Implementación del Framework de Ciberseguridad con la simulación de una PYME

Framework de Ciberseguridad para PYMES

Fase	Sección	Práctica
Análisis	**Requisitos**	Definir PYME
	Perfil actual y objetivo	Definir perfil actual y objetivo
	Gestión de activos	Inventariar Infraestructura: activos hardware y software
	Gestión de comunicaciones	Gestionar las comunicaciones
Diseño	**Políticas**	Definir las políticas de ciberseguridad de la organización
	Roles y las responsabilidades de seguridad	Definir los roles y las responsabilidades de seguridad
Implementación	**Plan de riesgos**	Desarrollar un plan de riesgos a través de una evaluación
	Seguridad de los datos	Implementar medidas de protección de los datos
	Seguridad de la red	Implementar medidas de protección de la red
	Conciencia y capacitación	Implementar una cultura de ciberseguridad
	Plan ante incidentes	Desarrollar un plan para mitigar incidentes
Mejora continua	**Auditoría**	Realizar auditoría de ciberseguridad
	Actualización de estrategias	Actualizar las estrategias de seguridad

Contenido

Introducción

Para evaluar la efectividad del Framework de Ciberseguridad, se realizó una simulación representativa de una pequeña y mediana empresa (PYME) que opera con un conocimiento limitado en ciberseguridad. La simulación recrea un entorno típico de PYME, con las siguientes características:

Descripción de la Empresa Simulada

La empresa simulada es una organización que ofrece servicios contables llamada ContabilidadSegura. Es de siete empleados, cada uno con un equipo de cómputo personal conectado a una red de área local (LAN). Este entorno simulado se ha diseñado para reflejar una estructura básica que podría encontrarse en una pequeña empresa que aún no cuenta con medidas de ciberseguridad avanzadas. La estructura de red y las políticas de seguridad se desarrollarán según el Framework propuesto.

Infraestructura de Red

La red de la empresa está configurada con un router y un switch que conecta todos los equipos de cómputo de los empleados. Esta infraestructura sencilla permite la comunicación interna entre los dispositivos y también la conexión a internet. El router actúa como el punto central de acceso a internet, mientras que el switch permite la interconexión de todos los equipos dentro de la LAN.

Medios de Comunicación

Para sus operaciones diarias, la empresa utiliza el correo electrónico como principal medio de comunicación, tanto interno como externo. Esto refleja el uso de herramientas de productividad típicas en PYMES, donde los empleados dependen del correo electrónico para intercambiar información y coordinar tareas.

Objetivos de la Simulación

- Probar la eficacia de las políticas y prácticas de ciberseguridad definidas en el Framework, en un entorno representativo de una PYME.
- Identificar vulnerabilidades y evaluar el impacto de las medidas de seguridad aplicadas en la red simulada.
- Desarrollar e implementar estrategias para proteger la confidencialidad, integridad y disponibilidad de los datos de la empresa.

Pruebas Realizadas

En la simulación, se implementaron medidas de ciberseguridad como el control de acceso, la segmentación de la red y el monitoreo de tráfico, con el objetivo de prevenir accesos no autorizados y proteger los datos de la empresa. Además, se realizaron auditorías periódicas para evaluar la efectividad de estas medidas y realizar ajustes en las políticas según fuera necesario.

Análisis de la empresa

Requisitos

Para determinar si la empresa puede beneficiarse del Framework de ciberseguridad, se debe analizar cada uno de los requisitos clave definidos para una PYME.

Guía de evaluación:

Tamaño de la Empresa

Requisito: La empresa debe tener entre 1 y 200 empleados.

Evaluación: Verifica el número de empleados en tu empresa. Si tienes entre 1 y 200 empleados, cumples este criterio.

Estado: ✓ Cumple / ✗ No cumple.

Recursos Tecnológicos

Conectividad a Internet

Requisito: La empresa debe tener acceso a internet para conectarse al mundo digital y facilitar sus operaciones.

Evaluación: Asegúrate de que tu empresa cuenta con una conexión a internet estable y segura.

Estado: ✓ Cumple / ✗ No cumple.

Infraestructura de Red

Requisito: La empresa debe contar con una red local (LAN), un switch y un router para gestionar la conectividad interna y el acceso a internet.

Evaluación: Verifica que tu empresa tenga una infraestructura de red básica, al menos un router para gestionar la conexión a internet y un switch para conectar los equipos de la LAN.

Estado: ✓ Cumple / ✗ No cumple.

Acceso Inalámbrico (opcional)

Requisito: Se recomienda contar con una red Wi-Fi para dispositivos móviles y visitantes.

Evaluación: Si tu empresa utiliza Wi-Fi para dispositivos móviles o permite el acceso inalámbrico, cumple con este criterio recomendado.

Estado: ✓ Cumple / ✗ No cumple / Opcional.

Hardware

Requisito: La empresa debe disponer de entre 1 y 50 computadoras o dispositivos móviles, impresoras, y, en algunos casos, un servidor.

Evaluación: Realiza un inventario de tus dispositivos de hardware. Si tienes al menos una computadora por empleado (entre 1 y 50 en total) y dispositivos adicionales como impresoras o servidores, cumples con este requisito.

Estado: ✓ Cumple / ✗ No cumple.

