TERMINOS Y CONDICIONES DE USO DE SAFE WEB –

Aprobado por:	*Nombre: Pedro Ospino* *Cargo: Gerente de TI* *Fecha: 21/01/2019*

REGISTRO DE CAMBIOS

Revisión	Fecha	Responsable	Descripción del Cambio

LISTA DE DISTRIBUCION

DOCUMENTO CONTROLADO. NO COPIAR SOLO PARA USO INTERNO

TÉRMINOS Y CONDICIONES

*Términos y condiciones Generales

Este sitio web es operado por Prixmasol S.A.S., el acceso al mismo y el uso de la información contenida en él, constituyen la aprobación del usuario con los "Términos y condiciones" aquí descritos. Por la utilización del sitio y/o sus servicios, el usuario se obligará a cumplir con los mismos, no pudiendo argumentar el desconocimiento de tales Términos y Condiciones.

El Usuario debe leer, entender y aceptar todas las condiciones establecidas en los Términos y Condiciones de Prixmasol S.A.S. así como en los demás documentos incorporados a los mismos por mención, previas a su uso, registro como Usuario y/o a la adquisición de productos y/o entrega de cualquier dato con un determinado fin.

En consecuencia, todas las visitas y transacciones que se realicen en este sitio, como así mismo sus efectos jurídicos, quedarán regidos por estas normas y sometidos a la legislación aplicable en Colombia.

Estas Condiciones de Servicio se aplican a todos los usuarios del sitio, incluyendo su limitación a usuarios que sean navegadores, proveedores, clientes, comerciantes, y/o colaboradores de contenido.

*Participación de los Usuarios e Información Personal

Prixmasol S.A.S. ejercerá un control previo permanente sobre la participación de los usuarios, para velar por el respeto de derechos de terceros y el cumplimiento de las normas aplicables. Los usuarios deberán abstenerse de irrespetar o amenazar de cualquier forma a otros usuarios del sitio web y/o de usarlo como medio para violar la integridad de los demás usuarios.

Así mismo, Prixmasol S.A.S. entiende que la información y materiales entregados por los usuarios son de su autoría exclusiva o tiene autorización de su uso, por tanto los usuarios se hacen responsables ante terceros por la violación de derechos de autor, debiendo dar los créditos requeridos a las fuentes, y se comprometen a indemnizar a Prixmasol S.A.S. por cualquier acción contra esta por infracción de derechos de propiedad intelectual de terceros.

El usuario certifica que tiene los derechos y otorga las autorizaciones necesarias sobre los archivos y la información que este registre en el sitio web, y autoriza a Prixmasol S.A.S. para el uso de la misma.

Prixmasol S.A.S., como exclusivo administrador del sitio web, se reserva el derecho a: negar el registro a cualquier persona, por cualquier motivo; incluir o no en el contenido del sitio web la información o el material recibido de los usuarios; mantener en el sitio web el material por el tiempo que considere relevante; modificar en cualquier tiempo y por cualquier motivo los términos y condiciones de la participación de usuarios; llevar el registro y almacenamiento de la información discutida dentro del sitio para estudio, análisis o reporte de eventos adversos.

El tratamiento dado a los datos personales recolectados a través de este sitio, están enmarcados bajo la Ley sobre Protección de Datos Personales (Ley 1581 de 2012), cuyo tratamiento en específico será de acuerdo a la Política de tratamiento de datos personales de Prixmasol S.A.S.

Para la utilización de nuestro sitio web es necesaria la utilización de cookies. Las cookies, se utilizan con la finalidad de facilitar la navegación y ofrecer un servicio personalizado y ágil, así como una herramienta estadística para obtener datos del uso de la plataforma en la web. En ningún caso se utilizan para almacenar información que pueda identificar al usuario.

***Derechos de propiedad**

Los contenidos, páginas y pantallas del sitio, junto con el logo y la marcas de propiedad de Prixmasol S.A.S., se encuentran debidamente registradas y protegidas por la Ley en Colombia y a nivel internacional. En ningún caso se podrá hacer uso de alguno de ellos sin la expresa autorización de la Empresa.

