



INSTITUTO TECNOLÓGICO DE MORELIA

Departamento de Sistemas Computacionales

Proyecto 3 SGSI para un banco

Alumnos:

- Víctor Eduardo Garcia Patiño
- Ricardo Jacobo Ferreira
- Edwin Eduardo Baltazar Reyes

Profesor: Ferreira Medina Heberto

Núm. De Control: 18121690

Correo electrónico: l18121690@morelia.tecnm.mx

Junio 2023

Contenido

1.Introducción	4
2.Planteamiento de Problema	4
3.Investigación y Desarrollo	5
3.1.Objetivo, misión y visión de la implementación del SGSI	5
3.1.1.Objetivo	5
3.1.2.Misión	5
3.1.3.Visión.....	5
3.2.Objetivo, misión y visión de la empresa.....	5
3.2.1.Objetivo.	5
3.2.2.Misión	5
3.2.3.Visión.....	5
3.3.Sistema de Gestión de Seguridad de la Información (Planificar, Hacer, Verificar y Actuar).....	5
3.3.1.Planificar.....	6
3.3.2.Hacer.....	6
3.3.3.Verificar.	6
3.3.4.Actuar.	6
4. Reglamento de la organización	7
4.1. Introducción al reglamento	7
4.2. Uso de equipos y dispositivos de TICs.	7
4.2.1. Ámbito de aplicación.....	7
4.2.2. Uso adecuado de los equipos IT.	7
4.2.3. Propiedad y responsabilidad.	8
4.2.4. Acceso y autorización.....	8
4.2.5. Uso personal y prohibido.	8
4.2.6. Seguridad de la información	8
4.2.7. Monitoreo y registro.....	8
4.2.8. Mantenimiento y actualización.....	8
4.2.9. Cumplimiento.....	8
4.3. Uso de Internet y correo electrónico.	9
4.3.1. Ámbito de aplicación.....	9
4.3.2. Uso adecuado de Internet y correo electrónico.	9
4.3.3. Propiedad y responsabilidad.	9
4.3.4. Acceso y autorización.....	9
4.3.5. Uso personal y prohibido.	9

4.3.6. Seguridad de la información.....	9
4.3.7. Monitoreo y registro.....	9
4.3.8. Correo electrónico	10
4.3.9. Cumplimiento.....	10
4.3.10. Descarga e instalación de contenido	10
4.4. Reglamento de empleados.....	10
5. Tipos de usuario.....	11
6. Políticas.....	12
6.1. Políticas de seguridad.....	12
6.2. Tráfico en la red	24
6.3. Políticas de acceso para los usuarios según su perfil.....	28
6.3.1. Políticas de Usuario.	28
6.3.2. Políticas de Empleado.....	30
6.3.3. Políticas de Ejecutivo.	33
6.3.4. Políticas de Administrador.....	36
7. Identificación de activos	39
8. Matriz de Riesgos.....	43
9. Plan de Contingencia	44
10. Muestra de Resultados.....	49
10.1. Configuraciones del entorno de red.....	49
Anexo 1. Archivos no permitidos para intercambiar en la red.....	70
Anexo 2. Lista de programas no permitidos.....	70
11. Conclusiones.....	71
12. Referencias	71

1.Introducción

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es una necesidad crítica para las organizaciones modernas debido a la importancia de la información y los datos en su funcionamiento diario. Un SGSI es un enfoque sistemático para gestionar la seguridad de la información de una organización y protegerla de cualquier amenaza o riesgo.

En la actualidad, muchas organizaciones han adoptado un SGSI debido a la creciente cantidad de amenazas cibernéticas y a la necesidad de cumplir con las normativas y regulaciones legales relacionadas con la protección de datos y la privacidad. La implementación de un SGSI ayuda a garantizar que la información de la organización esté protegida de manera adecuada y que se sigan los procedimientos necesarios para prevenir y mitigar cualquier riesgo o incidente de seguridad.

Según el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), un SGSI consta de cuatro componentes principales: planificación, implementación, evaluación y mejora continua. La planificación incluye la identificación de los objetivos de seguridad y los requisitos, mientras que la implementación implica la implementación de controles de seguridad y procedimientos. La evaluación se enfoca en medir la efectividad del SGSI, mientras que la mejora continua implica ajustar y mejorar el SGSI a medida que cambian las necesidades y los riesgos de la organización.

Un SGSI es un enfoque sistemático para gestionar la seguridad de la información de una organización y protegerla de cualquier amenaza o riesgo. Según la norma ISO 27001, un SGSI consta de cuatro componentes principales: la planificación, la implementación, la evaluación y la mejora continua. La planificación incluye la identificación de los objetivos de seguridad y los requisitos, mientras que la implementación implica la implementación de controles de seguridad y procedimientos. La evaluación se enfoca en medir la efectividad del SGSI, mientras que la mejora continua implica ajustar y mejorar el SGSI a medida que cambian las necesidades y los riesgos de la organización (ISO, 2013).

La implementación de un SGSI es crucial para proteger la información y los datos de una organización de amenazas cibernéticas y para garantizar el cumplimiento de las regulaciones legales relacionadas con la protección de datos. El enfoque sistemático de un SGSI ayuda a garantizar que la información de la organización esté protegida de manera adecuada y que se sigan los procedimientos necesarios para prevenir y mitigar cualquier riesgo o incidente de seguridad.

2.Planteamiento de Problema

El establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) implica un proceso riguroso y detallado que puede presentar desafíos para cualquier organización. Entre los principales desafíos se encuentra la identificación y evaluación de los riesgos de seguridad de la información específicos de la organización y la implementación de controles adecuados para mitigar estos riesgos. Además, el mantenimiento continuo del SGSI y la mejora continua también pueden ser desafíos importantes.

Otro problema común que enfrentan las organizaciones en la implementación de un SGSI es la falta de comprensión y compromiso de los empleados. La seguridad de la información no es solo una tarea del equipo de TI, sino que debe ser una responsabilidad compartida por todos los empleados. Por lo tanto, es importante que se implementen programas de concientización y capacitación en seguridad de la información para garantizar que todos los empleados comprendan la importancia de la seguridad de la información y estén comprometidos con el SGSI.

Por último, otro problema importante es la complejidad y el costo de la implementación de un SGSI. La implementación de un SGSI requiere recursos significativos, incluido el tiempo, el personal y el presupuesto, para garantizar que se identifiquen y aborden todos los riesgos de

seguridad de la información. Además, mantener y mejorar continuamente el SGSI también puede ser costoso y requerir recursos adicionales.

3. Investigación y Desarrollo

3.1. Objetivo, misión y visión de la implementación del SGSI

3.1.1. Objetivo

Gestionar los riesgos y minimizar la materialización de estos, además de garantizar el cumplimiento de la seguridad a través de la triada conocida como CID:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

También debe considerarse la aplicación y revisión de los procedimientos, mecanismos técnicos y tecnológicos que garanticen el acceso a los datos en forma segura.

3.1.2. Misión

Implementar un Sistema de Gestión de la Seguridad de la Información permite manejar de manera adecuada los riesgos al aplicar buenas prácticas de seguridad y mejora continua del SGSI para garantizar la confidencialidad, integridad y disponibilidad.

3.1.3. Visión

Reforzar y asegurar los servicios de red para maximizar el rendimiento, reducir o eliminar en gran medida las amenazas que acechan la información, facilitar la administración del sistema y lograr beneficios tangibles para la empresa.

Mejorar continuamente el SGSI para que se adapte a nuevos riesgos o riesgos no identificados al principio.

3.2. Objetivo, misión y visión de la empresa.

3.2.1. Objetivo.

Ofrecer productos y servicios financieros a sus clientes, y generar beneficios para sus accionistas y partes interesadas.

3.2.2. Misión

Brindar soluciones financieras de calidad a sus clientes, asegurando la rentabilidad sostenible y el crecimiento del negocio, y manteniendo una cultura empresarial ética y responsable.

3.2.3. Visión.

Convertirse en el líder del mercado en términos de calidad y rentabilidad en los servicios financieros que ofrece, mantener una fuerte relación con sus clientes y la comunidad, y ser reconocida por su compromiso con la responsabilidad social corporativa y la sostenibilidad.

3.3. Sistema de Gestión de Seguridad de la Información (Planificar, Hacer, Verificar y Actuar).

Según el INAI en el 2015 la implementación de un sistema tan completo como lo es un SGSI se necesita seguir los siguientes pasos:

3.3.1. Planificar.

Se planea:

- Identificar los objetivos de seguridad de la información y definir la política de seguridad del banco como lo mencionado en la sección 3.1. de este reporte, estableciendo los roles y responsabilidades para la gestión de la seguridad de la información.
- Realizar una evaluación de riesgos para identificar los riesgos de seguridad asociados con los sistemas de información del banco y determinar las medidas de control necesarias.
- Establecer un plan de acción de seguridad de la información, definiendo los objetivos, metas y plazos para la implementación de controles de seguridad y medidas de mitigación.

3.3.2. Hacer.

Para esta parte se implementará los controles de seguridad y las medidas de mitigación definidas en la etapa de planificación, incluyendo la instalación de software y hardware de seguridad, con su respectiva configuración de cortafuegos. La parte práctica de esta **sección se muestra en la parte de muestras de resultados de este documento.**

También se elaboró la implementación de un reglamento con políticas y evaluación de riesgos **que se muestran en la parte de muestra de resultados en este documento.** En estos de forma general se proporcionará formación y concienciación en seguridad de la información a todos los empleados y terceros que tengan acceso a los sistemas de información del banco y definir y documentar los procedimientos y normas para el uso de los sistemas de información y los servicios de tecnología de la información del banco.

3.3.3. Verificar.

Se tendrán que realizar las siguientes actividades:

- Realizar auditorías internas periódicas para verificar el cumplimiento de los controles de seguridad y las políticas de seguridad.
- Realizar pruebas de penetración y vulnerabilidades para identificar posibles brechas de seguridad en el sistema de información.
- Realizar análisis de incidentes de seguridad y reportarlos para identificar posibles mejoras en los controles y medidas de mitigación existentes.

3.3.4. Actuar.

Se tomarán medidas correctivas en caso de incumplimiento de las políticas de seguridad de la información o cuando se identifiquen vulnerabilidades o brechas de seguridad.

También se realizarán actualizamientos y mejoramientos continuos en los controles y medidas de mitigación en respuesta a los cambios en el entorno de amenazas o a las vulnerabilidades identificadas a lo largo de la vida de la empresa.

Y finalmente se revisarán y actualizarán regularmente la política de seguridad de la información para garantizar su relevancia y efectividad.

Este SGSI P-H-V-A es un proceso continuo y constante, por lo que se debe repetir y

actualizar regularmente para asegurarse de que el banco esté protegido contra las amenazas de seguridad de la información en constante evolución.

Fases		Pasos	Objetivos Específicos
Planificar	Planear el SGSDP	1. Alcance y objetivos 2. Política de gestión de datos personales 3. Funciones y obligaciones de quienes traten datos personales 4. Inventario de datos personales 5. Análisis de riesgos de los datos personales 6. Identificación de las medidas de seguridad y análisis de brecha	Definir los objetivos, políticas, procesos y procedimientos relevantes del SGSDP para gestionar los riesgos de los datos personales, con el fin de cumplir con la legislación sobre protección de datos y obtener resultados acordes con las políticas y objetivos generales de la organización.
Hacer	Implementar y operar el SGSDP	7. Implementación de las medidas de seguridad aplicables a los datos personales	Implementar y operar las políticas, objetivos, procesos y procedimientos del SGSDP, así como sus controles o mecanismos con indicadores de medición.
Verificar	Monitorear y revisar el SGSDP	8. Revisiones y auditoría	Evaluar y medir el cumplimiento del proceso de acuerdo con la legislación de protección de datos personales, la política, los objetivos y la experiencia práctica del SGSDP, e informar los posibles ajustes necesarios.
Actuar	Mejorar el SGSDP	9. Mejora continua y Capacitación	Para lograr la mejora continua se deben adoptar medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión por parte de la Alta Dirección, las auditorías al SGSDP y de la comparación con otras fuentes de información relevantes, como actualizaciones regulatorias, riesgos e impactos organizacionales, entre otros. Adicionalmente, se debe considerar la capacitación del personal.

4. Reglamento de la organización.

4.1. Introducción al reglamento.

Este reglamento tiene como objetivo establecer las normas y directrices para el uso adecuado y seguro de las tecnologías de la información y la comunicación (TICs) en el banco. El cumplimiento de este reglamento es obligatorio para todos los empleados y terceros que tengan acceso a los sistemas de información del banco.

4.2. Uso de equipos y dispositivos de TICs.

4.2.1. Ámbito de aplicación.

Este reglamento se aplica a todos los empleados y cualquier otro individuo que utilice los equipos de IT propiedad de la organización.

4.2.2. Uso adecuado de los equipos IT.

Los empleados deben utilizar los equipos de IT con fines laborales y en relación con las actividades propias de su trabajo. El uso personal de los equipos de IT está prohibido.

4.2.3. Propiedad y responsabilidad.

Todos los equipos de IT, incluyendo hardware, software, redes y otros recursos similares, son propiedad de la organización. Los empleados son responsables del uso adecuado y eficiente de los equipos de IT y deben protegerlos contra el acceso no autorizado, el uso indebido y el daño.

4.2.4. Acceso y autorización.

El acceso a los equipos de IT de la organización se otorga según las necesidades de cada usuario y se basa en el principio de necesidad mínima. Los empleados deben cumplir con las políticas de acceso y autorización de la organización y no deben compartir sus credenciales de acceso con terceros.

4.2.5. Uso personal y prohibido.

El uso personal de los equipos de IT de la organización está prohibido, salvo en casos excepcionales y autorizados por la dirección. Los empleados deben cumplir con las políticas de uso aceptable de la organización y no deben utilizar los equipos de IT para fines ilegales, inmorales, inapropiados, ofensivos o contrarios a los intereses de la organización.

4.2.6. Seguridad de la información.

Los empleados deben tomar medidas razonables para proteger la información confidencial y privada de la organización de la divulgación no autorizada o el acceso no autorizado. Esto incluye el uso de contraseñas seguras, no compartir información confidencial con terceros no autorizados, no descargar software o archivos no autorizados y no enviar información confidencial por correo electrónico o en línea.

4.2.7. Monitoreo y registro.

La organización se reserva el derecho de monitorear y registrar el uso de los equipos de IT por parte de los empleados. Los empleados deben cumplir con las políticas de monitoreo y registro de la organización y no deben intentar evadir o eludir dichas políticas.

4.2.8. Mantenimiento y actualización.

Los empleados deben informar a la organización inmediatamente si se produce algún problema con los equipos de IT y deben permitir que la organización realice mantenimiento y actualizaciones periódicas para garantizar que los equipos estén en óptimas condiciones.

4.2.9. Cumplimiento.

Cualquier incumplimiento de este reglamento puede resultar en medidas disciplinarias, incluyendo la terminación del empleo o la revocación del acceso a los equipos de IT de la organización.

4.3. Uso de Internet y correo electrónico.

4.3.1. Ámbito de aplicación.

Este reglamento se aplica a todos los empleados y cualquier otro individuo que utilice la red de Internet y correo electrónico propiedad de la organización.

4.3.2. Uso adecuado de Internet y correo electrónico.

Los empleados deben utilizar la red de Internet y correo electrónico con fines laborales y en relación con las actividades propias de su trabajo. El uso personal de la red de Internet y correo electrónico está prohibido.

4.3.3. Propiedad y responsabilidad.

La red de Internet y correo electrónico son propiedad de la organización. Los empleados son responsables del uso adecuado y eficiente de la red de Internet y correo electrónico y deben protegerla contra el acceso no autorizado, el uso indebido y el daño.

4.3.4. Acceso y autorización.

El acceso a la red de Internet y correo electrónico se otorga según las necesidades de cada usuario y se basa en el principio de necesidad mínima. Los empleados deben cumplir con las políticas de acceso y autorización de la organización y no deben compartir sus credenciales de acceso con terceros.