Software y Aplicaciones

Requisito: Cada dispositivo debe contar con un sistema operativo actualizado y aplicaciones de productividad (procesadores de texto, hojas de cálculo, etc.).

Evaluación: Verifica que tus equipos tengan sistemas operativos actualizados y al menos las aplicaciones de productividad básicas para facilitar las tareas diarias.

Estado: ✓ Cumple / ✗ No cumple.

Soluciones en la Nube

Requisito: Se recomienda utilizar soluciones basadas en la nube para almacenamiento seguro y colaboración en tiempo real.

Evaluación: Si tu empresa utiliza servicios en la nube (como Google Drive, Microsoft 365, o cualquier otra herramienta de almacenamiento o colaboración en línea), cumples con este requisito recomendado.

Estado: ✓ Cumple / ✗ No cumple / Opcional.

Resultados de la Evaluación

Una vez completada esta evaluación, se cuenta cuántos requisitos cumple la empresa. La empresa si cumple con la mayoría de los criterios (al menos los fundamentales como el tamaño de la empresa, conectividad a internet, infraestructura de red y hardware), ContabilidadSegura es una PYME según el Framework y puede beneficiarse de las prácticas de ciberseguridad propuestas.

Evaluación para la Empresa ContabilidadSegura

Tamaño de la Empresa

✓ Cumple (7 empleados).

Recursos Tecnológicos

Conectividad a Internet: ✓ Cumple (la empresa cuenta con acceso a internet).

Infraestructura de Red: ✓ Cumple (la empresa tiene un router y un switch para la conexión de los equipos).

Acceso Inalámbrico: ✗ No cumple / Opcional (la empresa no cuenta con red Wi-Fi, pero esto es opcional).

Hardware

✓ Cumple (la empresa dispone de 7 computadoras, una por empleado).

Software y Aplicaciones

✓ Cumple (los equipos tienen sistemas operativos y aplicaciones de productividad como correo electrónico).

Soluciones en la Nube

✗ No cumple / Opcional (la empresa no utiliza soluciones en la nube, pero esto es opcional).

Resumen de la Evaluación

La empresa ContabilidadSegura cumple con los requisitos esenciales definidos para una PYME en el Framework de ciberseguridad. Aunque no cuenta con una red Wi-Fi ni soluciones en la nube, estos elementos son opcionales y no limitan la aplicabilidad del Framework. Por lo tanto, se concluye que el Framework es adecuado para implementar medidas de ciberseguridad en esta empresa.

Perfil actual y objetivo

A continuación, se muestra una tabla que representa el nivel de madurez de cada práctica de ciberseguridad en la empresa simulada.

Práctica	Perfil Actual	Perfil Objetivo	Avance	Avance Por Face
Definir PYME	**Nivel 5**	**Nivel 5**	**100%**	**50%**
Definir perfil actual y objetivo	**Nivel 5**	**Nivel 5**	**0%**	

Inventariar Infraestructura: activos hardware y software	Nivel 1	Nivel 5	0%	
Gestionar las comunicaciones	Nivel 1	Nivel 5	0%	
Definir las políticas de ciberseguridad de la organización	Nivel 1	Nivel 5	0%	0%
Definir los roles y las responsabilidades de seguridad	Nivel 1	Nivel 5	0%	
Desarrollar un plan de riesgos a través de una evaluación	Nivel 1	Nivel 5	0%	0%
Implementar medidas de protección de los datos	Nivel 1	Nivel 5	0%	
Implementar medidas de protección de la red	Nivel 1	Nivel 5	0%	
Implementar una cultura de ciberseguridad	Nivel 1	Nivel 5	0%	
Desarrollar un plan para mitigar incidentes	Nivel 1	Nivel 5	0%	
Realizar auditoría de ciberseguridad	Nivel 1	Nivel 5	0%	0%
Actualizar las estrategias de seguridad	Nivel 1	Nivel 5	0%	

Avance General	**13%**

Interpretación de los Niveles

Nivel Actual: La mayoría de las prácticas de ciberseguridad se encuentran en Nivel 1 (Inicial), indicando que aún no han sido implementadas o están en una fase muy temprana de desarrollo.

Nivel Objetivo: La meta es alcanzar Nivel 5 (Óptimo) en todas las prácticas, lo cual representa un entorno de ciberseguridad completamente implementado, con políticas, controles y cultura organizacional en ciberseguridad bien establecidos.

Avance: Actualmente, la empresa ha logrado un avance general del 13%, alcanzando el Nivel 5 en la primera práctica, "Definir PYME", y el nivel 5 al finalizar esta práctica “Definir perfil actual y objetivo”. Las demás prácticas aún están en nivel inicial y serán desarrolladas progresivamente en las fases siguientes.

Gestión de activos

A continuación, se presenta el inventario de activos de la empresa ContabilidadSegura, que incluye tanto recursos de hardware como de software esenciales para sus operaciones diarias.