La información, imágenes, videos, demos, simuladores y otras herramientas, contenidas en este sitio han sido creadas y desarrolladas para el servicio y uso de nuestros afiliados y visitantes. No está permitido copiarlas, modificarlas o reproducirlas, total o parcialmente, venderlas, publicarlas o distribuirlas con fines comerciales.

Sin embargo, la información aquí contenida puede compartirla utilizando las herramientas que proveemos para ello, enlaces a redes sociales, compartir por correo electrónico, entre otras.

***Responsabilidad**

Prixmasol S.A.S., opera asegurando que la información contenida en su sitio web sea completa, exacta, actualizada y concordante con la definida por la normativa vigente.

Prixmasol S.A.S., garantiza la adopción de medidas que propendan a generar altos niveles de confidencialidad, disponibilidad e integridad de la información contenida en nuestro sitio.

Prixmasol S.A.S., podrá suspender transitoriamente o finalizar la publicación de la página sin aviso previo y en cualquier momento, sin que ello genere derecho a indemnización alguna en favor de los usuarios.

El usuario reconoce y acepta que el uso de esta página es bajo su propio y exclusivo riesgo.

La información, sólo estará disponible en este sitio mediante accesos técnicamente controlables, y disponible únicamente para los titulares de la información o terceros autorizados.

La información contenida en este sitio tiene carácter informativo, educativo y comercial sobre los productos y servicios que ofrecemos y se habilita a disposición del público en general.

***Enlaces a otros sitios**

Este sitio puede contener enlaces o conexiones a sitios de terceras entidades, respecto a los cuales no nos responsabilizamos por sus políticas o contenido.

Prixmasol S.A.S., se reserva el derecho de agregar y/o eliminar cualquier enlace o conexión a sitios de terceras entidades, en cualquier momento, sin aviso previo ni expresión de causa.

***Modificaciones y actualizaciones**

Cualquier función nueva o herramienta que se añadan, también estarán sujetas a los Términos y Condiciones. El usuario puede revisar la versión actualizada, en cualquier momento en este sitio web. Nos reservamos el derecho de actualizar, cambiar o reemplazar cualquier parte de los Términos de Servicio mediante la publicación de actualizaciones y/o cambios en nuestro sitio web. Es responsabilidad del usuario chequear esta página periódicamente para verificar cambios. Su uso continuo o el acceso al sitio web después de la publicación de cualquier cambio constituye la aceptación de dichos cambios.

***Preguntas y sugerencias**

Si presenta alguna duda o sugerencia respecto de los "Términos y condiciones" póngase en contacto con la Empresa por medio del correo info@prixmasol.com .

LINEAMIENTOS DE SEGURIDAD PARA USO DE FIREWALLS Y CONEXIONES VPN

Aprobado por:	*Nombre: Pedro Ospino* *Cargo: Gerente de TI* *Fecha: 21/01/2019*

REGISTRO DE CAMBIOS

Revisión	Fecha	Responsable	Descripción del Cambio

LISTA DE DISTRIBUCION

DOCUMENTO CONTROLADO. NO COPIAR SOLO PARA USO INTERNO

LINEAMIENTOS DE SEGURIDAD PARA USO DE FIREWALLS Y CONEXIONES VPN

OBJETIVO

Definir los controles generales de seguridad que deben implementarse en firewalls y conexiones VPN de Prixmasol S.A.S., para garantizar la confidencialidad, integridad y disponibilidad de la información de la organización.

ALCANCE

Este documento presenta un conjunto de controles mínimos y obligatorios que se deben aplicar a todos los firewalls y conexiones VPN que formen parte de la plataforma tecnológica de Prixmasol S.A.S

Los parámetros de configuración específicos dependen de la marca, modelo y versión de los dispositivos/software de firewall y VPN utilizados, de manera que deberán ser consultados directamente en la documentación del fabricante.