4.3.5. Uso personal y prohibido.

El uso personal de la red de Internet y correo electrónico de la organización está prohibido, salvo en casos excepcionales y autorizados por la dirección. Los empleados deben cumplir con las políticas de uso aceptable de la organización y no deben utilizar la red de Internet y correo electrónico para fines ilegales, inmorales, inapropiados, ofensivos o contrarios a los intereses de la organización.

4.3.6. Seguridad de la información.

Los empleados deben tomar medidas razonables para proteger la información confidencial y privada de la organización de la divulgación no autorizada o el acceso no autorizado. Esto incluye el uso de contraseñas seguras, no compartir información confidencial con terceros no autorizados, no descargar software o archivos no autorizados y no enviar información confidencial por correo electrónico o en línea.

4.3.7. Monitoreo y registro.

La organización se reserva el derecho de monitorear y registrar el uso de la red de Internet y correo electrónico por parte de los empleados. Los empleados deben cumplir con las políticas de monitoreo y registro de la organización y no deben intentar evadir o eludir dichas políticas.

4.3.8. Correo electrónico.

Los empleados deben utilizar el correo electrónico con moderación y no deben enviar correos electrónicos masivos sin autorización. Los empleados deben cumplir con las políticas de uso aceptable de la organización y no deben enviar correos electrónicos ofensivos, ilegales o inapropiados.

4.3.9. Cumplimiento.

Cualquier incumplimiento de este reglamento puede resultar en medidas disciplinarias, incluyendo la terminación del empleo o la revocación del acceso a la red de Internet y correo electrónico de la organización.

4.3.10. Descarga e instalación de contenido.

Queda prohibido el uso de programas para descargar o copiar de Internet archivos de procedencia no segura o ilegal (Anexo 1). Por estos motivos también queda prohibido instalar y ejecutar programas que permitan el intercambio de archivos (Anexo 2).

4.4. Reglamento de empleados.

4.4.1. La empresa asigna a los **empleados** los equipos y sistemas de información básicos necesarios para la ejecución de sus actividades laborales con la aprobación de la autoridad respectiva, convirtiéndose en los responsables de estos recursos.

4.4.2. El acceso a los equipos y servicios tiene por objetivo brindar facilidades para cumplir con los fines laborales de cada área o ambiente en los que se asignaron.

4.4.3. Cada **empleado** tiene el deber de: respetar y custodiar la integridad de los equipos informáticos asignados, cumplir las políticas implementadas en este documento.

4.4.4. Las violaciones a las políticas y disposiciones establecidas en este reglamento con respecto al uso, operatividad y disponibilidad de los recursos informáticos, puede originar en la restricción u otras acciones disciplinarias o legales por parte de la empresa, no asume responsabilidad alguna por el mal uso de los recursos informáticos asignados a los **empleados**, sin embargo como propietaria de equipos y sistemas de información, puede disponer de la información generada en ellos para apoyar las acciones disciplinarias y legales que crea convenientes en caso que se vea afectada por acciones de desprestigio por parte de los usuarios.

4.4.5. Aceptar cualquier cuenta o utilizar cualquier sistema de información se

constituye en aceptación de esta política por parte de los **empleados**, aun desconociendo este reglamento, por tal motivo se solicita a los usuarios de estos recursos el respeto y colaboración para el cumplimiento de las normas que a continuación se manifiestan.

5. Tipos de usuario

5.1 Usuario: Es el nivel más básico de usuario. Se refiere a todo aquel usuario que se registra en los sistemas o se conecta autorizadamente a la red. Tiene acceso a la información que es completamente pública y a funciones de cliente. No tiene privilegios para realizar cambios en la información de la organización. Pueden auto-registrarse.

5.2 Empleado: Se refiere a todo aquel usuario que realiza actividades laborales en la organización, tiene derechos de modificación de la información conforme y limitadamente a las actividades que realiza con fines laborales, por ejemplo, control de inventarios. Su acceso a la información es mayor al de un usuario básico, teniendo acceso a información de uso interno, limitándose a la necesaria para la realización de sus actividades laborales.

5.3 Ejecutivo: Se refiere a todo aquel integrante de la alta dirección, tiene derecho de acceso y modificación de información confidencial limitada a la necesaria para la realización de sus actividades laborales. Puede agregar empleados o ejecutivos.

5.4 Administrador: Se refiere a aquellos integrantes de seguridad de la información que tienen derechos de acceso total y modificación a la información. Tiene control total sobre los usuarios (creación, modificación, bloqueo, eliminación).

6. Políticas.

6.1. Políticas de seguridad

Política:	Cualquier desperfecto que se detecte en la infraestructura de red interna debe reportarse y corregirse inmediatamente. Fecha: 07/06/23 Versión:0
Antecedentes: Los desperfectos que no se atienden a la brevedad suelen derivar en problemas más grandes, mucho más difíciles y costosos de solucionar.	
Implementación: Cualquier persona sea cual sea su posición en el organigrama de la organización debe reportar cualquier desperfecto que note en la infraestructura de red en el momento en el que la note a su superior inmediato o al departamento de mantenimiento.	
Procedimiento: La persona en cuestión debe llenar el formato de reporte general.	
Sanciones: Se informará al superior inmediato por comportamiento negligente.	

Política:	<p>El personal indicado debe atender cualquier desperfecto en la infraestructura de red interna inmediatamente.</p> <p>Fecha: 07/06/23 Versión:0</p>
<p>Antecedentes: Los desperfectos que no se atienden a la brevedad suelen derivar en problemas más grandes, mucho más difíciles y costosos de solucionar.</p>	
<p>Implementación: Los formatos de reporte general entregados, deberán hacerse llegar al departamento de TIC's a la brevedad para que se atienda el caso.</p>	
<p>Procedimiento: Si existe personal interno capacitado para la realización de la tarea, este debe atenderla inmediatamente, si no. La empresa deberá contratar personal externo para la resolución del problema.</p>	
<p>Sanciones: Se informará al superior inmediato del encargado de la sucursal donde no se cumplan las medidas establecidas, o se declaren como realizadas cuando no ha sido de esta manera, para que tome las acciones correspondientes.</p>	

Política:	<p>Cuando sea posible y viable, deben realizarse actualizaciones del software o hardware que lo requiera.</p> <p>Fecha: 07/06/23 Versión:0</p>
<p>Antecedentes: El software mejora con el paso del tiempo, así como las funciones y soluciones que ofrece, por lo anterior y por razones de seguridad el software debe actualizarse constantemente, así como actualizar los recursos de hardware en base al aumento del requerimiento del mismo.</p>	
<p>Implementación: Todos los equipos se configurarán para realizar las actualizaciones automáticamente de manera que no afecten el servicio o funcionalidad que ofrece, el equipo de TIC's deberá intervenir en los casos que esto no sea posible.</p>	

Procedimiento: El equipo de TIC's debe ser cuidadoso con el tipo de actualizaciones que se realicen, prefiriendo en primer plano aquellas que sean estrictamente necesarias (principalmente las de seguridad y funcionalidad) dejando con menos prioridad a las estéticas (las cuales obtendrán prioridad cuando se trate de software que está en contacto con los clientes y que por razones de negocio es necesario que destaquen en este aspecto), por ejemplo.

Se evaluará la relación costo-beneficio de realizar actualizaciones de hardware a los equipos para así determinar si es la mejor opción, en dado caso se solicitará la adquisición de recursos a la empresa.

Sanciones: Se informará al superior inmediato del encargado de la sucursal donde no se cumplan las medidas establecidas, o se declaren como realizadas cuando no ha sido de esta manera, para que tome las acciones correspondientes,

Política:

El personal de TIC's contratado por la empresa debe ser una persona con la experiencia necesaria para realizar las actividades que le correspondan con la menor probabilidad de error posible.

Fecha: 07/06/23 Versión:0

Antecedentes: Los errores humanos han causado grandes daños y pérdidas a las organizaciones, por lo que es crucial contar con el mejor personal posible dentro de la empresa.

Implementación: El departamento de recursos humanos en colaboración con el departamento de TIC's seleccionarán al mejor candidato aspirante a algún puesto de trabajo.

Procedimiento: El departamento de TIC's proporcionará las pruebas técnicas para que los aspirantes demuestren sus habilidades; y entregará los resultados al departamento de RH, quién complementando con las otras pruebas realizará la decisión final de la selección de personal.

Política:

El personal de TIC's contratado por la empresa debe recibir capacitación para las actividades que desempeñará en la misma.

Fecha: 07/06/23 Versión:0

Antecedentes: La capacitación previa de las actividades que se realizarán en un puesto de trabajo previene errores y asegura más el porcentaje de éxito disminuyendo el de error.

Implementación: El aspirante seleccionado para el puesto de trabajo recibirá una capacitación en su área de trabajo para que aprenda sus funciones antes de desempeñarlas.

Procedimiento: El personal de TIC's orientará al aspirante seleccionado en sus funciones principales para que se encuentre listo para realizarlas.

Política:

Cualquier desperfecto que se detecte en los sistemas de TI debe reportarse y corregirse inmediatamente.

Fecha: 07/06/23 Versión:0

Antecedentes: Los desperfectos que no se atienden a la brevedad suelen derivar en problemas más grandes, mucho más difíciles y costosos de solucionar.

Implementación: Cualquier persona sea cual sea su posición en el organigrama de la organización debe reportar cualquier desperfecto que note en los sistemas de TI en el momento en el que la note a su superior inmediato o al departamento de mantenimiento.

Procedimiento: La persona en cuestión debe llenar el formato de reporte general.

Política:

El personal indicado debe atender cualquier desperfecto en los sistemas de TI inmediatamente.

Fecha: 07/06/23 Versión:0

Antecedentes: Los desperfectos que no se atienden a la brevedad suelen derivar en problemas más grandes, mucho más difíciles y costosos de solucionar.

Implementación: Los formatos de reporte general entregados, deberán hacerse llegar al departamento de TIC's a la brevedad para que se atienda el caso.

Procedimiento: Si existe personal interno capacitado para la realización de la tarea, este debe atenderla inmediatamente, si no. La empresa deberá contratar personal externo para la resolución del problema.

Política:

La empresa debe especificar a sus usuarios las consecuencias de acceder o usar la información sin autorización.

Fecha: 07/06/23 Versión:0

Antecedentes: Los empleados que no conocen las consecuencias de realizar actos prohibidos dentro de la empresa pueden llegar a creer que no pasará nada grave si lo hacen y tener altas probabilidades de hacerlo.

Implementación: El departamento de recursos humanos debe informar a los empleados las cosas que están prohibidas dentro de la empresa, así como sus consecuencias en caso de que cometan la falta.

Procedimiento: El departamento de recursos humanos informará a los empleados durante su proceso de selección, así como en sus reglamentos.

Política:	Cada empleado tiene acceso únicamente a su usuario. Fecha: 07/06/23 Versión:0
Antecedentes: Los incidentes son más fáciles de manejar cuando se identifica al usuario que los está llevando a cabo.	
Implementación: El departamento de TIC's creará un usuario único para cada empleado de la empresa.	
Procedimiento: El departamento de TIC's proporcionará al empleado su usuario de acceso el cual no debe ser compartido ni utilizado por ninguna otra persona en la empresa.	

Política:	<p>Los sistemas de TI deben manejar los permisos dependiendo de cada tipo de usuario.</p> <p>Fecha: 07/06/23 Versión:0</p>
<p>Antecedentes: El manejo de permisos resulta muy útil dentro de los sistemas de TI para que los usuarios no realicen operaciones para las que no están autorizados.</p>	
<p>Implementación: Los permisos de usuario se manejan por grupo de usuarios dependiendo del tipo de empleado o por usuario en lo individual para casos particulares.</p>	
<p>Procedimiento: El departamento de TIC's asignará a cada usuario los permisos que le correspondan.</p>	

Política:	<p>El personal de seguridad de la información deberá revisar las bitácoras de los sistemas para descartar ataques externos en caso de un uso o acceso no autorizado a la información.</p> <p>Fecha: 07/06/23 Versión:0</p>
<p>Antecedentes: Los atacantes pueden esconder su actividad detrás de un usuario autorizado para tratar de disimular su presencia.</p>	
<p>Implementación: El personal de TIC's debe revisar las bitácoras que tenga disponibles para identificar un posible vector de ataque.</p>	
<p>Procedimiento: El personal de TIC's revisará las bitácoras de servicios principalmente de red como lo son el Firewall o el IDS, para descartar un posible ataque.</p>	

Política:	<p>El usuario del empleado que realice algún acceso no autorizado a la información debe ser bloqueado de todos los sistemas de TI inmediatamente.</p> <p>Fecha: 07/06/23 Versión:0</p>
------------------	--

<p>Antecedentes: Es posible que cuando una persona logre realizar un acceso no autorizado quiera intentar hacerlo de nuevo.</p>
<p>Implementación: Cuando se detecte un acceso no autorizado por parte del personal, debe darse aviso inmediato al personal de TI.</p>
<p>Procedimiento: El personal de TI bloqueará inmediatamente de todos los sistemas al infractor.</p>

Política:	Cada empleado debe ser capacitado sobre el uso de la información en la empresa. Fecha: 07/06/23 Versión:0
Antecedentes: Los usuarios no suelen ser conscientes de los riesgos de seguridad para la información, por lo que estos deben ser capacitados acerca de cómo protegerla.	
Implementación: El personal de seguridad de la información capacitará al personal de la empresa en cuestión al uso de la información.	
Procedimiento: El personal de seguridad de la información llevará a cabo sesiones informativas en las que se proporcione al resto de la empresa información sobre cómo cuidar la información de la empresa.	

Política:	La empresa debe especificar a sus usuarios las consecuencias de realizar un daño a la infraestructura de TI. Fecha: 07/06/23 Versión:0
Antecedentes: Los empleados que no conocen las consecuencias de realizar actos prohibidos dentro de la empresa pueden llegar a creer que no pasará nada grave si lo hacen y tener altas probabilidades de hacerlo.	
Implementación: El departamento de recursos humanos debe informar a los empleados las cosas que están prohibidas dentro de la empresa, así como sus consecuencias en caso de que cometan la falta.	
Procedimiento: El departamento de recursos humanos informará a los empleados durante su proceso de selección, así como en sus reglamentos.	

Política:	Se debe realizar una detección de vulnerabilidades a los equipos de TI al menos una vez al mes. Fecha: 07/06/23 Versión:0
Antecedentes: Las vulnerabilidades están apareciendo todo el tiempo, por lo que es necesario verificar periódicamente que no aparezcan en nuestros equipos.	
Implementación: El personal de seguridad de la información realizará escaneos de vulnerabilidades en los equipos de TI.	
Procedimiento: El personal de seguridad de la información escaneará los servicios web con nikto y los equipos con nmap para así detectar las vulnerabilidades.	

Política:	Se debe realizar hardening a todos los equipos de TI cada vez que sea necesario. Fecha: 07/06/23 Versión:0
Antecedentes: Una medida para mitigar los riesgos de nuestros equipos es hacer hardening de las vulnerabilidades.	
Implementación: Las vulnerabilidades detectadas deberán ser corregidas.	
Procedimiento: El personal de seguridad de la información realizará el hardening de las vulnerabilidades en cuanto sea consciente de ellas.	

Política:	La comunicación debe estar regulada por un firewall. Fecha: 07/06/23 Versión:0
Antecedentes: La comunicación debe estar regulada por un firewall.	
Implementación: Aplicación de firewall y sus reglas correspondientes.	
Procedimiento: El personal de seguridad de la información configurará el firewall en base a las políticas de tráfico.	