Activo	Tipo	Ubicación	Descripción	Propietario de activo
Computadora Director de la empresa	Hardware	Oficina Director de la empresa	Equipo de cómputo personal para trabajo administrativo y supervisión de operaciones contables	Director de la empresa
Computadora Contador 1	Hardware	Oficina de Contabilidad	Equipo de cómputo personal para registro y análisis contable	Contador 1
Computadora Contador 2	Hardware	Oficina de Contabilidad	Equipo de cómputo personal para registro y análisis contable	Contador 2

Computadora Empleado Administrativo 1	Hardware	Oficina General	Equipo de cómputo para tareas administrativas	Empleado Administrativo 1
Computadora Empleado Administrativo 2	Hardware	Oficina General	Equipo de cómputo para tareas administrativas	Empleado Administrativo 2
Computadora Empleado Administrativo 3	Hardware	Oficina General	Equipo de cómputo para tareas administrativas	Empleado Administrativo 3
Computadora Empleado Administrativo 4	Hardware	Oficina General	Equipo de cómputo para tareas administrativas	Empleado Administrativo 4
Router	Dispositivo de red	Sala de Redes	Dispositivo para gestionar la conectividad a internet	Empresa
Switch	Dispositivo de red	Sala de Redes	Dispositivo para la conexión en red de los equipos	Empresa
Impresora Compartida	Hardware	Oficina General	Impresora de uso común para documentos internos	Todos los empleados
Servidor (opcional)	Hardware	Centro de Datos	Servidor para almacenamiento de datos en la red interna	Empresa
Sistema Operativo	Software	Instalado en cada PC	Sistema operativo utilizado en las computadoras (Windows 10)	Todos los empleados
Suite Ofimática	Software	Instalado en cada PC	Herramientas de productividad (Microsoft Office)	Todos los empleados

Software Contable	Software	Instalado en PCs de contabilidad	Software especializado en contabilidad y gestión financiera (Contpaqi)	Todos los empleados

Gestión de comunicaciones

A continuación, se puede observar la forma en la que se comunica la empresa ContabilidadSegura. Cada grupo utiliza distintos métodos de comunicación según sus necesidades operativas y el tipo de interacción requerida, ya sea interna o externa.

Grupo/Departamento	Método de Comunicación
Director de la Empresa	Correo Electrónico, Reuniones Presenciales, Teléfono
Contabilidad	Correo Electrónico, Mensajería Instantánea, Teléfono
Empleados Generales	Correo Electrónico

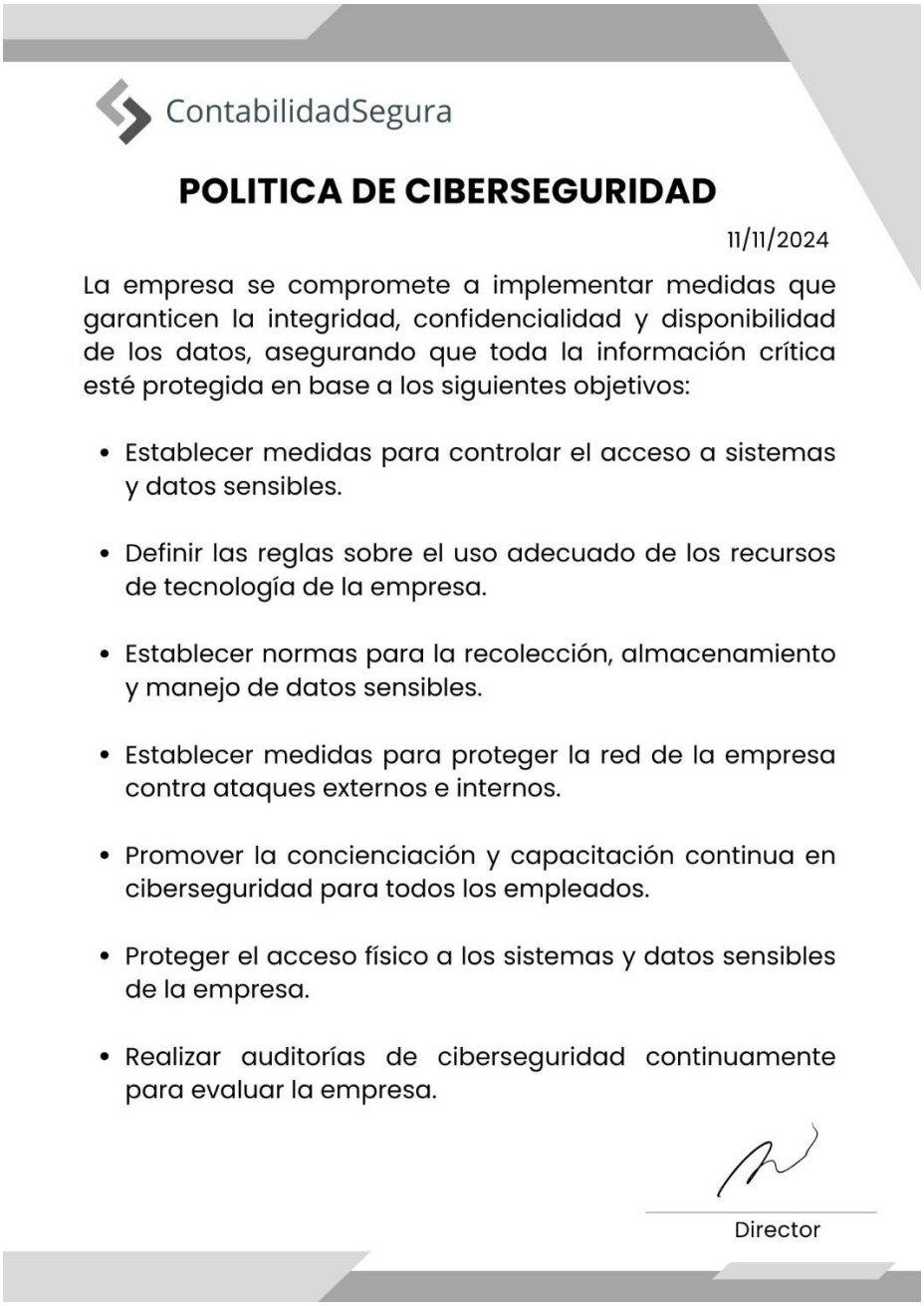
Descripción de la Gestión de Comunicaciones:

- **Dueño de la Empresa:** Utiliza el correo electrónico para comunicaciones formales y organiza reuniones presenciales para temas estratégicos o de alta relevancia con el equipo o cliente.
- **Contabilidad:** Este grupo emplea el correo electrónico para asuntos formales, mensajería instantánea para consultas rápidas dentro de la oficina, y el teléfono para atender a clientes o resolver situaciones urgentes.
- **Empleados Generales:** Se comunican principalmente mediante correo electrónico, lo cual permite una gestión organizada de las interacciones y facilita la trazabilidad de la información diaria.

Diseño de políticas, roles y responsabilidades

Políticas

Se ha realizado el documento de la política de ciberseguridad basado en las políticas establecidas en el Framework. Este documento tiene como objetivo definir y formalizar las medidas de protección que la empresa implementará para garantizar la integridad, confidencialidad y disponibilidad de la información crítica.



ContabilidadSegura

POLITICA DE CIBERSEGURIDAD

11/11/2024

La empresa se compromete a implementar medidas que garanticen la integridad, confidencialidad y disponibilidad de los datos, asegurando que toda la información crítica esté protegida en base a los siguientes objetivos:

- Establecer medidas para controlar el acceso a sistemas y datos sensibles.
- Definir las reglas sobre el uso adecuado de los recursos de tecnología de la empresa.
- Establecer normas para la recolección, almacenamiento y manejo de datos sensibles.
- Establecer medidas para proteger la red de la empresa contra ataques externos e internos.
- Promover la concienciación y capacitación continua en ciberseguridad para todos los empleados.
- Proteger el acceso físico a los sistemas y datos sensibles de la empresa.
- Realizar auditorías de ciberseguridad continuamente para evaluar la empresa.

Director

Roles y responsabilidades

A continuación, se definen los roles y responsabilidades de ContabilidadSegura, estos roles y responsabilidades están diseñados para asegurar que cada miembro de la empresa tenga claro su papel en la protección de la información y en el cumplimiento de las políticas de ciberseguridad.

Dada la estructura de la empresa, el **Director** de ContabilidadSegura también asume el rol de **Director de Ciberseguridad**, estableciendo la estrategia y visión en materia de protección de la información. Debido a la importancia de coordinar y supervisar las actividades de ciberseguridad, se ha designado a uno de los empleados como **Gerente de Ciberseguridad**, quien se encarga de implementar las políticas establecidas y gestionar las medidas de seguridad en la operación diaria de la empresa.

Rol	Responsabilidad
Director de Ciberseguridad	• Define la estrategia de ciberseguridad de la empresa y supervisa su implementación.
Gerente de Ciberseguridad	• Asegura que se implementen las políticas establecidas y coordina las actividades relacionadas con la protección de los sistemas e información de la empresa.
Contador	• Manejar y proteger los datos contables de los clientes, asegurando que se cumplan las políticas de acceso y confidencialidad.
Empleado Administrativo	• Realizar tareas administrativas y garantizar que se sigan los procedimientos de seguridad al manejar información sensible.

Implementación de medidas de ciberseguridad

Plan de riesgos

Plan de riesgos para los activos

Se presenta el **Plan de Riesgos de Activos**, diseñado para identificar y gestionar los riesgos asociados a los activos tecnológicos de la empresa. Cada activo ha sido evaluado en función de los riesgos potenciales a los que podría estar expuesto, como el robo de información, malware, acceso no autorizado y pérdida de datos. Se ha definido el impacto y la probabilidad de ocurrencia de cada riesgo, junto con medidas preventivas específicas para mitigar estos riesgos.

Este plan asegura que cada activo cuente con protecciones adecuadas, contribuyendo a la integridad y seguridad de la infraestructura tecnológica de la empresa. Además, se han asignado responsables para cada activo, quienes serán los encargados de supervisar y garantizar el cumplimiento de las medidas de seguridad implementadas.

