de que esto sea cumplido, cualquier proceso interno de asignación y/o rotación de equipos de cómputo le corresponde una lista de chequeo para su alistamiento, lista dentro de la cual se encuentra debidamente registrado la instalación y/o validación de Bit defender. La desinstalación de antivirus se encuentra restringida a la validación de clave de desinstalación, la cual se encuentra a disposición únicamente del área de medios tecnológicos y sistemas.
Utilizando la consola de administración de Bitdefender se implementan las siguientes políticas:

16. VIRUS Y SPYWARE

FIREWALL

- Desactiva el firewall de Windows y establece políticas de reglas centralizadas.
- Reglas preestablecidas en la instalación y que son recomendación de buenas prácticas por Bitdefender.

INTRUSIÓN PREVENCIÓN

Detecta y bloquea automáticamente ataques de red y a navegadores de internet, debe permanecer activada globalmente.

CONTROL DE APLICACIONES Y DISPOSITIVOS

- Conjunto de reglas que permiten controlar acceso de aplicaciones y/o dispositivos a los recursos del sistema, con el fin de prevenir riesgos de infección y/o seguridad; Se bloqueara el acceso a dispositivos de almacenamiento externo
- Bloqueo a ejecución de aplicaciones desde dispositivos almacenamiento externo y dispositivos de almacenamiento removibles incluyendo Autorun.inf.

USO DEL ANTIVIRUS POR LOS USUARIOS

- El usuario deberá comunicarse con el área de medios tecnológicos y sistemas en caso de problemas de virus para buscar la solución.
- El usuario será notificado por el área de medios tecnológicos y sistemas en los siguientes casos:
  - Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia.
  - Cuando sus archivos resulten con daños irreparables por causa de virus.
  - Cuando viole las políticas antivirus.

17. SEGURIDAD PERIMETRAL

La seguridad perimetral es uno de los métodos posibles de protección de la infraestructura, 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.

El área de medios tecnológicos y sistemas implementará soluciones lógicas y físicas que garanticen la protección de la información de Visan de posibles ataques internos o externos.

- Rechazar conexiones a servicios comprometidos
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
- Proporcionar un único punto de interconexión con el exterior.
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red
- Interna).
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde
- Internet
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

17.1. FIREWALL

- La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.
- Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
- El área de medios tecnológicos y sistemas establecerán las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- El firewall debe bloquear las "conexiones extrañas" y no dejarlas pasar para que no causen problemas.
- El firewall debe controlar los ataques de "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.
- 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).

17.2. REDES PRIVADAS VIRTUALES (VPN)

- Para tener acceso a la VPN de la compañía, el área de sistemas realizará un memorando explicando el uso y responsabilidad, esta conexión tendrá dos autorizaciones del jefe inmediato y la jefatura de sistemas
- La instalación de la VPN en equipos no corporativos deberá cumplir con las siguientes características:
  - Sistema operativo licenciado.
  - Actualizaciones del sistema operativo al día.
  - Antivirus licenciado.
  - Ausencia de programas maliciosos.
  - Esta verificación será llevada a cabo por el área de medios tecnológicos y sistemas. En caso de que el equipo no cumpla con estas especificaciones, la instalación de la VPN no se llevará a cabo.
- El área de medios tecnológicos y sistemas estará a cargo de configurar el software necesario y de asignar las claves a los usuarios que lo soliciten.

18. CONECTIVIDAD A INTERNET

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de Visan tienen las mismas responsabilidades en cuanto al uso de Internet.
- 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 incorporado en la misma.
- 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.
- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.
- Sólo puede haber transferencia de datos o de Internet en conexión con actividades propias del trabajo desempeñado.

19. RED INALÁMBRICA (WIFI)

Acceso a Funcionarios de Visan:

- La red inalámbrica (WIFI) es un servicio que permite conectarse a la red Visan e Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de Visan.

- Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.
- Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbricas (computadoras portátiles, Ipod, celulares, etc.) con capacidad de conexión Wireless.
- El área de medios tecnológicos y sistemas, son los encargados de la administración, habilitación y/o bajas de usuarios en la red inalámbrica de Visan.