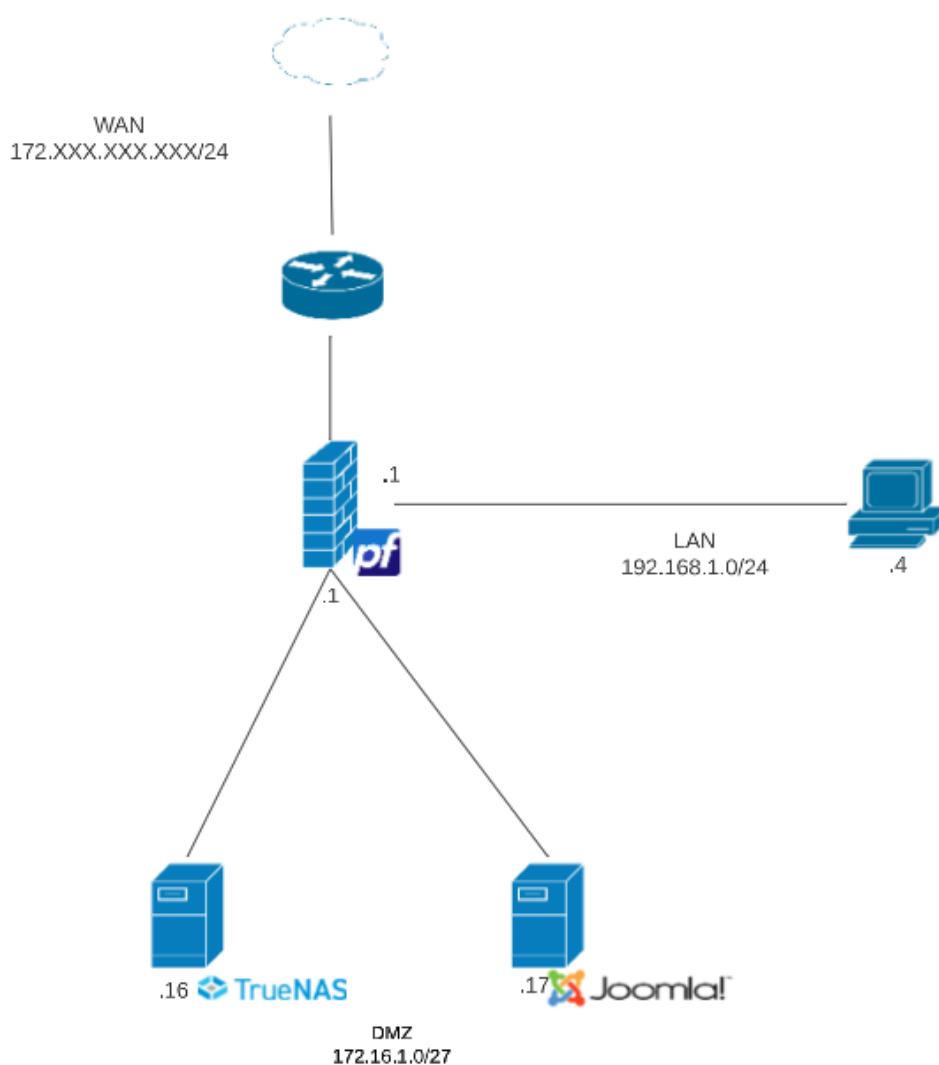
Política:

Los accesos remotos deben estar configurados de manera que solo el administrador pueda conectarse.

Fecha: 07/06/23 Versión:0

Antecedentes: Los ataques a servicios remotos pueden llegar a ser muy dañinos para las empresas, por lo que aumentar su seguridad es lo mejor que puede hacerse.

Implementación: La infraestructura de red deberá implementarse en base a la siguiente topología segura.



Procedimiento: El personal de TIC's llevara a cabo las instalaciones y configuraciones correspondientes teniendo en cuenta la presente política.
Implementación: Los servicios remotos deben únicamente permitir conexiones del administrador de red.
Procedimiento: El personal de seguridad de la información configurará los servicios y el firewall para que solo permita conexiones del administrador.

Política:	<p>Los servidores deben encontrarse en una DMZ y los equipos de las sucursales en una LAN dividida en VLANs por áreas de trabajo.</p> <p>Fecha: 07/06/23 Versión:0</p>
Antecedentes:	Una topología segura puede ayudar a mitigar el posible daño a la empresa.

Política:	<p>La empresa debe implementar un sistema IDS/IPS para hacer frente a ataques DOS y DDOS.</p> <p>Fecha: 07/06/23 Versión:0</p>
Antecedentes:	Los ataques DOS y DDOS pueden dejar a una empresa sin servicio, por lo que es necesario prevenir este tipo de ataques.
Implementación:	La empresa contará con sistemas IDS/IPS en sus servicios.
Procedimiento:	El personal de seguridad de la información deberá configurar estos sistemas para que mitiguen el riesgo de ocurrencia de este tipo de ataques.

6.2. Tráfico en la red

Con la finalidad de cumplir las *políticas generales de seguridad* y los *objetivos, misión y visión del SGSI* se definen las siguientes políticas de tráfico de red que deberán ser reguladas por el UTM para que sean cumplidas por los usuarios de la red. Las reglas definidas a continuación se basan en la topología segura previamente definida.

Tráfico en General:

Política:	El único tráfico permitido desde el exterior de la red de la organización (Internet por la interfaz WAN) hacia la DMZ será de acceso a los servicios que la organización ofrece y pública al internet. Fecha: 07/06/23 Versión:0
Antecedentes: Los ataques remotos a servicios pueden comprometer los activos de información a niveles críticos. Un NAT mal configurado puede permitir a atacantes enviar trafico malicioso a puertos o servicios que ni siquiera son usados al exterior de la red.	
Implementación: Las reglas de NAT en el firewall solo permitirán solicitudes a los servicios que la organización quiera brindar a internet. No debe permitirse el trafico hacia otros puertos o activos.	
Procedimiento: El personal de seguridad de la información configurará las reglas del firewall para que solo permita solicitudes desde internet a los servicios que la organización decida brindar.	

Política:	Ningún cliente de la LAN debe recibir trafico (a menos que sea de respuesta) desde Internet. Fecha: 07/06/23 Versión:0
Antecedentes: Los equipos en la LAN pueden pertenecer a personal de la alta dirección de la organización y/o contener información confidencial y crítica para la continuidad de negocio. Por lo que cualquier acceso no autorizado o compromiso a los activos podría comprometer críticamente a la organización.	
Implementación: Las reglas del firewall solo permitirán tráfico de respuesta a los activos en la LAN, cualquier otro intento de tráfico en ese sentido debe ser bloqueado.	

Procedimiento: El personal de seguridad de la información configurará las reglas del firewall para que cumpla con lo definido en la presente política.

Política:

Los servidores deben tener acceso a internet exclusivamente para actualizaciones o con objetivo de brindar los servicios autorizados.

Antecedentes: Los servicios deben actualizarse constantemente para recibir parches de seguridad a las vulnerabilidades que pudieran contener. De esta manera se logra mantener seguros a los activos.

Implementación: Las reglas del firewall deben permitir las solicitudes de los servidores a internet. Pero el reglamento debe especificar que solo esta permitido para los fines establecidos en la presente política y penar el tráfico indebido.

Procedimiento: El personal de seguridad de la información configurará las reglas del firewall para que cumpla con lo definido en la presente política.

Política:	El tráfico de la DMZ hacia la LAN sólo se permite cuando es en respuesta a los servicios previamente solicitados. Fecha: 07/06/23 Versión:0
Antecedentes: La segmentación de la red tiene como finalidad minimizar los posibles daños de un ataque. Un atacante que pudiera comprometer un activo de la DMZ o tener acceso a ella no debe poder alcanzar desde ahí a los activos de la LAN.	
Implementación: Las reglas del firewall deben restringir el tráfico de DMZ -> LAN limitado a solo respuesta.	
Procedimiento: El personal de seguridad de la información configurará las reglas del firewall para que cumpla con lo definido en la presente política.	

Política:	El tráfico de la LAN hacia internet se permite solo con fines laborales. Fecha: 07/06/23 Versión:0
Antecedentes: El personal requiere de comunicación a internet para realizar sus labores, pero el tráfico se limita solo a esta finalidad, ya que un uso distinto a este aumenta los riesgos de ataque.	

Implementación: Las reglas del firewall deben permitir el tráfico LAN -> INTERNET con fines laborales cualquier uso distinto está sancionado. Los sitios explícitamente prohibidos serán bloqueados desde el UTM.

Procedimiento: El personal de seguridad de la información configurará las reglas del firewall para que cumpla con lo definido en la presente política.

Política:

El tráfico de la LAN hacia la DMZ está permitido solo hacia los servicios. El acceso administrativo está permitido únicamente para el Administrador autorizado. Fecha: 07/06/23 Versión:0

Antecedentes: Los clientes en la LAN podrían requerir de servicios hospedados en la DMZ. Sin embargo, el tráfico debe limitarse únicamente a estos ya que un acceso mayor podría aumentar las posibilidades de un ataque en esta dirección.

Implementación: Las reglas del firewall deben permitir el tráfico LAN -> DMZ para acceder a los servicios. El acceso administrativo es exclusivo para el/los administrador/es autorizado/s.

Procedimiento: El personal de seguridad de la información configurará las reglas del firewall para que cumpla con lo definido en la presente política.

Una tabla simplificada de las políticas generales de tráfico se ve de la siguiente manera:

Origen	Destino	Política
WAN (Internet)	DMZ (Sólo Servicios)	Permitido
WAN (Internet)	LAN (Clientes)	Denegado
DMZ (Servidores)	WAN (Internet)	Permitido
DMZ (Servidores)	LAN (Clientes)	Denegado
LAN (Clientes)	WAN (Internet)	Permitido

LAN (Clientes)	DMZ (Servicios) (Admin, acceso administrativo)	Permitido
----------------	--	-----------

6.3. Políticas de acceso para los usuarios según su perfil.

6.3.1. Políticas de Usuario.

Política:	<p>Los usuarios tienen acceso limitado a la red y solo pueden acceder a recursos específicos, como correo electrónico y navegación web.</p> <p>Fecha: 07/06/23 Versión:0</p>
Antecedentes:	<p>La política de usuario que establece el acceso limitado a la red para los usuarios tiene como objetivo proteger los recursos de la red y mantener la seguridad de la información. Los usuarios pueden ser la puerta de entrada para que los atacantes accedan a la red, por lo que restringir su acceso es una medida importante para evitar vulnerabilidades y proteger la red.</p>
Implementación:	<p>Identificar los recursos de la red que estarán disponibles para los usuarios, crear un grupo de usuarios en el servidor de la red y asignar los permisos necesarios ,restringir el acceso a otros recursos de la red, configurar el firewall de la red para bloquear el acceso no autorizado a la red y permitir solo el acceso a los recursos identificados, establecer políticas de contraseñas seguras para los usuarios, establecer políticas de seguridad para los dispositivos móviles, como requerir autenticación y encriptación de los datos</p>
Procedimiento:	<p>Monitorear el acceso de los usuarios a los recursos de la red y asegurarse de que estén accediendo solo a los recursos autorizados.</p>

Política:	<p>Política de contraseñas.</p> <p>Fecha: 07/06/23 Versión:0</p>
Antecedentes:	<p>La política de contraseñas es una de las medidas de seguridad más importantes para proteger los sistemas de información de una organización. Una contraseña fuerte y segura reduce el riesgo de ataques de hackers y evita que los usuarios no autorizados accedan a los sistemas y datos de la organización.</p>

Implementación: los usuarios deben tener contraseñas seguras y deben cambiarlas regularmente

Procedimiento: Definir los requisitos de complejidad de la contraseña, establecer caducidad de la contraseña, configurar bloqueos después de varios intentos, establecer historial de contraseñas, configurar la verificación de contraseñas al crearlas y al cambiarlas, educar a los usuarios sobre cómo crear y mantener contraseñas seguras, revisar regularmente la política y realizar ajustes según sea necesario

Política:	Política de tiempo de sesión. Fecha: 07/06/23 Versión:0
------------------	--

Antecedentes:

los usuarios pueden dejar sus sesiones abiertas por largos períodos de tiempo, lo que aumenta la posibilidad de que un atacante pueda acceder a la sesión y obtener información crítica. Además, si un usuario deja su sesión abierta en un sistema público o compartido, cualquier persona podría acceder a su cuenta y realizar actividades maliciosas.

Implementación: se debe establecer un tiempo límite para las sesiones de usuario para evitar el acceso no autorizado a los recursos de la red.

Procedimiento:

Identificar los sistemas que contienen información sensible y los sistemas que están conectados a Internet.

Determinar el tiempo máximo de duración de la sesión en función de los riesgos y necesidades de la organización.

Configurar la política de tiempo de sesión a nivel de sistema en cada uno de los sistemas identificados.

Informar a los usuarios de la política de tiempo de sesión y las consecuencias de incumplirla.

Monitorear el cumplimiento de la política de tiempo de sesión y tomar medidas adecuadas en caso de incumplimiento.

Política:	Política de puertos y servicios. Fecha: 07/06/23 Versión:0
Antecedentes: Evitar la exposición a amenazas y riesgos cibernéticos, ya que algunos puertos y servicios pueden ser explotados por los atacantes para obtener acceso no autorizado a la red y comprometer la seguridad de la organización.	
Implementación: se deben restringir los puertos y servicios a los que los usuarios pueden acceder para reducir el riesgo de vulnerabilidades de seguridad.	
Procedimiento: Identificar los puertos y servicios que son necesarios para el funcionamiento normal de la red. Evaluar los riesgos asociados con cada puerto y servicio y determinar si se deben restringir o bloquear.	

6.3.2. Políticas de Empleado.

Política:	Los empleados tienen acceso más amplio a la red que los usuarios y pueden acceder a recursos adicionales como bases de datos y aplicaciones de negocio. Fecha: 07/06/23 Versión:0
Antecedentes: La política de empleado se implementa en organizaciones donde los empleados requieren acceso a recursos específicos de la empresa para llevar a cabo sus funciones. Esta política se implementa para garantizar la seguridad y protección de los datos empresariales y limitar el acceso solo a aquellos empleados que tienen una necesidad legítima de acceder a ellos.	
Implementación: definir roles y permisos específicos para diferentes tipos de empleados en la organización. Los empleados pueden clasificarse en diferentes niveles según su función y responsabilidades.	
Procedimiento: Identificar los diferentes niveles de empleados y las funciones específicas de cada nivel. Definir los recursos a los que cada nivel de empleado debe tener acceso. Implementar medidas de seguridad adicionales para restringir el acceso no autorizado a los datos empresariales.	

<p>Configurar permisos de acceso y autenticación de usuarios para cada recurso.</p> <p>Establecer procedimientos para administrar y monitorear el acceso de los empleados a los recursos.</p>	
Política:	<p>Política de autenticación</p> <p>Fecha: 07/06/23 Versión:0</p>
<p>Antecedentes:</p> <p>validar la identidad de un usuario que intenta acceder a un sistema o recurso. Es esencial tener una política de autenticación clara y efectiva para garantizar que solo los usuarios autorizados puedan acceder a los recursos de la empresa.</p>	
<p>Implementación: se debe utilizar la autenticación multifactorial para garantizar que solo los empleados autorizados tengan acceso a los recursos de la red.</p>	
<p>Procedimiento:</p> <p>Selección del método de autenticación adecuado, Configuración del sistema de autenticación, Creación de políticas de contraseñas, Capacitación de los usuarios, y Auditoría y revisión regular.</p>	

Política:	<p>Política de privacidad</p> <p>Fecha: 07/06/23 Versión:0</p>
<p>Antecedentes:</p> <p>es necesario contar con una política de privacidad clara y efectiva para proteger la información y la privacidad de los empleados y clientes.</p>	
<p>Implementación: se deben establecer políticas claras para el uso y acceso de datos confidenciales de la empresa, y los empleados deben estar capacitados en las mejores prácticas de privacidad.</p>	
<p>Procedimiento:</p> <p>Identificar los datos personales que se manejan en la empresa y los empleados que tienen acceso a ellos.</p> <p>Establecer los procedimientos y controles necesarios para proteger la</p>	

información, incluyendo la gestión de contraseñas, la encriptación de datos y la restricción de acceso a los datos sensibles.