Activo	Tipo	Riesgos Potenciales	Impacto	Probabilidad	Prevención	Responsable
Computadora Director	Hardware	Robo de información, malware	Extremo	Media	Uso de antivirus, contraseñas seguras y políticas de acceso	• Director de la Empresa • Gerente de Ciberseguridad
Computadora Contador 1	Hardware	Pérdida de datos, acceso no autorizado	Alto	Alta	Respaldo de datos, cifrado y control de acceso	• Gerente de Ciberseguridad • Contador 1
Computadora Contador 2	Hardware	Pérdida de datos, acceso no autorizado	Alto	Alta	Respaldo de datos, cifrado y control de acceso	• Gerente de Ciberseguridad • Contador 2
Computadora Empleado Administrativo 1	Hardware	Acceso no autorizado, phishing	Medio	Alta	Capacitación en ciberseguridad, uso de contraseñas seguras	• Gerente de Ciberseguridad • Empleado Administrativo 1
Computadora Empleado Administrativo 2	Hardware	Acceso no autorizado, phishing	Medio	Alta	Capacitación en ciberseguridad, uso de contraseñas seguras	• Gerente de Ciberseguridad • Empleado Administrativo 2
Computadora Empleado Administrativo 3	Hardware	Acceso no autorizado, phishing	Medio	Alta	Capacitación en ciberseguridad, uso de	• Gerente de Ciberseguridad

					contraseñas seguras	• Empleado Administrativo 3
Computadora Empleado Administrativo 4	Hardware	Acceso no autorizado, phishing	Medio	Alta	Capacitación en ciberseguridad, uso de contraseñas seguras	• Gerente de Ciberseguridad • Empleado Administrativo 4
Router	Dispositivo de Red	Ataque de red, acceso no autorizado	Alto	Media	Configuración segura, implementación para proteccion de la red	• Gerente de Ciberseguridad
Switch	Dispositivo de Red	Acceso no autorizado a la red interna	Alto	Baja	Restricción de acceso físico, configuración de seguridad	• Gerente de Ciberseguridad
Servidor (opcional)	Hardware	Pérdida de datos, ataques de red	Muy Alto	Media	Respaldo regular, firewall, acceso restringido	• Gerente de Ciberseguridad
Sistema Operativo	Software	Vulnerabilidades, malware	Alto	Media	Actualizaciones automáticas, uso de antivirus	• Gerente de Ciberseguridad
Suite Ofimática	Software	Pérdida de datos, malware	Medio	Media	Respaldo de archivos, uso de antivirus	• Gerente de Ciberseguridad
Software Contable	Software	Acceso no autorizado, pérdida de datos	Muy Alto	Media	Cifrado de datos, control de acceso, respaldo regular	• Gerente de Ciberseguridad • Contador 1 y 2

Plan de riesgos para las comunicaciones

Se presenta el **Plan de Riesgo de Comunicaciones**, que aborda los posibles riesgos en los métodos de comunicación utilizados en la empresa. Los riesgos identificados incluyen phishing, interceptación de comunicaciones y divulgación de datos sensibles. Este plan describe las medidas preventivas que se implementarán para proteger la comunicación interna y externa de la organización, tales como capacitación en ciberseguridad, uso de herramientas seguras y encriptación de mensajes. La asignación de responsables en cada departamento asegura que los empleados sean conscientes de los riesgos y cumplan con los procedimientos establecidos para mantener la seguridad en todas las interacciones de la empresa.

Departamento	Método de Comunicación	Riesgos Potenciales	Prevención	Responsable
Dirección	Correo Electrónico, Teléfono, Reuniones	Phishing, interceptación de llamadas	Capacitación en ciberseguridad, uso de herramientas seguras	• Director de la Empresa • Gerente de Ciberseguridad
Contabilidad	Correo Electrónico, Mensajería Instantánea, Teléfono	Divulgación de datos sensibles, phishing	Capacitación en ciberseguridad, encriptación de mensajes	• Gerente de Ciberseguridad
Empleados Generales	Correo Electrónico	Phishing, malware	Capacitación, uso de filtros de correo y herramientas de seguridad	• Gerente de Ciberseguridad