FORMATO DE EXCEPCIONES

El documento "GSRTI - Formato de Excepciones.docx" debe ser utilizado para aquellos casos en los que no se pueda aplicar algún control especificado en el presente documento.

PREMISAS Y RESPONSABILIDADES

El contenido de este documento se fundamenta en, y apoya el cumplimiento de, los requerimientos establecidos en la Política de Seguridad y Riesgos de TI de PRIXMASOL. Está basado en mejores prácticas de la industria y para sus futuras revisiones se toman en cuenta las recomendaciones emanadas de la Gerencia de Infraestructura de TI y las coordinaciones relacionadas con su cumplimiento. La creación y modificación de los requisitos de configuración segura para diversos elementos de la plataforma tecnológica de PRIXMASOL es responsabilidad de la Gerencia de Seguridad y Riesgos de TI.

La implementación y mantenimiento operativo de los controles y configuraciones de seguridad sobre cada firewall o dispositivo de conexión VPN en particular es responsabilidad del área de Infraestructura de TI; específicamente de la coordinación de Redes y Telecomunicaciones.

CONTROLES DE SEGURIDAD PARA FIREWALLS

Categoría: Ambiente y arquitectura

1 Deben utilizarse firewalls para la protección de:

- Comunicación entre redes y sistemas internos de PRIXMASOL hacia redes externas.
- Comunicación entre redes de usuarios finales y redes de servidores internos.
- Comunicación desde redes externas a servicios publicados por PRIXMASOL. En este caso los servidores deben ser colocados en un segmento de red DMZ (zona desmilitarizada).
- Para aplicaciones distribuidas, basadas en múltiples capas, sólo debe colocarse en la DMZ la capa de presentación.
- Las capas de aplicación y base de datos deben ser implementadas en la red interna de servidores.

2 Dependiendo de la criticidad de los servicios, se debe considerar la implementación de esquemas de alta disponibilidad o balanceo de carga que permitan garantizar la continuidad de la operación.

3 La administración de los firewalls (configuración de políticas, monitoreo, generación de reportes y gestión de eventos) debe ser centralizada.

Categoría: Instalación y configuración

4 Actualizar el sistema a la última versión disponible y probada por el fabricante.

5 Implementar las recomendaciones de seguridad del fabricante.

6 En base a la plataforma utilizada, se deben aplicar los controles de seguridad apropiados:

- Cuando se utilice un equipo de propósito general, se deben aplicar las configuraciones de seguridad específicas para su plataforma, definidas por la Gerencia de Seguridad y Riesgos de TI.
- Cuando se utilice un aplicativo (appliance) especializado, se deben aplicar las configuraciones generales de seguridad para dispositivos conectados a la red de la empresa.
- Cuando el Firewall provea servicios de VPN, aplicar las configuraciones de seguridad establecidas en la sección "Controles de seguridad para conexiones VPN", más adelante en este mismo documento.

7 El nombre del dispositivo debe asignarse en base al estándar de nombramiento de servidores definido por la Coordinación de Arquitectura de TI.

8 Sincronizar la fecha/hora contra un servidor NTP (Network Time Protocol).

9 La administración de la plataforma debe considerar:

a. El uso de una red de administración dedicada, limitando los accesos sólo para los administradores.
b. La administración remota será en base a comunicaciones cifradas (herramientas propietarias, HTTPS, SSH, SFTP).

10 Colocar un mensaje de advertencia antes de permitirle a un usuario administrador autenticarse en el dispositivo:
"ADVERTENCIA: el acceso a este sistema está estrictamente limitado a personal autorizado por PRIXMASOL, C.A. El acceso no autorizado a este sistema, o el uso indebido del mismo, está prohibido y es contrario a la Política de Seguridad y Riesgos de TI de la empresa y a la legislación vigente. El uso que realice de este sistema puede ser objeto de monitoreo."

11 Se debe realizar un análisis de vulnerabilidades antes de la salida a producción del firewall y remediarse los riesgos detectados. Estas pruebas deben repetirse al menos una vez al año.