Identificación y activación

- Para hacer uso de la red inalámbrica WIFI, el solicitante necesariamente deberá ser miembro de la compañía si no se asignara a la red de visitantes.
- Se debe registrar la dirección MAC de las tarjetas inalámbricas de todos y cada uno de los dispositivos de comunicación.
- Para conectarse a la red inalámbrica se deberá emplear autenticación tipo WPA2- AUTO-PSK para lo cual los nombres de usuarios y contraseñas cambiarán periódicamente (de 6 a 12 meses) con la finalidad de proporcionarles seguridad en el acceso a los usuarios.

Seguridad

- A pesar de que se han establecido sistemas de encriptación de datos mediante el uso de seguridad WPA2-AUTO-PSK, NO SE RECOMIENDA hacer uso de tarjetas de crédito para compras.
- El área de medios tecnológicos y sistemas se reservan el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red. No se deben realizar intentos de ingreso no autorizado a cualquier dispositivo o sistema de la red inalámbrica. Cualquier tipo de ingreso no autorizado es una práctica ilegal
- No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica. Esta práctica es una violación a la privacidad y constituye un robo de
- los datos de usuario, y puede ser sancionado.

Tecnología

- A pesar de que se usan amplificadores de señal, la cobertura queda sujeta a diversos factores, por lo que NO SE GARANTIZA en ninguna forma el acceso desde cualquier punto fuera de cobertura de Visan .
- Sólo será soportado el protocolo TCP/IPV.4 en la red inalámbrica. El área de medios tecnológicos y sistemas se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios de Visan.
- No se permiten la operación ni instalación de "puntos de acceso" (access points) conectados a la red cableada de Visan sin la debida autorización por parte del área de medios tecnológicos y sistemas .

- No se permite configurar las tarjetas inalámbricas como "puntos de acceso" o la configuración de equipos como servidores adicionales.

Ciberseguridad accesos de navegación

Uso permitido

- Se permite el acceso a sitios web relacionados con las funciones laborales del usuario.
- El acceso a servicios en la nube, aplicaciones web y plataformas colaborativas estará habilitado según el requerimiento y verificación del sitio
- La navegación debe realizarse desde los dispositivos corporativos provistos o autorizados.

Uso prohibido

- Queda prohibido el acceso a sitios con contenido ofensivo, pornográfico, violento, discriminatorio o ilegal.
- No está permitido el uso de plataformas de streaming (ej. Netflix, Spotify), redes sociales o juegos en línea durante el horario laboral,

Salvo autorización expresa

- Se prohíben las descargas de software, archivos ejecutables o contenido multimedia que no tenga relación directa con la labor asignada.

Supervisión y monitoreo

- Todo el tráfico web será monitoreado por el área de TI mediante herramientas de control de acceso a internet (firewall, proxy, etc.).
- Se generarán reportes periódicos sobre el uso de internet y se tomarán acciones preventivas o correctivas en caso de detectar anomalías.

Responsabilidades del usuario

- Usar internet exclusivamente para fines laborales autorizados.
- No compartir credenciales de acceso ni conectarse con dispositivos no autorizados.
- Informar inmediatamente sobre cualquier uso indebido o intento de acceso sospechoso.

Excepciones

- Entre las medidas de seguridad se encuentra configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los usuarios podrán notificar esta eventualidad para que sea resuelta a la brevedad posible.
- En caso de eventos, cursos, talleres, conferencias, etc, se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil.

- En el caso de estos eventos las restricciones para acceder podrán ser "anuladas" temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos un día hábil.

Acceso a Invitados:

- La red inalámbrica (Invitados) es un servicio que permite conectarse única y exclusivamente a personal externo de Visan (clientes, proveedores) a internet sin la necesidad de algún tipo de cableado. La Red inalámbrica de Invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura de Visan.
- Los usuarios invitados no tendrán acceso a la Red de Visan ni a ningún recurso de uso privado de Visan.
- La red inalámbrica es de tipo Portal Cautivo el área de medios tecnológicos y sistemas tendrá una lista de usuarios invitados con contraseñas que se actualizarán cada dos meses.
- Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, Visan se reservan el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los usuarios de Visan.
- Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de la Política de Seguridad más reciente.

Disposiciones

- Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.
- 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 medios tecnológicos y sistemas ; una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.
- La falta de conocimiento de las normas aquí descritas por parte de los usuarios no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento.

JHON JAIRO MUNERA ESTUPIÑAN
REPRESENTANTE LEGAL