Seguridad de los datos

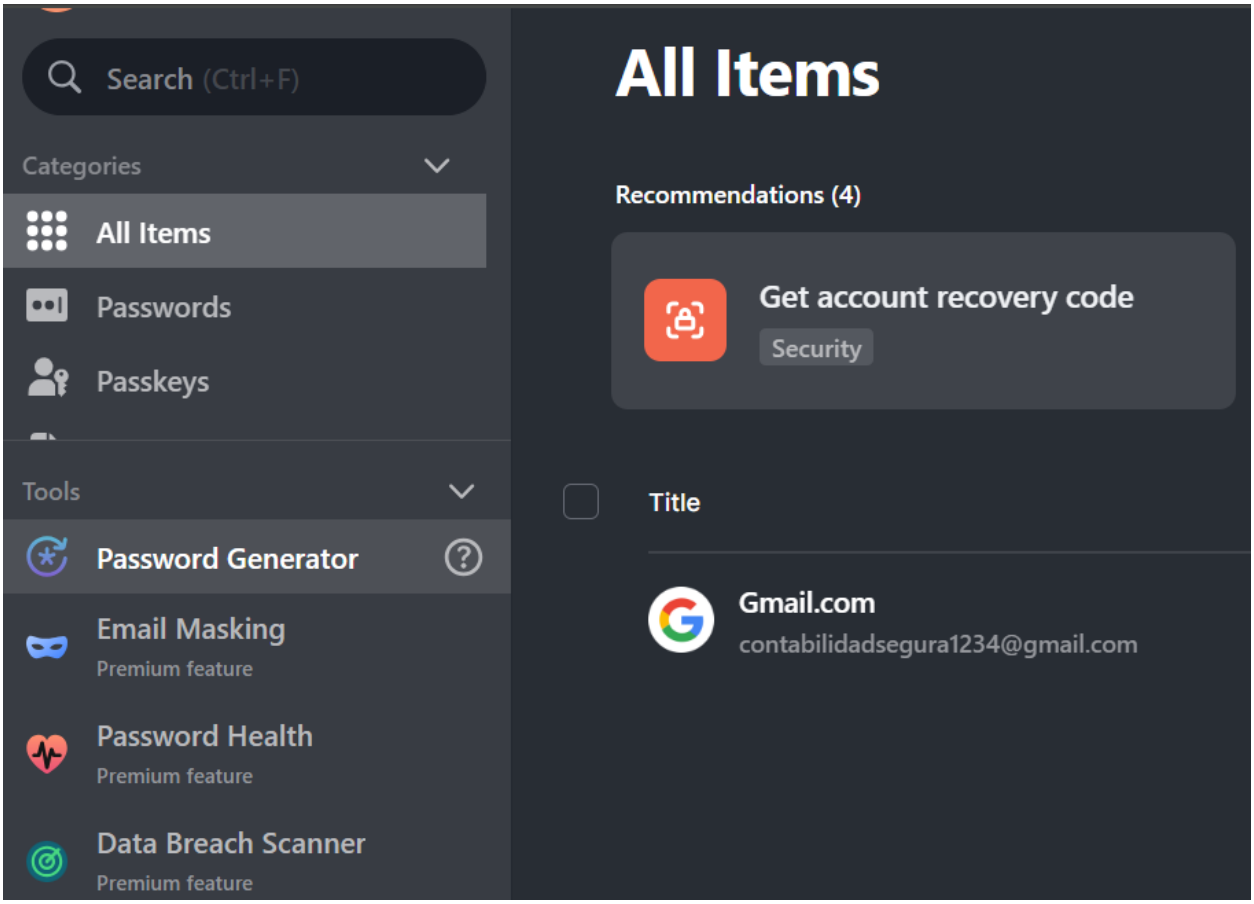
Gestión de contraseñas

Para la Protección de Accesos, se ha implementado el uso del Gestor de Contraseñas NordPass. Esta herramienta permite almacenar, gestionar y proteger de forma segura todas las contraseñas de la empresa, centralizando el acceso a las credenciales de manera encriptada. NordPass garantiza que las contraseñas estén protegidas mediante algoritmos de cifrado avanzados, reduciendo el riesgo de accesos no autorizados y asegurando que los empleados utilicen contraseñas fuertes y únicas para cada cuenta.

Ingresar a NordPass en el siguiente link:

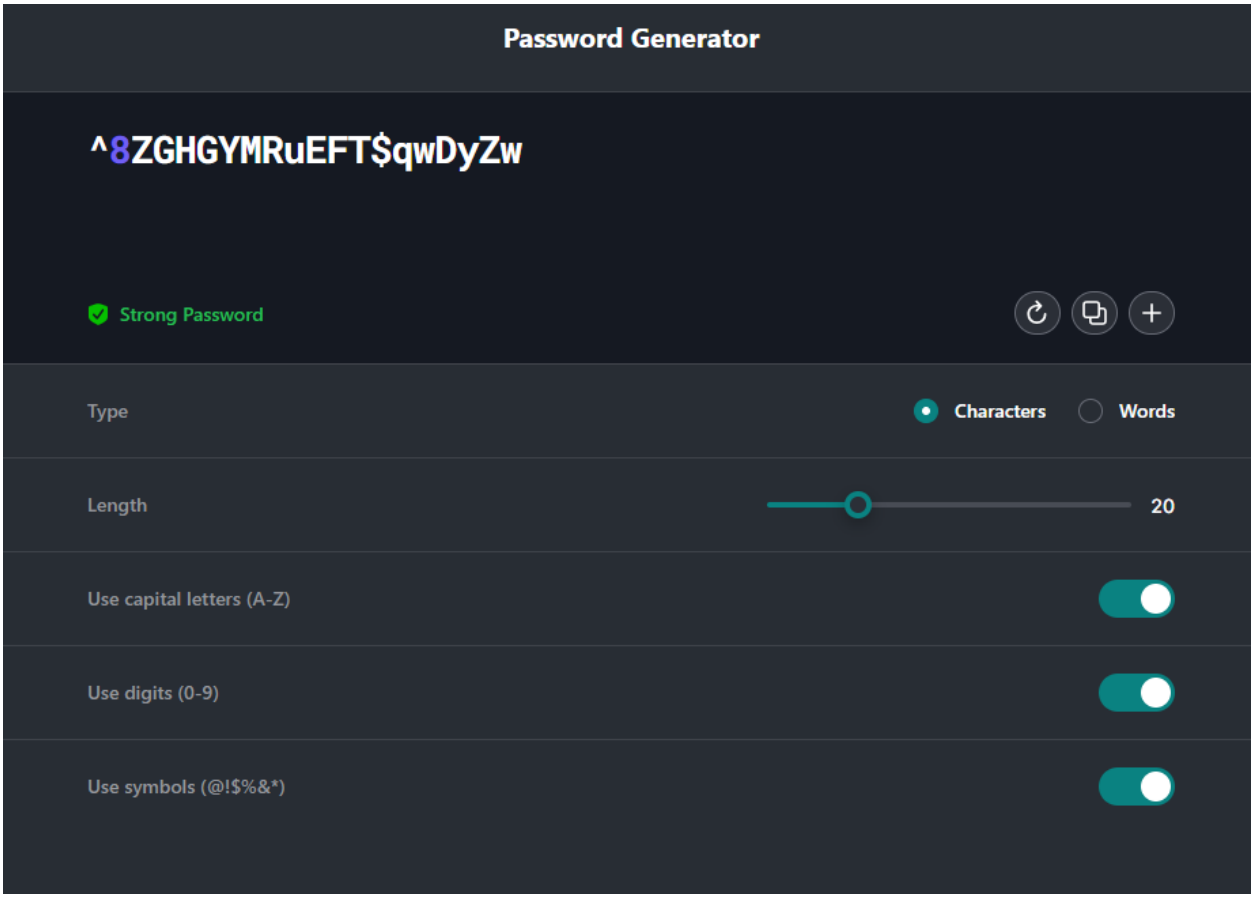
https://nordpass.com/es/plans/

A continuación, se muestra las capturas de pantalla del uso de la herramienta, en su versión gratuita.



Las configuraciones seleccionadas incluyen:

- **Tipo de caracteres**: La contraseña está configurada para utilizar una combinación de letras, números y símbolos.
- **Longitud**: La contraseña generada tiene una longitud de 20 caracteres, lo cual proporciona una mayor seguridad frente a ataques de fuerza bruta.
- **Uso de mayúsculas (A-Z)**: Se incluyen letras mayúsculas para incrementar la complejidad.
- **Uso de dígitos (0-9)**: Se incluyen números para añadir variedad y dificultar la predicción de la contraseña.
- **Uso de símbolos (@!$%&*)**: Se incluyen caracteres especiales, lo cual aumenta significativamente la seguridad de la contraseña.



El **Gerente de Ciberseguridad** fue responsable de gestionar las contraseñas de acuerdo con estas características, asegurando que todas las contraseñas utilizadas en la empresa sean robustas y cumplan con los estándares de seguridad establecidos.

Gestión de copias de seguridad

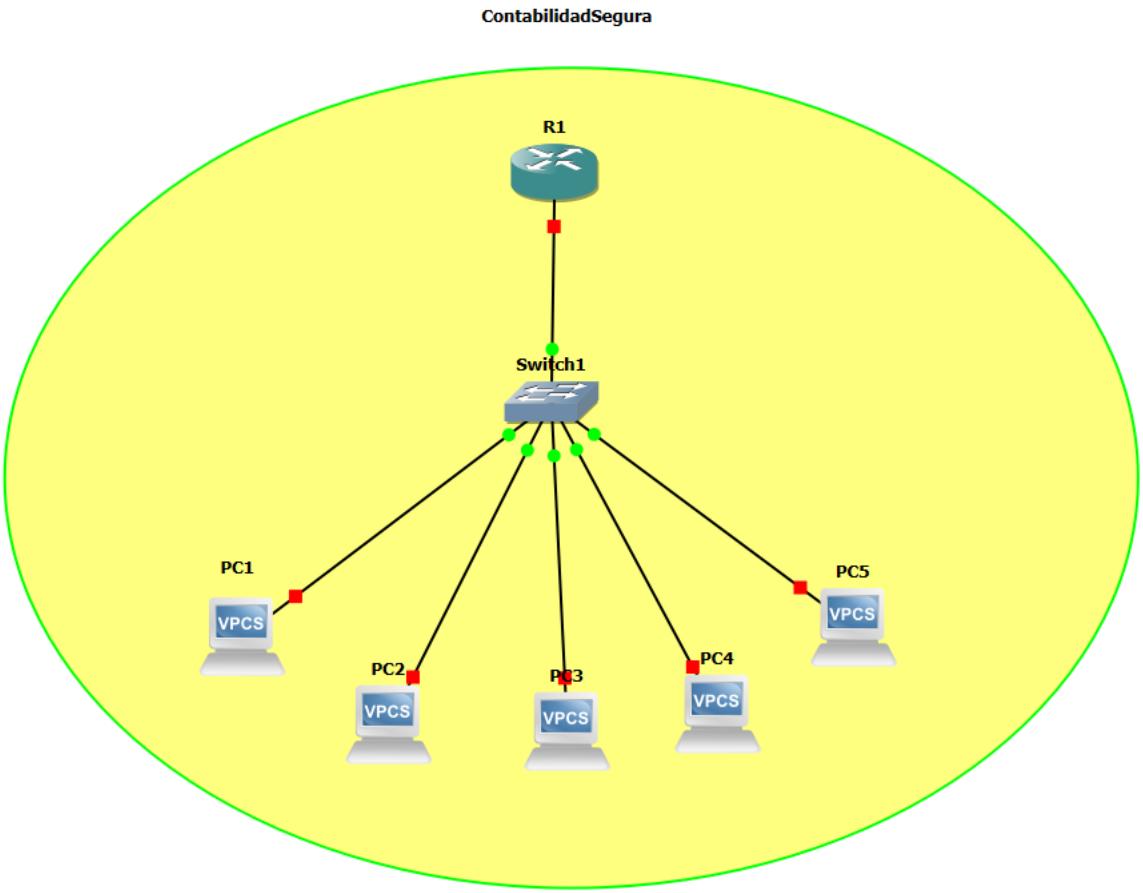
Utilizando GNS3 se realizó la topología de red de la empresa, en base a ello se hicieron copias de seguridad de los equipos, para proteger la información de la empresa…

Seguridad de la red

Se utilizo la herramienta GNS3 para hacer la topología de la red de la empresa ContabilidadSegura.