Implementar medidas para garantizar la exactitud y actualidad de los datos personales.

Establecer los procedimientos para notificar a los empleados sobre el uso y la divulgación de sus datos personales.

Establecer los procedimientos para que los empleados puedan acceder y corregir sus datos personales.

Establecer los procedimientos para manejar las quejas y las violaciones de la privacidad.

Política:	Política de monitoreo. Fecha: 07/06/23 Versión:0
Antecedentes: establece para asegurar que los empleados estén cumpliendo con las normas y regulaciones de la empresa, además de garantizar la seguridad y protección de los activos de la organización. A través del monitoreo, se pueden detectar y prevenir actividades maliciosas, como el robo de información, el uso indebido de los recursos de la empresa y la violación de la política de seguridad.	
Implementación: se debe monitorear el tráfico de red de los empleados para detectar actividad sospechosa y prevenir amenazas internas. Para implementar una política de monitoreo, es necesario establecer un conjunto de reglas y procedimientos que se aplicarán a todos los empleados. Esto incluye el uso de herramientas de monitoreo y la definición de los parámetros de monitoreo, como los sitios web y aplicaciones que se monitorean, los archivos y directorios que se monitorean y los eventos que se registran.	
Procedimiento: Establecer los objetivos de monitoreo: definir los objetivos y los resultados esperados del monitoreo. Identificar los recursos que se monitorearán: identificar los recursos de la empresa que se monitorearán, como sistemas, dispositivos y aplicaciones. Definir los parámetros de monitoreo: definir los parámetros de monitoreo, como las aplicaciones y sitios web que se monitorearán, los archivos y directorios que se monitorearán y los eventos que se registrarán. Seleccionar las herramientas de monitoreo: seleccionar las herramientas de monitoreo que se utilizarán para llevar a cabo el monitoreo. Notificar a los empleados: notificar a los empleados que la empresa lleva a	

cabo monitoreo y explicarles las razones detrás de la política.

Monitorear y analizar: monitorear los recursos y analizar los resultados obtenidos para detectar posibles violaciones de seguridad o incumplimientos de las políticas.

Tomar medidas: tomar medidas adecuadas en caso de detectar violaciones o incumplimientos, como la aplicación de sanciones disciplinarias o la implementación de medidas correctivas.

6.3.3. Políticas de Ejecutivo.

Política:	Los ejecutivos tienen acceso a recursos críticos de la red, como bases de datos y servidores de archivos Fecha: 07/06/23 Versión:0
Antecedentes: La política de Ejecutivo es una política de seguridad de la información que se aplica a los ejecutivos de la organización. Los ejecutivos tienen acceso a recursos críticos de la red, como bases de datos y servidores de archivos, lo que hace que su acceso deba ser restringido y protegido adecuadamente. Los antecedentes de esta política son la necesidad de garantizar que los recursos críticos estén protegidos y sean accesibles solo para personas autorizadas.	
Implementación: La política de Ejecutivo se implementa mediante la asignación de permisos y roles de acceso adecuados a los ejecutivos de la organización. Se deben establecer mecanismos de autenticación y autorización sólidos para garantizar que solo los ejecutivos autorizados tengan acceso a los recursos críticos. Los controles de acceso físico y lógico también deben ser establecidos y monitoreados regularmente.	
Procedimiento: Identificación de los recursos críticos de la red que solo deben ser accesibles por los ejecutivos. Identificación de los ejecutivos que requieren acceso a los recursos críticos de la red. Asignación de roles y permisos adecuados a los ejecutivos para garantizar un acceso controlado a los recursos críticos. Establecimiento de mecanismos de autenticación y autorización sólidos para garantizar que solo los ejecutivos autorizados tengan acceso a los recursos críticos. Establecimiento de controles de acceso físico y lógico para garantizar que solo los ejecutivos autorizados puedan acceder a los recursos críticos.	

Monitoreo regular de los accesos a los recursos críticos para detectar posibles violaciones de seguridad y tomar medidas correctivas.

Política:	Política de autenticación. Fecha: 07/06/23 Versión:0
Antecedentes: verificar la identidad de los ejecutivos que intentan acceder a recursos críticos de la red. Los antecedentes de esta política son la necesidad de proteger los recursos de la red de accesos no autorizados y asegurar la integridad y confidencialidad de la información crítica almacenada en la red.	
Implementación: se debe utilizar la autenticación multifactorial y el acceso debe ser restringido solo a los ejecutivos autorizados.	
Procedimiento: Identificación de los recursos críticos de la red a los que solo los ejecutivos tienen acceso. Identificación de los usuarios que tienen acceso a estos recursos críticos. Establecimiento de un proceso de autenticación que incluya la verificación de la identidad de los usuarios. Selección de los métodos de autenticación apropiados para los usuarios de los recursos críticos. Establecimiento de requisitos para las contraseñas, incluyendo complejidad, longitud y caducidad. Implementación de políticas de bloqueo de cuenta y notificación de actividades sospechosas. Capacitación y concientización de los ejecutivos sobre las políticas y procedimientos de autenticación. Evaluación periódica de la eficacia de las políticas y procedimientos de autenticación.	

Política:	Política de privacidad. Fecha: 07/06/23 Versión:0
------------------	--

<p>Antecedentes:</p> <p>Los ejecutivos son miembros importantes de la organización y tienen acceso a información confidencial y crítica de la empresa. Es importante que se implementen políticas de privacidad para garantizar que la información se mantenga segura y no sea accesible para personas no autorizadas.</p>
<p>Implementación: se deben establecer políticas claras para el uso y acceso de datos confidenciales de la empresa, y los ejecutivos deben estar capacitados en las mejores prácticas de privacidad.</p> <p>Se debe comenzar con una evaluación de los datos a los que tienen acceso y los riesgos asociados con su divulgación. Es importante establecer restricciones de acceso y medidas de seguridad para garantizar que solo los empleados autorizados puedan acceder a la información.</p>
<p>Procedimiento:</p> <p>Identificar los datos a los que los ejecutivos tienen acceso y evaluar los riesgos asociados con su divulgación.</p> <p>Establecer restricciones de acceso y medidas de seguridad para garantizar que solo los empleados autorizados puedan acceder a la información.</p> <p>Proporcionar capacitación y orientación a los ejecutivos sobre las políticas de privacidad y las medidas de seguridad que deben seguir.</p> <p>Monitorear regularmente el acceso y uso de la información por parte de los ejecutivos para detectar cualquier actividad sospechosa o inusual.</p> <p>Tomar medidas inmediatas si se detecta alguna violación de la política de privacidad, incluyendo la aplicación de sanciones disciplinarias y la notificación de las autoridades correspondientes si es necesario.</p>

<p>Política:</p>	<p>Política de monitoreo</p> <p>Fecha: 07/06/23 Versión:0</p>
<p>Antecedentes:</p> <p>La política de monitoreo para los ejecutivos se refiere a la supervisión y vigilancia de los recursos críticos de la red, como bases de datos y servidores de archivos, para garantizar que se estén utilizando de manera apropiada y que no se estén comprometiendo la seguridad de la empresa. El monitoreo se puede llevar a cabo mediante herramientas de software o hardware específicas que permiten a los administradores de red monitorear y registrar las actividades de los usuarios.</p>	

<p>Implementación: se debe monitorear continuamente la actividad de red de los ejecutivos para detectar cualquier actividad sospechosa.</p>
<p>Procedimiento:</p> <p>Monitoreo continuo: se debe monitorear continuamente el uso de los recursos críticos para detectar actividades sospechosas o inapropiadas.</p> <p>Análisis de los registros: se deben analizar regularmente los registros de monitoreo para detectar cualquier actividad sospechosa o inapropiada.</p> <p>Respuesta a las alertas: si se detecta actividad sospechosa o inapropiada, se debe tomar acción inmediata para investigar y responder a la situación.</p> <p>Actualización de la política: se debe actualizar regularmente la política de monitoreo para asegurarse de que está alineada con los objetivos y necesidades de la empresa, así como con las regulaciones y leyes aplicables.</p>

6.3.4. Políticas de Administrador.

<p>Política:</p>	<p>Los administradores tienen acceso completo a la red y los recursos protegidos por el firewall.</p> <p>Fecha: 07/06/23 Versión:0</p>
<p>Antecedentes:</p>	<p>La política de administrador es una política de seguridad que se enfoca en la protección de los recursos críticos de la organización. Los administradores tienen acceso completo a la red y, por lo tanto, pueden ser capaces de realizar cambios importantes y tener acceso a información confidencial. Por lo tanto, se requiere una política de administrador bien definida para garantizar que los administradores cumplan con los requisitos de seguridad y no comprometan los recursos de la organización.</p>
<p>Implementación:</p>	<p>se realiza a través de un conjunto de directrices y reglas que definen cómo se debe acceder a los recursos de la red y cómo se debe utilizar el acceso de administrador.</p> <p>Acceso controlado: El acceso de administrador debe estar controlado y limitado solo a aquellos usuarios que necesitan acceso a los recursos críticos.</p> <p>Autenticación fuerte: Los administradores deben autenticarse mediante una autenticación fuerte, como la autenticación multifactorial, para garantizar que solo los administradores autorizados tengan acceso.</p> <p>Seguimiento de actividad: La actividad de los administradores debe ser monitoreada y registrada para que se pueda detectar cualquier actividad sospechosa o maliciosa.</p>

Privilegios de acceso mínimos: Los administradores solo deben tener los privilegios necesarios para realizar sus tareas y no deben tener acceso a recursos que no necesitan.

Procedimiento:

Definir los requisitos de seguridad, Establecer roles y responsabilidades, Establecer políticas de acceso, Monitorear y registrar la actividad de los administradores y Actualizar regularmente las políticas.

Política:

Política de autenticación.

Fecha: 07/06/23 Versión:0

Antecedentes:

La política de autenticación para administradores se implementa para garantizar que solo personas autorizadas tengan acceso a las credenciales y privilegios de administración, reducir el riesgo de acceso no autorizado y prevenir posibles daños a la red y los sistemas.

Implementación: se debe monitorear continuamente la actividad de red de los ejecutivos para detectar cualquier actividad sospechosa.

Procedimiento:

Reunir los detalles de los administradores y sus roles en la organización.

Determinar los requisitos de autenticación seguros y establecer políticas de contraseñas robustas.

Establecer un proceso de aprobación para otorgar acceso a los administradores nuevos o existentes.

Configurar los sistemas para limitar el acceso de administración solo a los administradores autorizados y limitar el acceso remoto a través de VPN u otros mecanismos seguros.

Establecer una política de cambio de contraseña regular para los administradores.

Monitorear y auditar el acceso de administración para detectar actividades sospechosas y tomar medidas inmediatas si se detecta algún problema.

Política:	Política de cambio de contraseña Fecha: 07/06/23 Versión:0
<p>Antecedentes:</p> <p>La política de cambio de contraseña es una medida de seguridad fundamental para garantizar la integridad de las cuentas de administrador y prevenir el acceso no autorizado a los recursos de la red. Esta política se establece para asegurar que las contraseñas sean actualizadas regularmente y sean suficientemente seguras para resistir ataques de fuerza bruta y otras técnicas de hackeo.</p>	
<p>Implementación: los administradores deben cambiar sus contraseñas con regularidad y utilizar contraseñas seguras.</p> <p>Requiere que los administradores creen contraseñas fuertes y complejas para cada cuenta, que se cambien regularmente y que se mantengan en secreto. Las contraseñas deben tener al menos 8 caracteres, incluyendo números, letras mayúsculas y minúsculas, y símbolos especiales. Además, se debe implementar un sistema de expiración de contraseña que obligue a los administradores a cambiar sus contraseñas cada cierto tiempo, por ejemplo, cada 90 días.</p>	
<p>Procedimiento:</p> <p>El procedimiento para implementar la política de cambio de contraseña puede incluir los siguientes pasos:</p> <p>Crear una política de cambio de contraseña: Esto puede incluir definir la longitud y complejidad de la contraseña, la frecuencia de cambio y la política de reutilización de contraseñas antiguas.</p> <p>Notificar a los administradores sobre la política: Los administradores deben ser informados sobre la política de cambio de contraseña y las razones detrás de ella.</p> <p>Establecer un calendario de cambio de contraseña: Esto puede incluir programar fechas específicas para el cambio de contraseña y establecer recordatorios para los administradores.</p> <p>Monitorear el cumplimiento de la política: Los administradores deben ser supervisados para asegurar que están cumpliendo con la política de cambio de contraseña.</p> <p>En caso de incumplimiento: Si un administrador no cumple con la política de cambio de contraseña, se deben tomar medidas para remediar la situación, lo que puede incluir la revocación de privilegios de administrador o la imposición de sanciones disciplinarias.</p>	

Política:	Política de revisión de registros. Fecha: 07/06/23 Versión:0
Antecedentes: La política de revisión de registros es una parte crítica de cualquier estrategia de seguridad cibernética. Los registros son documentos electrónicos que se utilizan para registrar los eventos que se producen en un sistema informático. Estos eventos pueden ser acciones de usuario, errores del sistema, intentos de acceso no autorizado y otros incidentes de seguridad. La revisión de registros es importante porque proporciona información sobre cómo se han utilizado los recursos del sistema y si se han producido eventos de seguridad relevantes.	
Implementación: los administradores deben estar sujetos a revisiones periódicas de registros para garantizar la integridad de la red y la seguridad de los datos.	
Procedimiento: Recopilación de registros: Se recopilan registros del sistema que contienen información sobre eventos relevantes. Análisis de registros: Los registros se analizan en busca de patrones o eventos que puedan indicar una amenaza de seguridad. Alerta de eventos sospechosos: Si se detecta un evento sospechoso, se debe notificar al equipo de seguridad de la organización. Investigación del evento: Se investiga el evento sospechoso para determinar si se trata de una amenaza real de seguridad. Corrección de vulnerabilidades: Si se detecta una vulnerabilidad, se debe corregir para evitar futuros eventos de seguridad. Documentación: Se documentan todos los eventos relevantes y las medidas tomadas para abordarlos. Revisión periódica: Los registros se revisan periódicamente para detectar patrones o tendencias de seguridad y para asegurarse de que la política de revisión de registros sigue siendo efectiva.	

7. Identificación de activos

En la empresa se identificaron los siguientes activos

Equipo	Información y servicios que maneja
---------------	---

Servidor web local	Se encarga de ejecutar la capa de presentación de la página de la empresa (front-end), además de estar vinculada con los elementos de back-end.
Servidor de DB	Se encarga de administrar los datos para el almacenamiento de datos de los usuarios.
Equipos de cómputo	Son los equipos proporcionados por la empresa para que los trabajadores mantengan el acceso a los servicios que se proporcionan dentro de la organización.
Servidor de almacenamiento en red (Truenas)	Servicio establecido por la empresa que permite a sus usuarios almacenar información de forma segura, realizar backup, compartir archivos y mantener a salvo ficheros que contienen información sensible contra potenciales ciberataques.
Infraestructura de comunicación	Se encarga de proporcionar la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o una comunicación, ya sea ésta en forma de voz, datos, vídeo o una mezcla de los anteriores, entre los diferentes equipos informáticos de la compañía.

Firewall UTM (Pfsense)	Dispositivo encargado de regular el tráfico entre dos o más redes (Internet y red interna, o redes internas, Internet y DMZ), además de mantener reglas que permitan o no el acceso a cierto servicio, página web o desde el exterior al interior de la organización.
Las personas de la organización (Desarrolladores, usuarios operadores, clientes finales)	Se encarga de administrar y monitorizar el correcto funcionamiento del sistema incluyendo cambios de versiones, administración de acceso y realización de copias de respaldo.
Suministro eléctrico	Se encarga de proveer alimentación eléctrica de buena calidad a todos los equipos electrónicos que conforman el sistema de información de la compañía.
Sistema de protección contra descargas	Se encarga de proteger a las personas y de paso a los equipos informáticos de descargas eléctricas ocasionadas por descargas atmosféricas y corrientes parásitas de otros sistemas.
AP principal	Se encarga de que los dispositivos permitidos en la empresa que cuenten con capacidad inalámbrica se conecten a la red cableada principal que se encuentra protegida por el firewall PFSense.
IPS	Sistema que ayuda a identificar el tráfico malicioso y bloquea de manera proactiva el ingreso de dicho tráfico a su red.