Categoría: Autenticación y autorización

12 Las cuentas administrativas no requeridas deben ser eliminadas, o en su defecto bloqueadas y expiradas.

13 Deben establecerse diferentes roles de usuarios en función de los requerimientos y de acuerdo con la política de
mínimo privilegio.

Se deben definir al menos los siguientes tipos de usuarios de administración:

- Administrador del sistema: encargado de la configuración y administración del sistema. Tiene derechos de control total.
- Usuario supervisor: sólo cuenta con permiso de lectura de la configuración del firewall. (p.e., auditores, operadores, etc.)

14 Si el firewall lo permite, los administradores deben utilizar un esquema de autenticación fuerte.

15 Se deben considerar los siguientes controles para la autenticación de usuarios:

- Los administradores del firewall deben utilizar cuentas nombradas No deben crearse cuentas genéricas ni compartidas. Debe utilizarse el estándar de nombres de cuentas de usuario definido por la coordinación de Arquitectura de TI.
- Gestión de contraseñas:
- Longitud mínima: 12 caracteres
- Expiración de la sesión: 5 minutos.
- Número de reintentos de autenticación y bloqueo automático: 3 intentos fallidos.
- Cifrado fuerte de las contraseñas en el dispositivo.
- Si el dispositivo lo permite, se deben considerar funciones adicionales de autenticación basadas en LDAP, TACACS, RADIUS, KERBEROS o tokens de autenticación.

16 Eliminar del sistema los usuarios que hayan sido dados de baja. Categoría: Políticas de firewall

17 La política de seguridad aplicada por el firewall debe estar basada en las siguientes premisas:

- Cumple con las políticas de seguridad de PRIXMASOL.
- Debe estar aprobada por la Gerencia de Seguridad y Riesgos de TI.
- Toda comunicación que no está explícitamente permitida debe ser denegada.
- No se permiten conexiones "any to any".
- Las reglas que permiten las conexiones deben ser específicas en cuanto a origen, destino y puertos permitidos, aplicando la norma de sólo permitir lo absolutamente necesario.
- La última regla a aplicar debe ser la que deniega todo el tráfico explícitamente. Se debe registrar los eventos asociados con esta regla.

18 Todas las reglas deben estar documentadas, y deben organizarse en base a los siguientes criterios:

- Debido a que por lo general los firewalls operan bajo el esquema de aplicar la primera regla coincidente, se deben organizar las reglas de manera que no se permita inadvertidamente tráfico no autorizado.
- Las reglas deben ser ordenadas en base a su frecuencia de utilización de manera de mejorar el rendimiento.

19 Se debe establecer el filtrado de paquetes DNS (UDP/TCP 53):

- El firewall sólo debe permitir transferencias de zonas (TCP/53) entre los servidores DNS autorizados.
- Sólo se deben permitir consultas DNS (UDP/53) hacia Internet a los servidores DNS internos.

20 Restringir tráfico ICMP (ICMP/3, 8, 11) sólo para administradores de sistemas de comunicaciones. Bloquear mensajes echo requests y replies, y mensajes salientes del tipo "time exceeded" y "host unreachable".

21 Si el firewall lo permite, activar los mecanismos de protección antispoofing de direcciones IP. Se debe considerar el bloqueo explícito y el logging de tráfico dirigido hacia direcciones externas inválidas:
Direcciones no enrutables:

- 0.0.0.0
- 255.255.255.255
- 127.0.0.0 - 127.255.255.255
- Direcciones privadas (RFC 1918) y reservadas:
- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255
- 240.0.0.0
- 169.254.0.0 - 169.254.255.255
- Otros:
- UDP echo
- ICMP broadcast (RFC 2644)
- Bloqueo de tráfico IPv6, mientras no sea implementado este protocolo.
- También se debe agregar el bloqueo de las redes IP públicas asignadas a PRIXMASOL cuando ellas sean el origen del tráfico entrante en las interfaces internas.

22 Se debe filtrar el tráfico broadcast. No se recomienda activar el registro de logs para eventos de este tipo debido a su volumen y al bajo nivel de información que proporcionan.