Radius Server	<p>Permiten autenticar a usuarios de conexiones a Internet, usuarios cableados, usuarios que se quieren autenticar contra un servidor NAS o un servicio, y clientes inalámbricos WiFi. Son ampliamente usados por los operadores de Internet y en las redes WiFi de hoteles, universidades o en cualquier lugar donde se quiera proporcionar una seguridad adicional a la red inalámbrica.</p>
VPN	<p>Es una conexión cifrada a Internet desde un dispositivo a una red. La conexión cifrada ayuda a garantizar la transmisión segura de datos confidenciales. Evita que las personas no autorizadas espíen el tráfico y permite que el usuario trabaje de manera remota. La tecnología de VPN se usa ampliamente en los entornos corporativos y es una de las mejores herramientas para garantizar la privacidad en Internet.</p>
ISP	<p>Es una entidad o empresa que proporciona servicios de acceso a Internet a usuarios y organizaciones, refiere a los recursos tangibles e intangibles que posee un ISP para ofrecer servicios de conectividad y comunicación a sus clientes</p>

8. Matriz de Riesgos





MATRIZ DE RIESGOS

RIESGOS(MAGERIT)	Probabilidad (Ocurrencia) 9	Gravedad (Impacto)	Valor del Riesgo	Nivel de Riesgo
Caída de TrueNAS	3	5	15	Muy grave
Caída del AP principal	2	4	8	Apreciable
Caída de Firewall Perimetral	4	5	20	Muy grave
Caída ISP	4	5	20	Muy grave
Caída de servicio Web	5	5	25	Muy grave
Caída de DB	5	4	20	Muy grave
Caída de radius server	2	4	8	Apreciable
Servidor web desactualizado	2	3	6	Apreciable
Servidor TrueNAS desactualizado	2	3	6	Apreciable
Hackeo de la DB	5	5	25	Muy grave
Hackeo de servicio web	5	5	25	Muy grave
DDoS al servicio web	4	4	16	Muy grave
Hackeo al AP principal	2	4	8	Apreciable
Firewall perimetral desactualizado	2	5	10	Importante
VPN	2	5	10	Importante

Borrar Datos

LEYENDA

			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal. Se vigilará aunque no requiere medidas preventivas de partida.

9. Plan de Contingencia

Riesgo	Descripción	Equipo de Respuesta	Notificación	Contacto	Salvaguarda
Caída de TrueNAS	Interrupción del servicio de almacenamiento en red	Equipo de Administración de Almacenamiento en Red	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Almacenamiento en Red (TrueNAS)	Realizar copias de seguridad periódicas, implementar redundancia de datos, realizar pruebas de integridad y disponibilidad del sistema, y tener un plan de recuperación de desastres para restaurar rápidamente el servicio en caso de una falla.
Caída de AP principal	Pérdida de conectividad inalámbrica en la red principal	Equipo de Administración de Red	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Red	Configurar y mantener un AP secundario como respaldo, implementar redundancia en la infraestructura inalámbrica y tener procedimientos para restablecer rápidamente la conectividad inalámbrica en caso de una falla en el AP principal.
Caída de Firewall Perimetral	Interrupción del control y regulación del tráfico de red en la frontera de la red	Equipo de Administración de Firewall Perimetral	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Firewall Perimetral	Tener un firewall secundario como respaldo, implementar un sistema de detección de intrusos para monitorear el tráfico en caso de una falla del firewall principal, y tener un plan de respuesta y recuperación para mitigar rápidamente los riesgos asociados con la falta de protección del firewall.
Caída del Servicio	Interrupción de la disponibilidad	Equipo de Administración	Equipo de Respuesta a	Administrador del	Tener un servidor web secundario

Web	y accesibilidad del sitio web de la empresa	de Servidor Web	Incidentes, Administrador de TI	Servidor Web	como respaldo, realizar copias de seguridad periódicas, implementar una solución de balanceo de carga y tener un plan de recuperación para restablecer rápidamente el servicio web en caso de una interrupción.
Caída del ISP	Interrupción del servicio de acceso a Internet	Equipo de Administración de Red	Equipo de Respuesta a Incidentes, Administrador de TI	Proveedor de Servicio de Internet (ISP)	Implementar una conexión de respaldo a través de otro proveedor de servicios de Internet, tener un plan de contingencia para utilizar conexiones móviles como alternativa y mantener la comunicación con el ISP para obtener actualizaciones y soluciones rápidas en caso de una interrupción del servicio.
Caída de la Base de Datos	Interrupción del acceso y disponibilidad de la base de datos	Equipo de Administración de Base de Datos	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Base de Datos	Realizar copias de seguridad periódicas, implementar redundancia de datos, monitorear constantemente el rendimiento y disponibilidad de la base de datos, y tener un plan de recuperación.
Hackeo de la Base de Datos	Acceso no autorizado a la base de datos y robo o manipulación de información sensible	Equipo de Administración de Seguridad de la Información	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Seguridad de la Información	Implementar medidas de seguridad robustas, como autenticación fuerte y cifrado de datos, mantener actualizado el software de seguridad, realizar auditorías y pruebas de penetración periódicas, y tener un plan de

					respuesta a incidentes para mitigar y recuperarse rápidamente en caso de un hackeo de la base de datos
Caída de Radius Server	Interrupción del servicio de autenticación de usuarios	Equipo de Administración de Servidor de Autenticación	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador del Servidor de Autenticación	Tener un servidor de Radius secundario como respaldo, implementar medidas de redundancia, configurar políticas de respaldo y restauración, y mantener actualizada la configuración y los certificados del servidor de autenticación.
Servidor desactualizado	Utilización de un servidor con software o sistemas operativos sin actualizar	Equipo de Administración de Servidor	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador del Servidor	Implementar un plan de mantenimiento y actualización regular de software y sistemas operativos en los servidores, monitorear las actualizaciones de seguridad y parches, y tener un proceso para realizar pruebas y verificaciones antes de implementar las actualizaciones en producción.
DDoS al Servicio Web	Ataque de denegación de servicio dirigido al servidor web	Equipo de Administración de Seguridad de la Información	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Seguridad de la Información	Implementar soluciones de mitigación de DDoS, como sistemas de detección y mitigación de ataques, servicios de protección de DDoS y balanceo de carga, monitorear constantemente el tráfico y la disponibilidad del servicio web, y tener un plan de

					respuesta a incidentes para mitigar y recuperarse rápidamente en caso de un ataque DDoS.
Hackeo del Servicio Web	Acceso no autorizado al servidor web y compromiso de la integridad o confidencialidad	Equipo de Administración de Seguridad de la Información	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Seguridad de la Información	Implementar medidas de seguridad como firewalls, detección de intrusos, monitoreo de registros de acceso, encriptación de datos y autenticación fuerte, mantener actualizado el software de seguridad, realizar pruebas de seguridad periódicas y tener un plan de respuesta a incidentes para mitigar y recuperarse rápidamente en caso de un hackeo del servicio web
VPN comprometida	Compromiso de la conexión VPN y exposición de datos confidenciales	Equipo de Administración de Red y Seguridad de la Información	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Red, Administrador de Seguridad de la Información	Implementar medidas de seguridad en la solución de VPN, como autenticación de doble factor, cifrado de datos y monitoreo constante del tráfico de VPN, mantener actualizado el software de seguridad de la solución de VPN, realizar pruebas de seguridad y auditorías periódicas, y tener un plan de respuesta a incidentes para mitigar y recuperarse rápidamente en caso de una compromiso de la

					VPN.
Hackeo del AP Principal	Acceso no autorizado al punto de acceso principal y compromiso de la red inalámbrica	Equipo de Administración de Seguridad de la Información	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Seguridad de la Información	Implementar medidas de seguridad en el AP principal, como autenticación fuerte, encriptación inalámbrica y control de acceso, mantener actualizado el firmware del AP, monitorear constantemente la actividad de la red inalámbrica en busca de comportamientos sospechosos y tener un plan de respuesta a incidentes para mitigar y recuperarse rápidamente en caso de un hackeo del AP principal.
Firewall Perimetral Desactualizado	Utilización de un firewall con reglas obsoletas o sin las últimas actualizaciones	Equipo de Administración de Firewall Perimetral	Equipo de Respuesta a Incidentes, Administrador de TI	Administrador de Firewall Perimetral	Mantener actualizado el firmware y las reglas del firewall perimetral, realizar auditorías periódicas de seguridad, implementar políticas de seguridad adecuadas, monitorear los registros de actividad y eventos del firewall, y tener un proceso para aplicar rápidamente las actualizaciones y parches de seguridad.

10. Muestra de Resultados

10.1. Configuraciones del entorno de red

Ilustración 1 - Configuración de interfaces de red del laboratorio

```
UMware Virtual Machine - Netgate Device ID: 97bf49b58d3e94e791ea

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.2.18/26
LAN (lan)      -> em1      -> v4: 192.168.10.1/24
DMZ (opt1)     -> em2      -> v4: 172.16.10.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Ilustración 2 - Configuración de PFsense

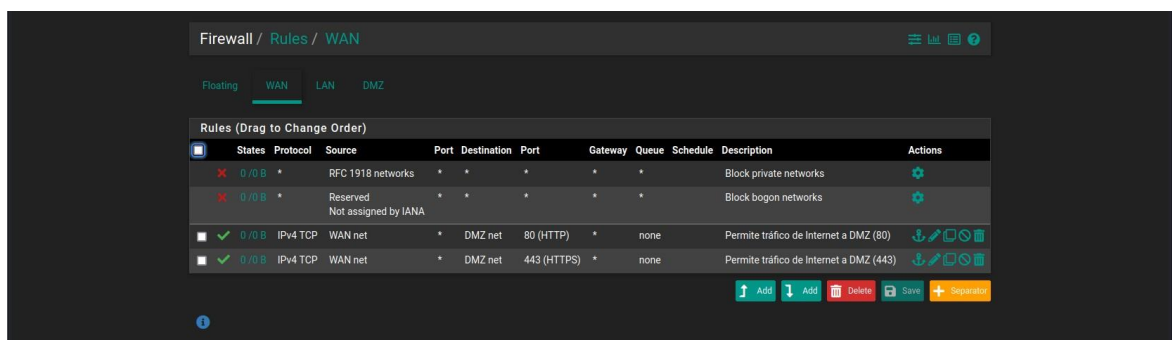


























Ilustración 3 - Reglas de Firewall de la interfaz WAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/3.44 MB	*	*	*	LAN Address	443 80	*	*		Anti-Logout Rule	
✓ 0/0 B	IPv4 TCP	192.168.10.5	*	172.16.10.3	22 (SSH)	*	none		Permitir administrador entrar a través de SSH a Linux Server	 
✓ 1/401 KB	IPv4 ICMP	LAN net	*	DMZ net	*	*	none		Permitir ping desde LAN a DMZ	 
✓ 2/4.19 MB	IPv4 TCP	192.168.10.5	*	DMZ net	*	*	none		Permite acceso de Administrador a toda la DMZ	 
✓ 0/17 KB	IPv4 TCP	LAN net	*	172.16.10.3	80 (HTTP)	*	none		Acceso de LAN a servicios WEB (80)	 
✓ 0/0 B	IPv4 TCP	LAN net	*	172.16.10.3	443 (HTTPS)	*	none		Acceso de LAN a servicios WEB (443)	 
✓ 0/0 B	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		DNS	 
✓ 0/298 KB	IPv4 *	LAN net	*	LAN net	*	*	none		Permite acceso dentro de la subred	 
✓ 7/45.65 MB	IPv4 *	LAN net	*	Private IPv4s	*	*	none		Permite LAN a Internet	 
✗ 0/13 KB	IPv4 TCP	LAN net	*	DMZ net	*	*	none		Bloqueo	 

 Add  Add  Delete  Save  Separator

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.





Ilustración 4 - Reglas de Firewall de interfaz LAN

Firewall / Rules / DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating WAN LAN DMZ

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/0 B	IPv4 *	DMZ net	*	LAN net	*	*	none		Bloquear tráfico de DMZ a LAN	 
✓ 0/0 B	IPv4 *	DMZ net	*	*	*	*	none		Permitir acceso de DMZ a Internet	 








 Add  Add  Delete  Save  Separator






Ilustración 5 - Reglas de Firewall de interfaz DMZ

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NAT

Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
WAN	TCP	*	*	WAN address	80 (HTTP)	172.16.10.3	80 (HTTP)	HTTP to web server	 

 Add  Add  Delete  Save  Separator



Legend
 Pass
 Linked rule

Ilustración 6 - Regla de NAT para acceder del exterior al servicio Web

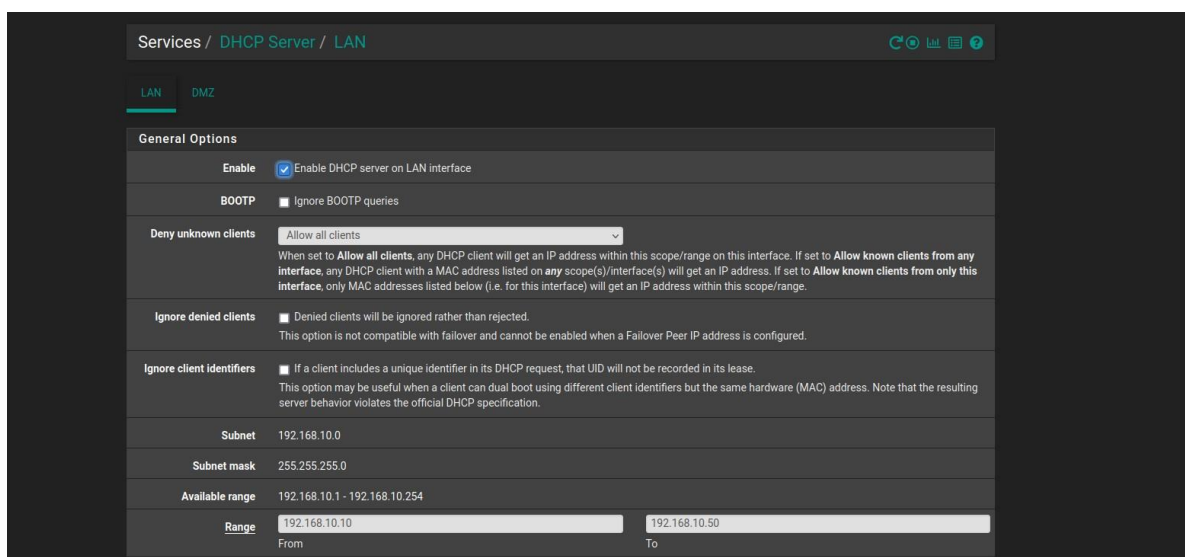


Ilustración 7 - Habilitar servidor DHCP en interfaz LAN

Control de acceso

En un SGSI es importante preservar la Confidencialidad, Integridad y Disponibilidad (CID) de la información (CIA, por sus siglas en inglés Confidentiality, Integrity and Availability) para lo cual resulta conveniente llevar un control de acceso que cuente con las características de Autorización y Contabilidad de usuarios. La cual se lleva a cabo por medio de un Radius Server, (FreeRADIUS en este caso), el cual complementado por un captive portal en el UTM aseguran que solo hay tráfico en la red de usuarios autorizados, de manera que si un atacante captura la contraseña de ingreso a la red, no podrá navegar a través de ella si no cuenta con un usuario registrado en el sistema.

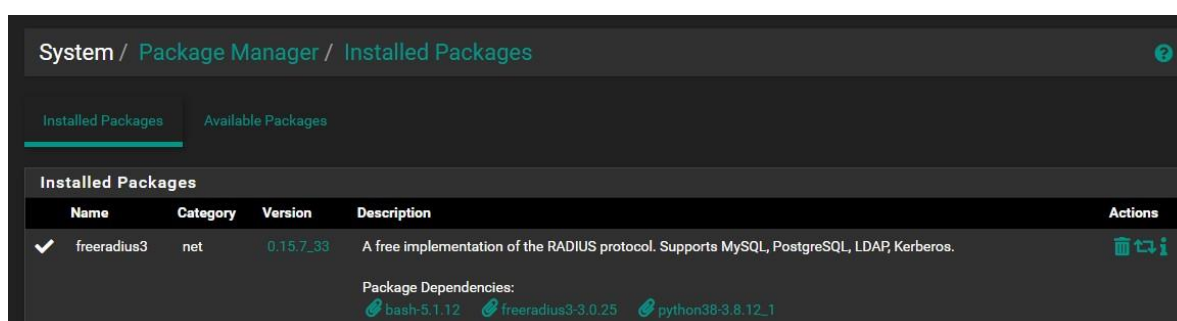


Ilustración 8 - Implementación de Radius Server en el UTM.

Package / FreeRADIUS: Interfaces / Interfaces

[Users](#)
[MACs](#)
[NAS / Clients](#)
[Interfaces](#)
[Settings](#)
[EAP](#)
[SQL](#)
[LDAP](#)
[View config](#)
[XMLRPC Sync](#)

Interface	IP Address	Port	Interface Type	IP Version	Description	
*		1812	auth	ipaddr	FR Auth	
*		1813	acct	ipaddr	FR Acc	
*		1816	status	ipaddr	FR Stat	
						Add

Save

Ilustración 9 - Configuración del Radius Server en el UTM (interfaces).

General Configuration

Client IP Address

192.168.10.1

Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).

Client IP Version

IPv4

Client Shortname

CaptivePortal

Enter a short name for the client. This is generally the hostname of the NAS.

Client Shared Secret

Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. [FreeRADIUS is limited to 31 characters for the shared secret.](#)
Warning: Single quotes in shared secret must be escaped with a backslash (`'`). Backslash must be escaped by using two backslashes (`\\`).

Miscellaneous Configuration

Client Protocol

UDP

Enter the protocol the client uses. (Default: UDP)

Client Type

other

Enter the NAS type of the client. This is used by checkrad.pl for simultaneous use checks. (Default: other)

Require Message Authenticator

No

RFC5080 requires Message-Authenticator in Access-Request. But older NAS (switches or accesspoints) do not include that. (Default: no)

Max Connections

16

Takes only effect if you use TCP as protocol. Limits the number of simultaneous TCP connections from a client. (Default 16)

NAS Login

If supported by your NAS, you can use SNMP or finger for simultaneous-use checks instead of (s)radutmp file and accounting. Leave empty to choose (s)radutmp. (Default: empty)

NAS Password

If supported by your NAS, you can use SNMP or finger for simultaneous-use checks instead of (s)radutmp file and accounting. Leave empty to choose (s)radutmp. (Default: empty)

Description

NAS for Captive Portal

Enter any description you like for this client.

Ilustración 9.1 - Configuración del Radius Server en el UTM (Cliente NAS).

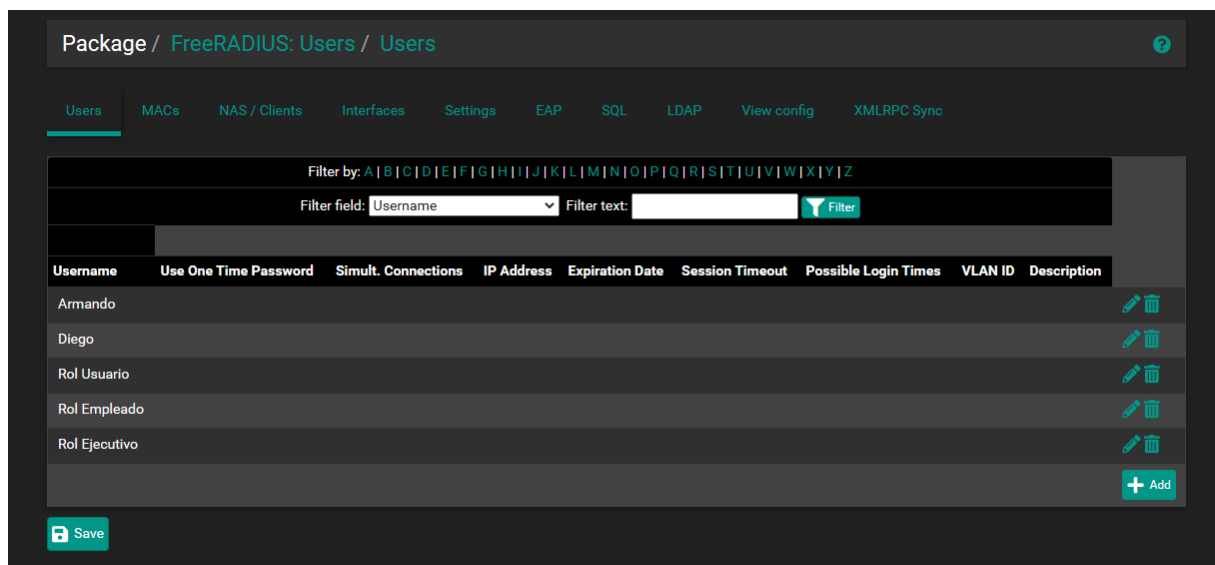


Ilustración 9.2 - Configuración del Radius Server en el UTM (Agregando usuarios).

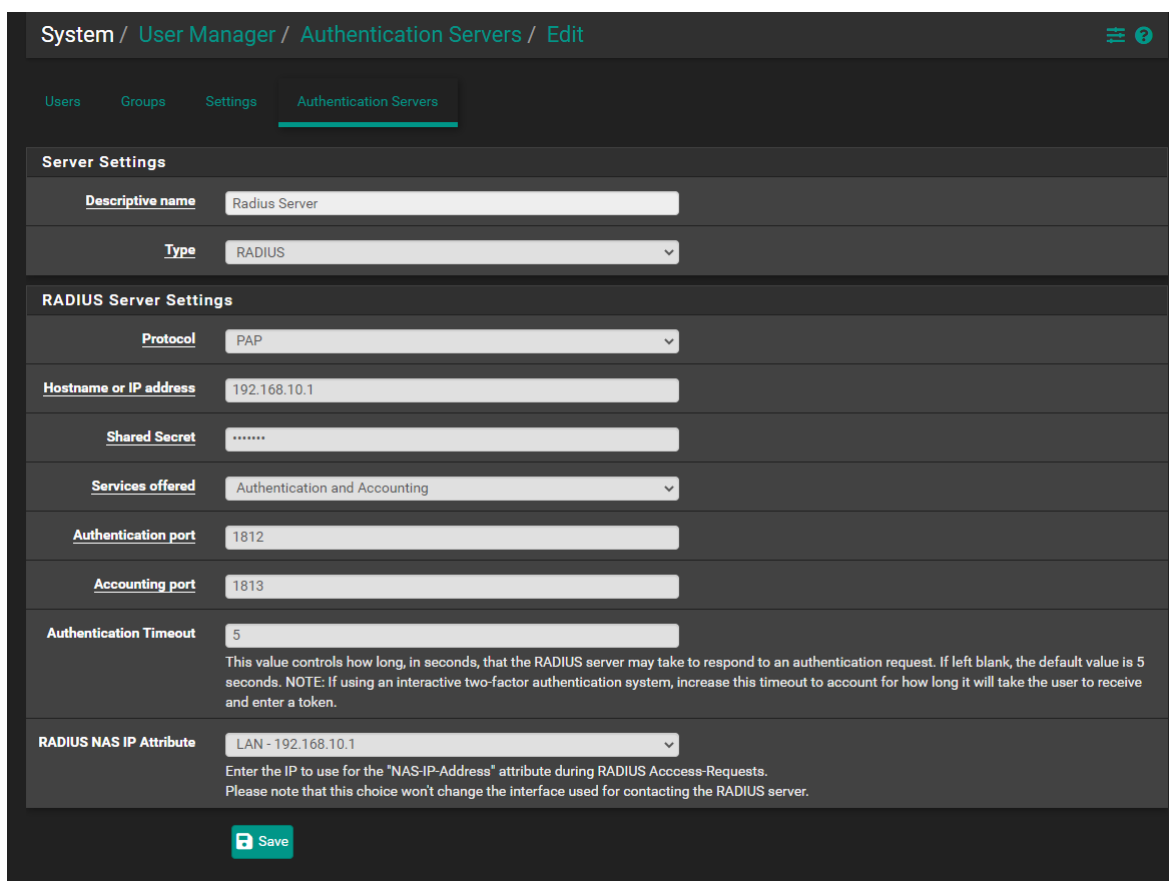


Ilustración 10 - Configuración del servidor de autenticación en el UTM.

Captive Portal Configuration	
Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Description	<input type="text" value="LAN Network"/> A description may be entered here for administrative reference (not parsed).
<u>Interfaces</u>	<div> <div>WAN</div> <div>LAN</div> <div>DMZ</div> </div> Select the interface(s) to enable for captive portal.

Ilustración 11 - Configuración de captive portal

Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
----------------------------	---

Ilustración 11.1 - Configuración de captive portal

Captive Portal Login Page	
Display custom logo image	<input checked="" type="checkbox"/> Enable to use a custom uploaded logo
Logo Image	<div> <div>Elegir archivo</div> <div>No se eligió ningún archivo</div> </div> <p>Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, It can be of any image type: .png, .jpg, .svg This image will not be stored in the config. The default logo will be used if no custom image is present.</p>
Display custom background image	<input checked="" type="checkbox"/> Enable to use a custom uploaded background image
Background Image	<div> <div>Elegir archivo</div> <div>No se eligió ningún archivo</div> </div> <p>Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. This image will not be stored in the config. The default background image will be used if no custom background is present.</p>
Terms and Conditions	<div> <div></div> </div> <p>Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out</p>

Ilustración 11.2 - Configuración de captive portal

Authentication	
Authentication Method	<div>Use an Authentication backend</div> <p>Select an Authentication Method to use for this zone. One method must be selected.</p> <ul style="list-style-type: none"> - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.
Authentication Server	<div> <div>Radius Server</div> <div>Local Database</div> </div> <p>You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.</p>
Secondary authentication Server	<div> <div>Radius Server</div> <div>Local Database</div> </div> <p>You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.</p>
NAS Identifier	<div>CaptivePortal-RADIUS</div> <p>Specify a NAS identifier to override the default value (CaptivePortal-lan)</p>

Ilustración 11.3 - Configuración de captive portal

Accounting

RADIUS ☒ Send RADIUS accounting packets.
If enabled, accounting request will be made for users identified against any RADIUS server.