23 Se deben deshabilitar el "source routing" y el "IP forwarding".

24 Los dispositivos en las redes internas de la empresa sólo deben utilizar direccionamiento IP privado. El firewall, o los
routers de conexión a Internet, deberán realizar traducción de direcciones (NAT) tanto para servicios entrantes como salientes.

25 Se deben bloquear todas las conexiones originadas desde Internet hacia la red interna. Además, se deben bloquear todas las conexiones originadas en el segmento DMZ y dirigidas hacia la red interna, salvo en aquellos sistemas específicos (front-end) que necesiten acceder a servicios de servidores internos (back-end). Estos casos deben estar justificados y documentados.

26 Se debe llevar un registro de las políticas aplicadas en el firewall, con el detalle de los accesos otorgados, datos del solicitante, aprobaciones, propósito, duración, entre otros.

27 Se debe limitar el uso de reglas temporales, de prueba o contingencia. Las mismas deben tener un período de vigencia definido. Estas reglas deben eliminarse una vez concluido este período.

Categoría: Administración, mantenimiento y monitoreo.

28 El firewall debe estar configurado para almacenar logs de manera local y centralizada. En el momento en que se implemente en la organización una solución de gestión centralizadas de eventos, todos los logs de los firewalls deben ser enviados vía protocolo syslog hacia dicha solución.

29 Los logs y alertas deben ser revisados continuamente para identificar amenazas, errores de configuración y vulnerabilidades. Se deben configurar alertas en tiempo real para notificar a los administradores sobre la ocurrencia de eventos críticos. Las notificaciones deben incluir:

- Eventos operacionales como reinicio del sistema, falta de espacio en disco, etc.
- Modificaciones de políticas.
- Cambios de estado de sistemas de alta disponibilidad.
- Intentos de conexión no autorizados al firewall.

30 Habilitar los servicios de registro de eventos para las políticas del firewall. La información de conexiones a registrar debe contemplar, como mínimo, los siguientes aspectos:

- Dirección IP origen.
- Puerto de conexión origen.
- Dirección IP destino.
- Servicio o puerto de conexión destino.
- Usuario autenticado y esquema de autenticación en caso de tratarse de una conexión autenticada.
- Fecha y hora.
- Acción ejecutada por el firewall (aceptar, rechazar, descartar).
- Se debe decidir para cada caso específico los eventos que se deben registrar.

31 Mantener actualizado el firewall según las recomendaciones del fabricante y de acuerdo con los siguientes criterios:

- Se dará prioridad a las actualizaciones referentes a problemas de seguridad o que afecten a la disponibilidad del sistema.
- Se acordará un calendario de paradas de los sistemas para la aplicación de actualizaciones y parches.
- Deberán crearse procedimientos de urgencia para la aplicación de actualizaciones que resuelvan una vulnerabilidad crítica del sistema que comprometa directamente su seguridad.

32 Configurar de forma robusta el servicio SNMP con los siguientes criterios:

- Utilizar SNMP v3, habilitando el cifrado de la comunicación y la autenticación mediante usuario/contraseña.
- Cambiar los nombres de las comunidades por defecto y utilizar contraseñas fuertes.

33 Se debe monitorear el rendimiento de los componentes del firewall para garantizar la identificación y canalización de posibles problemas de recursos y disponibilidad de servicios.

34 Se deben definir un procedimiento de respaldo seguro de la configuración del firewall. Este respaldo debe ejecutarse al menos una vez al mes.

35 Se debe definir un procedimiento para el manejo y registro de incidencias, así como un procedimiento de recuperación.

36 Se debe realizar al menos una revisión semestral de las políticas del firewall.
Se deben examinar los cambios desde la última revisión, considerando:

- Quién y bajo qué circunstancias realizó los cambios.
- Identificación de reglas redundantes.
- Identificación y validación de reglas eliminadas.
- Identificación y depuración de reglas temporales.
- Identificación de servicios que ya no están operativos y eliminación de reglas asociadas.
- Se debe evaluar si las reglas reflejan la política de seguridad vigente para PRIXMASOL.