Accounting Server RADIUS Server

You can add a Radius Accounting server in the [User Manager](#).

Send accounting updates ☐ No updates ☐ Stop/Start ☒ Stop/Start (FreeRADIUS) ☐ Interim

Ilustración 11.4 - Configuración de captive portal

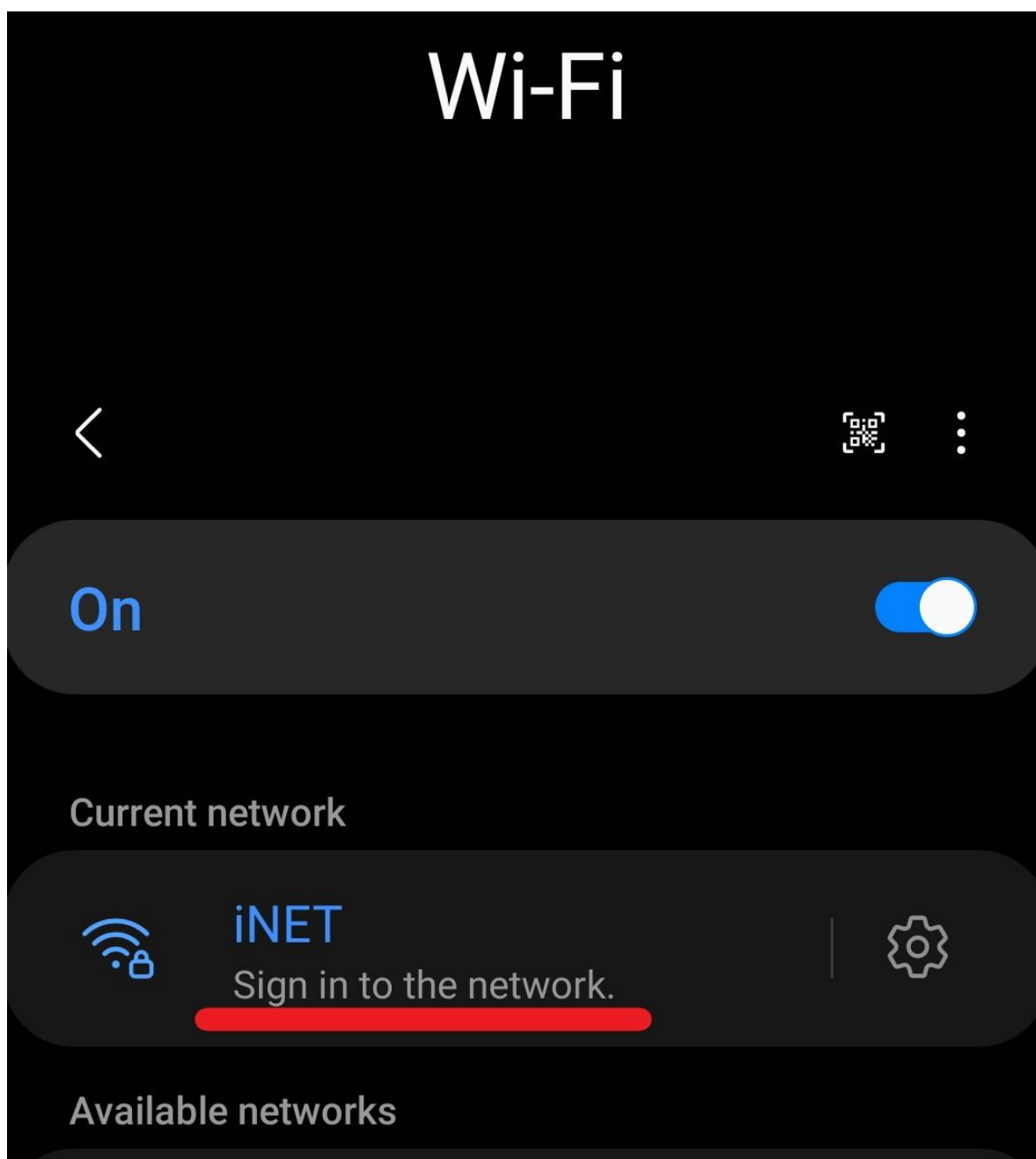


Ilustración 12 - Autenticación requerida al conectarse a la red

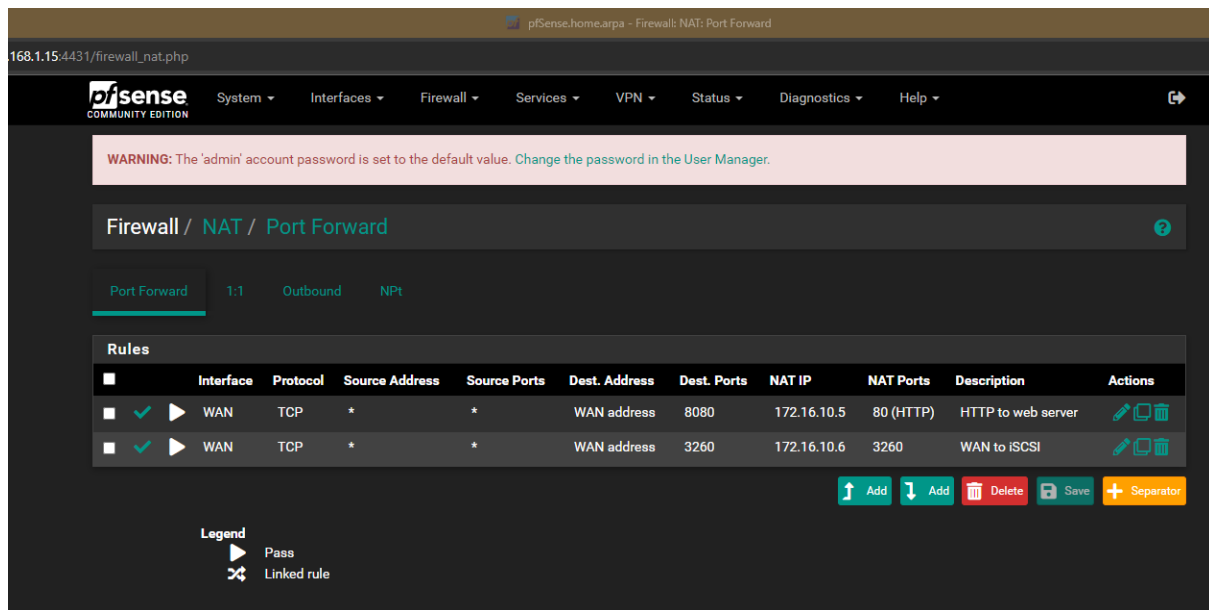


Ilustración 14 - Regla NAT para servicios de DMZ.

Establecer políticas de filtrado para contenido explícito

Squidguard

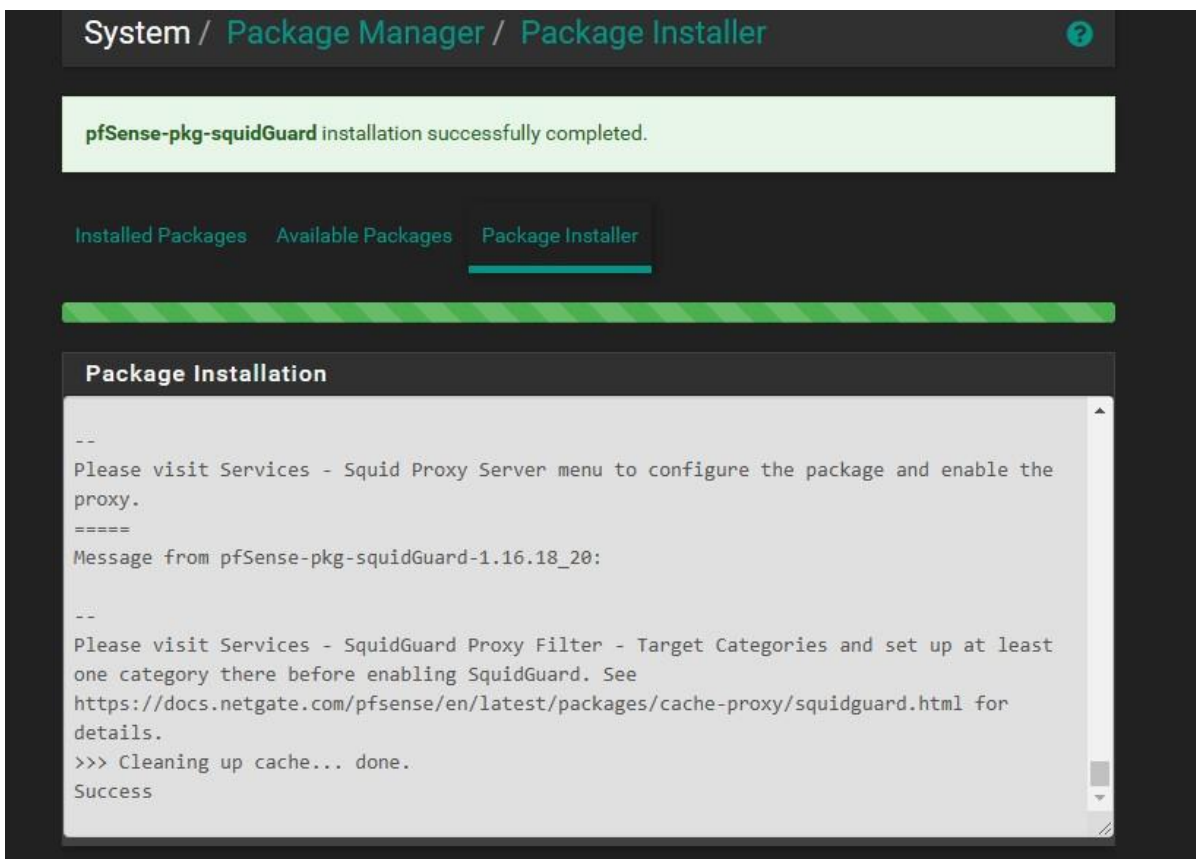


Ilustración 17 -. Instalación de squidguard

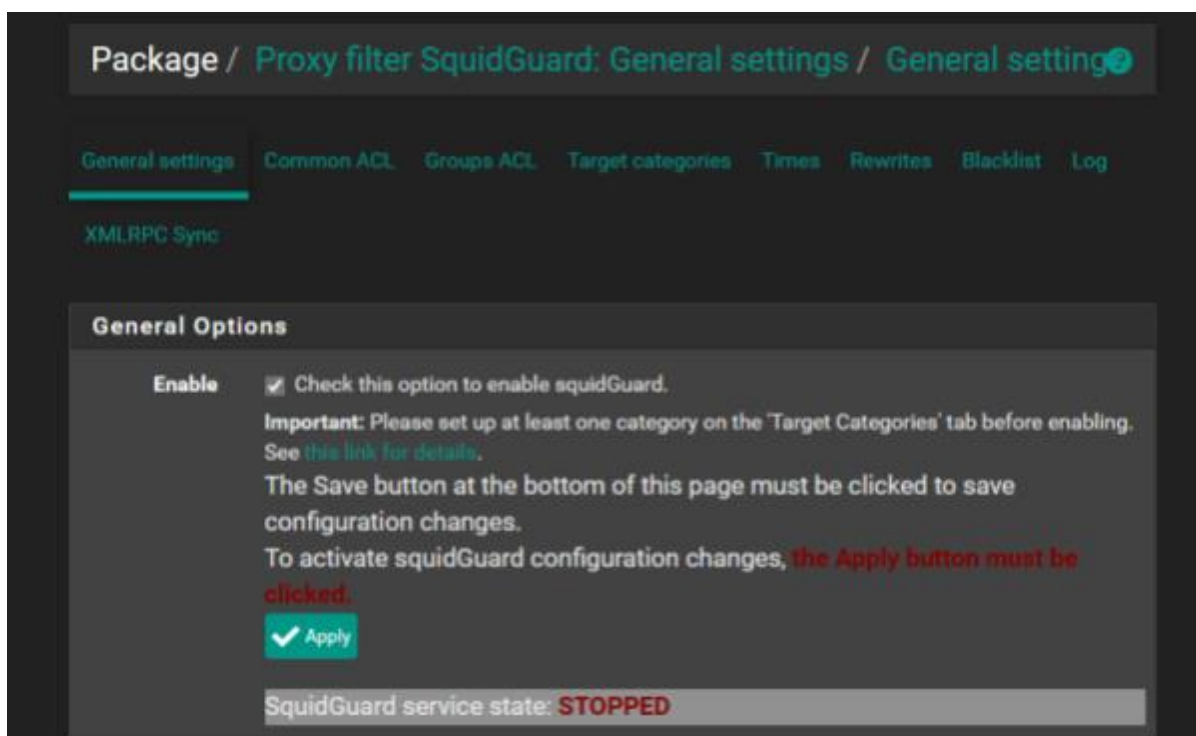


Ilustración 17 -. Habilitando ProxyFilter: SquidProxy

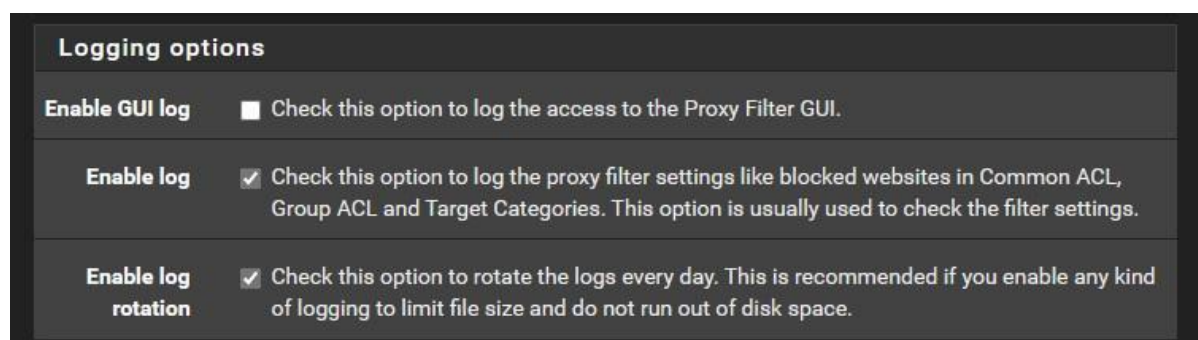


Ilustración 18 Configurando registro de Logs

Blacklist options

Blacklist

☒ Check this option to enable blacklist

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

Blacklist URL

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL
blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

Save

Ilustración 19 Agregando listas para bloquear sitios web

Blacklist Update

0 %

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Download

Cancel

Restore Default

Enter FTP or HTTP path to the blacklist archive here.

Blacklist update Log

Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 63 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.

Ilustración 20 - Descargando lista para las blocklist

General Options

Name

whitelist

Enter a unique name of this rule here.

The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.

Order

Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.

Domain List

google.ac google.ad google.ae google.al google.am google.as
google.at google.az google.ba google.be google.bf google.bg
google.bi google.bj google.bs google.bt google.by google.ca
google.cat google.cd google.cf google.cg google.ch google.ci
google.cl google.cm google.cn google.co.ao google.co.bw
google.co.ck google.co.cr google.co.hu google.co.id
google.co.il google.co.in google.co.je google.co.jp
google.co.ke google.co.kr google.co.ls google.com google.co.ma
google.com.af google.com.ag google.com.ai google.com.ar
google.com.au google.com.bd google.com.bh google.com.bn

Enter destination domains or IP-addresses here. To separate them use space.

Example: mail.ru e-mail.ru yahoo.com 192.168.1.1

Ilustración 21 - Configurando las whitelists

General Options

Target Rules

Target Rules List + -

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories

Whitelist [whitelist]	access	whitelist	▼
[blk_blacklists_adult]	access	deny	▼

[blk_blacklists_malware]	access	deny	▼
[blk_blacklists_manga]	access	---	▼
[blk_blacklists_marketingware]	access	---	▼
[blk_blacklists_mixed_adult]	access	deny	▼
[blk_blacklists_mobile-phone]	access	---	▼
[blk_blacklists_phishing]	access	deny	▼

Ilustración 23 - Categorías bloqueadas para los usuarios de la red

SquidProxy

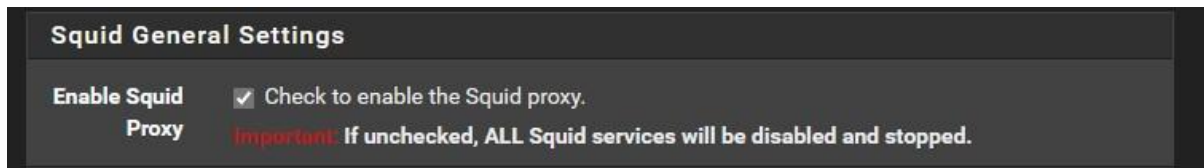


Ilustración 24 - Habilitando SquidProxy

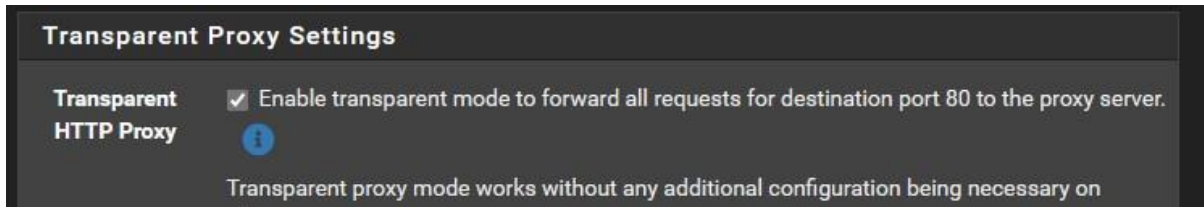


Ilustración 25 - Configurando Proxy Transparente para HTTP

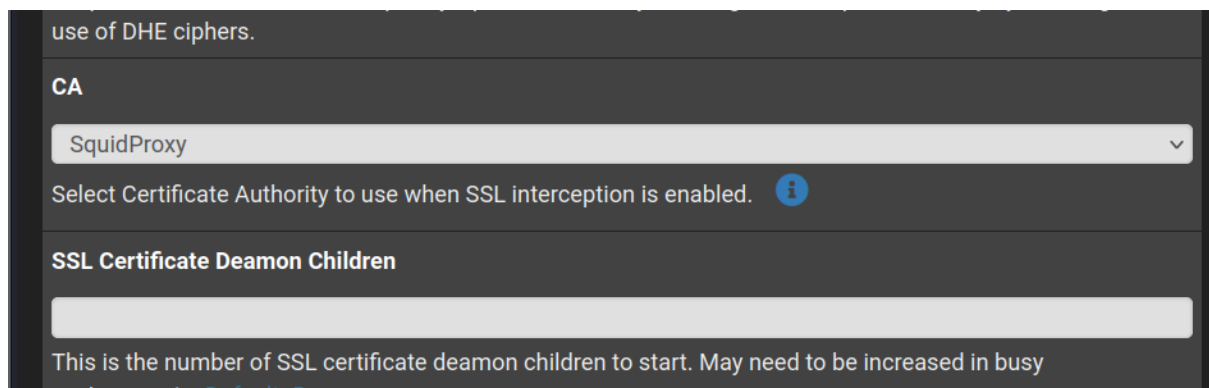


Ilustración 26 - Insertar certificado SSL

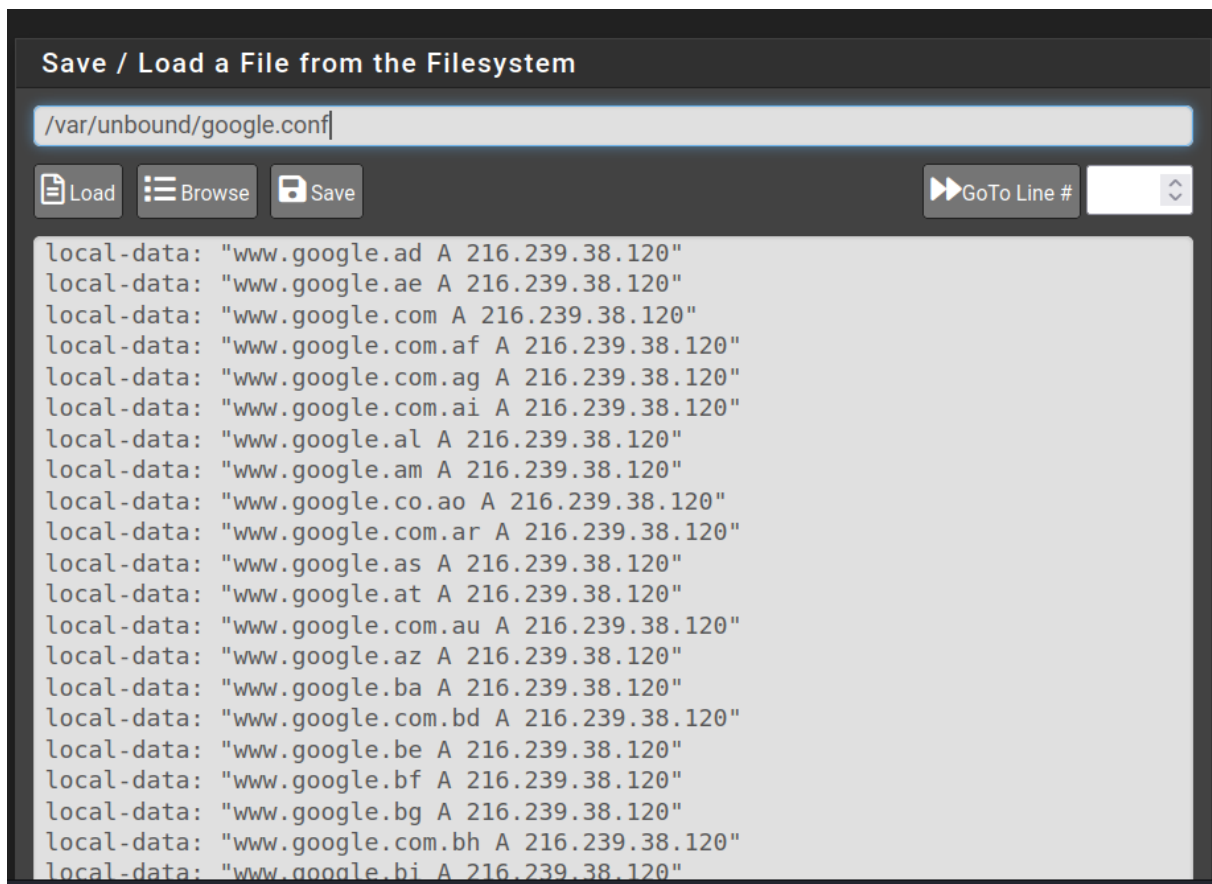


Ilustración 27 - Bloqueo por DNS

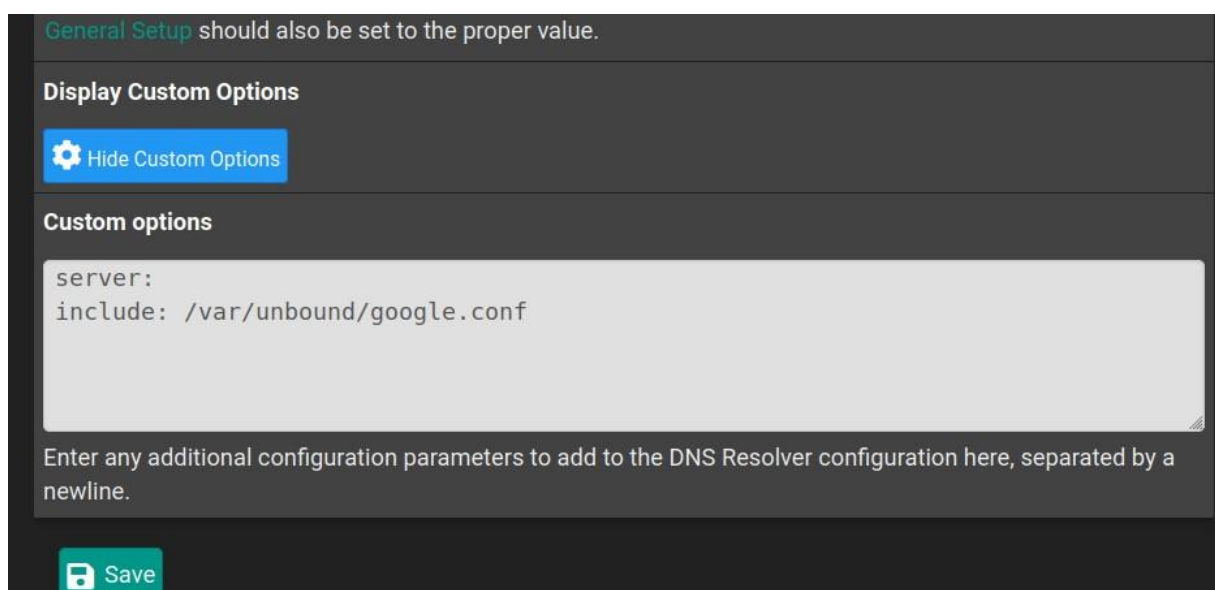


Ilustración 28 - Ruta del fichero google.conf

Construir enlace seguro con VPN

Requisitos para crear una VPN







Installed Packages						
Name	Category	Version	Description	Actions		
✓ openvpn-client-export	security	1.6_8	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	 		
			Package Dependencies:			
			 openvpn-client-export-2.5.2			 openvpn-2.5.4_1
			 zip-3.0_1			 p7zip-16.02_3

Ilustración 29 - Descargar paquete openvpn-client-export






VPN	✓	self-signed	3	CN=internal-ca 	OpenVPN Server    
Valid From: Thu, 15 Dec 2022 19:44:13 -0600					
Valid Until: Sun, 12 Dec 2032 19:44:13 -0600					

Ilustración 30 - Crear entidad certificadora

















Harry cert User Certificate CA: No Server: No	VPN	CN=Harry 	User Cert    
Valid From: Thu, 15 Dec 2022 22:19:06 -0600			
Valid Until: Sun, 12 Dec 2032 22:19:06 -0600			
VPN Server Certificate CA: No Server: Yes	VPN	CN=VPN 	OpenVPN Server    
Valid From: Thu, 15 Dec 2022 22:42:19 -0600			
Valid Until: Sun, 12 Dec 2032 22:42:19 -0600			
Armando User Certificate CA: No Server: No	VPN	CN=Armando 	    
Valid From: Thu, 15 Dec 2022 22:43:30 -0600			
Valid Until: Sun, 12 Dec 2032 22:43:30 -0600			

Ilustración 31 - Crear certificado de servidor y certificados dedicados para los usuarios que se conectarán al servicio de VPN





OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.11.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN	  
					 Add

Ilustración 32 - Creación de servidor OpenVPN

Mode Configuration

Server mode
Remote Access (SSL/TLS + User Auth)

Backend for authentication

Radius Server
Local Database

Device mode
tun - Layer 3 Tunnel Mode

"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Ilustración 33 - Configurar el modo de autenticación (Radius server)

Endpoint Configuration

Protocol
UDP on IPv4 only

Interface
WAN

The interface or Virtual IP address where OpenVPN will receive client connections.

Local port
1194

The port used by OpenVPN to receive client connections.

Ilustración 34 - Establecer protocolos, interfaz y puerto de conexión

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="192.168.11.0/24"/> This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
IPv6 Tunnel Network	<input type="text"/> This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	<input type="text" value="192.168.10.0/24"/> IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Ilustración 35 - Establecer red para usuarios por VPN y linkear con red LAN

Exportar perfiles de usuario

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Server

Remote VPN 1194

Ilustración 36 - Acceder al menú Client Export

OpenVPN Clients		
User	Certificate Name	Export
Certificate with External Auth	Harry cert	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installer (2.5.2-lx01): 64-bit 32-bit - Legacy Windows Installers (2.4.11-lx01): 10/2016/2019 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config
Certificate with External Auth	Armando	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installer (2.5.2-lx01): 64-bit 32-bit

Ilustración 37 - Exportar fichero correspondiente al usuario y dispositivo (teléfono, computadora, S.O.)

IDS/IPS

IDS (Intrusion Detection System) / IPS (Intrusion Prevention System) es un sistema que ayuda a detectar y bloquear tráfico malicioso en la red. En este caso se implementó la solución IDS / IPS snort para llevar a cabo esa tarea y se aprovisionó con las reglas de la comunidad.

The image shows a configuration interface for Snort, divided into two main sections: General Settings and Alert Settings.

General Settings

- Enable:** A checkbox labeled "Enable interface" is checked.
- Interface:** A dropdown menu shows "LAN (em1)". Below it, text says: "Choose the interface where this Snort instance will inspect traffic."
- Description:** A text input field contains "LAN". Below it, text says: "Enter a meaningful description here for your reference."
- Snap Length:** A text input field contains "1518". Below it, text says: "Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications."

Alert Settings

- Send Alerts to System Log:** A checkbox is checked. Text below says: "Snort will send Alerts to the firewall's system log. Default is Not Checked."
- System Log Facility:** A dropdown menu shows "LOG_AUTH". Text below says: "Select system log Facility to use for reporting. Default is LOG_AUTH."
- System Log Priority:** A dropdown menu shows "LOG_ALERT". Text below says: "Select system log Priority (Level) to use for reporting. Default is LOG_ALERT."
- Enable Packet Captures:** A checkbox is unchecked. Text below says: "Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file."
- Enable Unified2 Logging:** A checkbox is unchecked. Text below says: "Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked." and "Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled."

Ilustración 39 - Configuración general del IDS/IPS 1

The image shows the "Block Settings" section of the Snort configuration interface.

Block Settings

- Block Offenders:** A checkbox is checked. Text below says: "Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked."
- IPS Mode:** A dropdown menu shows "Legacy Mode". Text below says: "Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspecting engine between the NIC and the OS. Default is Legacy Mode." and "Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Snort can then determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and blocks traffic directly."

Ilustración 40 - Configuración general del IDS/IPS 2

Snort GPLv2 Community Rules	
Enable Snort GPLv2	<input checked="" type="checkbox"/> Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.	
Emerging Threats (ET) Rules	
Enable ET Open	<input checked="" type="checkbox"/> Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.	
Enable ET Pro	<input type="checkbox"/> Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account ETPro for Snort offers daily updates and extensive coverage of current malware threats.	
Sourcefire OpenAppID Detectors	
Enable OpenAppID	<input checked="" type="checkbox"/> Click to enable download of Sourcefire OpenAppID Detectors
The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.	
OpenAppID Version	Installed Detection Package Version=356
Enable AppID Open Text Rules	<input type="checkbox"/> Click to enable download of the AppID Open Text Rules
Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.netgate.com/openappid/appid_rules.tar.gz .	
FEODO Tracker Botnet C2 IP Rules	
Enable FEODO Tracker Botnet C2 IP Rules	<input checked="" type="checkbox"/> Click to enable download of FEODO Tracker Botnet C2 IP rules
Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet.	
Rules Update Settings	
Update Interval	<div>NEVER</div> <div>Please select the interval for rule updates. Choosing NEVER disables auto-updates.</div>
Update Start Time	

Services / Snort / Updates

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	c56274aef915a08d6d8421e9caaa17f1	Friday, 16-Dec-22 01:36:09 CST
Emerging Threats Open Rules	1f40f3b7772ab011dda2d90a28eec5cf	Friday, 16-Dec-22 01:36:10 CST
Snort OpenAppID Detectors	fba164dfe992d6022740a6b390d51765	Friday, 16-Dec-22 01:36:09 CST
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	431af147acbdb9899a9d3c2af93a644f	Friday, 16-Dec-22 01:38:54 CST

Anexo 1. Archivos no permitidos para intercambiar en la red.

Lista de extensiones de archivos no permitidos para almacenar/descargar desde Internet.
(Ferreira Medina, López Maldonado, Valencia García, & Gálvez Macías, 2020)

ASF --> Windows Media AVI--> BSPlayer

BIK --> RAD Video Tools DIV --> DivX Player DIVX --> DivX Player DVD --> PowerDVD

IVF --> Indeo M1V --> (mpeg)

MOV(*) --> QuickTime MOVIE --> (mov) MP2V

--> (mpeg)

MP3 --> Música comprimida MP4 --> (MPEG-4)

MPA --> (mpeg) MPE --> (mpeg) MPEG --> (mpeg) MPG --> (mpeg)

MPV2 --> (mpeg)

QT --> QuickTime QTL

--> QuickTime

RPM --> RealPlayer SMK

--> RAD

Video Tools VIV --> Video VIV

WAV --> Música digital WM --> Windows Media

WMA --> Música comprimida para Windows

Media

WMV --> Windows Media WOB --> PowerDVD

Anexo 2. Lista de programas no permitidos.

- Nmap: Una herramienta de escaneo de puertos y mapeo de redes utilizada para descubrir vulnerabilidades en sistemas y redes.
- Metasploit: Un marco de pruebas de penetración que permite identificar y explotar vulnerabilidades en sistemas.
- John the Ripper: Un programa de fuerza bruta utilizado para descifrar contraseñas.
- Cain and Abel: Una herramienta de recuperación de contraseñas y análisis de red que puede utilizarse para realizar ataques de suplantación de identidad.
- Wireshark: Un analizador de protocolos de red que puede ser utilizado para interceptar y capturar información confidencial transmitida a través de la red.
- Hydra: Una herramienta de fuerza bruta utilizada para probar contraseñas y credenciales de acceso en servicios como FTP, SSH y servidores web.
- Aircrack-ng: Una suite de herramientas de auditoría de seguridad inalámbrica utilizada para realizar ataques de cracking de contraseñas en redes Wi-Fi.

- Remote Access Trojans (RAT): Estos programas, como DarkComet, NetBus o Poison Ivy, se utilizan para obtener acceso remoto no autorizado a sistemas y pueden ser utilizados para controlarlos de manera encubierta.
- SQLMap: Una herramienta de prueba de penetración específicamente diseñada para automatizar la detección y explotación de vulnerabilidades en bases de datos SQL.
- Netcat: Una herramienta de red versátil que puede ser utilizada para abrir puertas traseras, transferir archivos de forma encubierta o realizar ataques de denegación de servicio.

Estas herramientas no son necesariamente maliciosas por sí mismas, pero su uso indebido puede comprometer la seguridad de una red empresarial. También es importante tener en cuenta que esta lista no es exhaustiva y existen otras herramientas similares que podrían representar riesgos para la seguridad. [OpenAI. (2023, 1 de junio).

11. Conclusiones

Las empresas comprometidas con la implantación de un SGSI mantendrán en todo momento la confiabilidad de sus usuarios debido a los estándares que son puestos en marcha para optimizar sus procesos y gestionar los riesgos relacionados a la integridad de la información, además de las buenas prácticas ofrecidas por estándares como ISO 27002.

Implementar un SGSI no depende solo del cumplimiento de los parámetros brindados por la ISO 27001 sino es fundamental la participación de la Alta Dirección de la empresa, porque ellos son los principales interesados en que sus procesos se cumplan.

Además, es importante incentivar a los miembros de la empresa a seguir una cultura de seguridad para que la organización mantenga su información protegida ante siniestros, y en caso de suceder alguna amenaza poder tomar un plan de contingencia que permita la superar la afectación.

Para que la implementación de un SGSI sea exitosa, debe realizarse mediante un ciclo de mejora continua, la metodología propuesta por los estándares del SGSI es PHVA (Planear, Hacer, Verificar y Actuar) mediante la cual se garantiza la mejora continua del SGSI para que siga adaptándose a los cambios y reforzando en las oportunidades de mejora, de manera que cumpla con el objetivo propuesto, proteger la información alineándose a los intereses y objetivos de negocio y de gobernanza de la organización.

12. Referencias

ISO. (2013). Norma Internacional ISO/IEC 27001:2013. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. Recuperado de <https://www.iso.org/standard/54534.html>

Instituto Nacional de Estándares y Tecnología (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. Recuperado de <https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity>

Oosterlinck, A. (2019). Implementation of an Information Security Management System (ISMS) according to ISO 27001. Recuperado de <https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/implementation-of-an-information-security-management-system-isms-according-to-iso-27001>

INAI. (junio de 2015). INAI. Recuperado el 23 de octubre de 2022, de <http://www.transparencia.udg.mx/sites/default/files/Gu%C3%ADa%20para%20la%20implementaci%C3%B3n%20de%20un%20SGSDP.pdf>

Ferreira Medina, H., López Maldonado, A. G., Valencia García, A., & Gálvez Macías, L. A. (2020). Implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en

Institutos de Investigación; caso IIES-UNAM. Morelia, México. Recuperado el 22 de marzo de 2023