CONTROLES DE SEGURIDAD PARA CONEXIONES VPN

Categoría: Ambiente y arquitectura

1 La infraestructura de VPN requiere el uso de dispositivos dedicados y especializados, de preferencia firewalls y
routers. Los mismos deben estar ubicados en una DMZ (zona desmilitarizada).

2 Evaluar las recomendaciones de implementación segura del fabricante, Implementar el esquema que mejor se adapte a los requerimientos de seguridad y funcionalidad de PRIXMASOL. Se debe evaluar la necesidad de implementar una solución de VPN robusta y redundante.

3 Toda conexión VPN debe estar protegida por un firewall. Sólo se debe permitir el tráfico autorizado en base a

origen, destino, protocolo, y horario. Debe considerarse filtrar el tráfico asociado con:

- Los servicios propios de la VPN
- Servicios requeridos para el funcionamiento del dispositivo (p.e., AAA, LDAP).
- Administración del dispositivo.
- Auditoría, monitoreo y manejo de logs.

4 La infraestructura de VPN debe estar integrada con un sistema AAA (authentication, autorization, accounting).

Categoría: Instalación y configuración

5 Actualizar el sistema a la última versión disponible y probada por el fabricante.

6 En base a la plataforma utilizada como concentrador de VPN, se deben aplicar los controles de seguridad apropiados:

- Cuando se utilice un equipo de propósito general, se deben aplicar las configuraciones de seguridad específicas para su plataforma, definidas por la Gerencia de Seguridad y Riesgos de TI.
- Cuando se utilice un aplicativo (appliance) especializado, se deben aplicar las configuraciones generales de seguridad para dispositivos conectados a la red de la empresa.
- Si el servicio de VPN es provisto por un firewall, aplicar las configuraciones de seguridad establecidas en la sección "Controles de seguridad para firewalls", más adelante en este mismo documento.

7 Sincronizar la fecha/hora contra un servidor NTP (Network Time Protocol).

Categoría: VPN punto a punto

8 Se establecerán conexiones VPN Punto a Punto entre la red corporativa de PRIXMASOL, su proveedores de servicios, socios de negocios y clientes y cuando la criticidad de la información de la información transmitida lo requiera.

Estas VPN serán del tipo IPSec y deberán proveer protección de confidencialidad e integridad de la información.

9 Las VPN IPSec deben usar los algoritmos de cifrado en el siguiente orden de preferencia:

- AES-CBC (AES in Cipher Block Chaining mode) con clave de 128 bits.
- Triple DES (3DES-CBC).
- Se prohíbe el uso del algoritmo Data Encryption Standard (DES)

10 Las VPN IPSec deben usar el algoritmo de protección de integridad HMAC-SHA-1

11 Las VPN IPSec deben proveer protección de replay.

12 Las asociaciones de seguridad (SA) de IKE no deben tener una duración mayor a 24 horas (86400 segundos). Las asociaciones de seguridad (SA) IPSec no deben durar más de 8 horas (28800 segundos). Es importante asegurar que los pares estén configurados con tiempos de duración compatibles. Algunas implementaciones pueden rechazar la negociación si el par propone una duración mayor a la suya.

13 El grupo Diffie-Hellman (DH) utilizado para el intercambio de información para generar las claves de IKE debe ser consistente con los requerimientos de seguridad y la fortaleza de las claves de cifrado. Se debe utilizar el Grupo 2 de DH (1024-bit MODP) para Triple DES y AES con llaves de 128 bits. Para niveles superiores de seguridad, se puede utilizar el Grupo 5 de DH (1536-bit MODP) o el Grupo 14 de DH (2048-bit MODP) para AES.

14 Se debe especificar el uso de Main Mode en la Fase 1 de IKE. El modo agresivo se utilizará sólo cuando no se pueda configurar Main Mode.

15 Utilizar Perfect Forward Secrecy, siempre y cuando no genere una carga excesiva o problemas de interoperabilidad.

16 Seleccionar el esquema de autenticación que más convenga según las necesidades de la VPN:

- Clave compartida (Preshared key)
- Firmas digitales
- Infraestructura de claves públicas.
- Autenticación externa

Cada uno de estos métodos tiene ventajas y desventajas que deben ser evaluados en base a los requerimientos, disponibilidad de recursos y características de los dispositivos utilizados.

17 En el caso de utilizarse preshared-key, las claves compartidas deben cumplir con las siguientes características:

- Ser actualizadas periódicamente para reducir el impacto potencial asociado con el compromiso de claves.
- Se deben mantener en secreto y transferirse por canales alternos seguros.
- Deben ser complejas
- Asociarse a direcciones IP específicas
- Las claves no deben ser compartidas por más de 2 dispositivos.

18 Se debe restringir a nivel de firewall el acceso provisto a través de las VPN, de acuerdo a las siguientes premisas:

- Se debe restringir el acceso en base a origen, destino, protocolo, y horario.
- Sólo se debe permitir el tráfico autorizado.
- Se debe poder identificar a los usuarios y/o los dispositivos de acceso de manera de poder deshabilitar el acceso rápidamente en caso de requerirse.

19 El dispositivo IPSec debe ser configurado para almacenar registros históricos de las conexiones exitosas y fallidas,
con el suficiente detalle para permitir el manejo de incidentes y solventar fallas de funcionamiento.
En el momento en que se implemente en la organización una solución de gestión centralizadas de eventos, todos los logs de los firewalls deben ser enviados vía protocolo syslog hacia dicha solución.

20 Se deben utilizar direcciones IP públicas para las VPN con terceras partes. Utilizar NAT para enmascarar el direccionamiento interno.

Categoría: VPN para accedo remoto de usuarios

21 Se debe mantener una lista actualizada de los usuarios autorizados.
Los permisos de acceso deben ser granulares y asignarse en base a grupos o roles. La lista debe especificar permisología de cada usuario. Adicionalmente se debe anexar la lista de servicios, aplicaciones y recursos que puede acceder cada grupo o rol. Los accesos deben otorgarse en base al principio de menor privilegio. La lista debe ser auditada trimestralmente. Se debe deshabilitar inmediatamente el acceso de los usuarios que ya no lo requieran.

22 El acceso remoto de los administradores, proveedores y usuarios en general, se realizará a través de clientes VPN IPSec, y desde equipos provistos por la organización. En el caso de proveedores, socios de negocio y contratistas, el acceso VPN debe estar estrictamente restringido a casos justificados. En estos casos, el acceso no debe ser permanente, sino habilitado bajo demanda.

23 Sólo los administradores y proveedores de servicios de soporte podrán utilizar aplicaciones o protocolos de asistencia remota.

24 Si la plataforma VPN lo soporta, sólo permitir las conexiones desde clientes que cuenten con una configuración segura. Se pueden considerar los siguientes elementos iniciales

- Antimalware instalado y actualizado
- Sistema operativo actualizado
- Cliente VPN actualizado
- Aplicaciones actualizadas
- Sólo debe haber una conexión de red activa
- Firewall local activo

25 Las contraseñas utilizadas para el acceso a la VPN deben ser complejas (uso de caracteres especiales, mayúsculas,
minúsculas, y números) y cumplir con los siguientes criterios:

- Mantener el historial de 12 contraseñas
- Tener una edad máxima de 30 días
- Tener una edad mínima de 0 días
- Tener una longitud mínima de 8 caracteres
- Cifrado "reversible" desactivado
- Advertir su vencimiento 4 días antes

26 En caso de que existan VPN SSL, deben cumplir con las siguientes premisas:

- Utilizar certificados de al menos 128 bits y generados por autoridades certificadoras (CA) confiables.
- Utilizar exclusivamente suites de cifrado seguras (al menos 128 bits)
- Utilizar TLS 1.0 (SSL 3.1) o posterior
- Utilizar preferiblemente HMAC-SHA-1

27 Se debe forzar la desconexión de las sesiones inactivas luego de 5 minutos.