A continuación, se muestra la implementación de las prácticas de ciberseguridad para la protección de la red.

Se muestra una red LAN, se configuro la red con los 7 equipos, 1 switch, 1 router y 1 servidor.



Conciencia y capacitación

La capacitación en ciberseguridad busca sensibilizar a los empleados sobre las amenazas a la seguridad de la información y proporcionarles las herramientas necesarias para proteger los activos de la empresa. Esto incluye medidas básicas de seguridad, gestión adecuada de contraseñas, detección de correos maliciosos, y protocolos en caso de incidentes.

Objetivos de aumentar la conciencia de ciberseguridad en ContabilidadSegura

- Aumentar el conocimiento de los empleados sobre ciberseguridad.
- Promover el uso de buenas prácticas en el manejo de la información.
- Reducir el riesgo humano como punto de vulnerabilidad en la seguridad de la empresa.
- Asegurar que todos los empleados comprendan claramente sus roles y responsabilidades en relación con la ciberseguridad.

Estrategia de Capacitación

Para aumentar la conciencia en ciberseguridad, se impartirán capacitaciones dirigidas a todos los empleados de la empresa ContabilidadSegura. Estas capacitaciones tienen como objetivo sensibilizar a los empleados sobre las amenazas más comunes, enseñarles buenas prácticas de seguridad, y garantizar que conozcan sus roles y responsabilidades. Las capacitaciones incluirán talleres, simulaciones y recursos educativos, como se detalla en el siguiente cronograma:

Cronograma de Capacitación

Capacitación Inicial

Público: Todos los empleados.

Duración: 2 horas.

Contenido: Introducción a la ciberseguridad, buenas prácticas, gestión de contraseñas y roles y responsabilidades.

Frecuencia: Se impartirá al momento de la incorporación de nuevos empleados o al inicio del plan de capacitación.

Talleres Trimestrales de Refuerzo

Público: Todos los empleados.

Duración: 1 hora por sesión.

Contenido:

- Actualización sobre nuevas amenazas.
- Prácticas avanzadas de seguridad.
- Resolución de casos prácticos.

Simulaciones Semestrales de Phishing

Público: Todos los empleados.

Duración: Variable según los resultados.

Contenido: Correos electrónicos simulados diseñados para evaluar la capacidad de los empleados para identificar intentos de phishing.

Objetivo: Aprender de los errores y reforzar la capacidad de respuesta.

Evaluación de Capacitación en Ciberseguridad

Se realizará una evaluación a todos los usuarios para medir el nivel de comprensión y aplicación de las prácticas de ciberseguridad adquiridas por los empleados de ContabilidadSegura durante las capacitaciones y actividades de sensibilización. También busca identificar áreas de mejora.

La evaluación comprenderá los siguientes aspectos:

Evaluación Teórica (40%)

Un cuestionario con preguntas de opción múltiple y verdadero/falso.

Ejemplos de Preguntas:

¿Qué características debe tener una contraseña segura?

¿Cómo reconocer un correo electrónico de phishing?

¿A quién debe reportarse un incidente de seguridad?

Resultado Esperado: Al menos un 80% de respuestas correctas.

Simulaciones Prácticas (40%)

Simulación de Phishing: Se enviará un correo falso de phishing para evaluar si los empleados detectan y reportan la amenaza correctamente.

Escenario Simulado:

Un incidente de seguridad ficticio será planteado para que los empleados demuestren cómo actuarían según los protocolos establecidos.

Criterios de Evaluación:

- Identificación de la amenaza (phishing).
- Correcta comunicación del incidente al Gerente de Ciberseguridad.

Encuestas de Percepción y Confianza (20%)

Una breve encuesta para medir la percepción de los empleados sobre la importancia de la ciberseguridad en la empresa y su confianza en aplicar las prácticas aprendidas.

Ejemplo de Preguntas:

¿Te sientes más preparado para detectar correos electrónicos sospechosos después de la capacitación?

¿Qué temas te gustaría reforzar en futuras capacitaciones?

Indicadores Clave (KPIs)

Tasa de Aprobación:

Al menos el 90% de los empleados deben aprobar las evaluaciones teóricas y prácticas.

Resultados de Simulaciones de Phishing:

Reducción del porcentaje de empleados que caen en simulaciones de phishing (objetivo: menos del 10%).

Mejora en la Percepción:

Al menos el 85% de los empleados deben reportar sentirse más seguros y capacitados para manejar incidentes de ciberseguridad.

Cumplimiento de Roles y Responsabilidades:

El 100% de los empleados debe comprender y cumplir sus roles en los procesos de ciberseguridad.

Plan ante incidentes

Se realizo un plan de Mitigación de Incidentes diseñado para abordar problemas específicos en ContabilidadSegura y garantizar una respuesta rápida y efectiva, minimizando los impactos operativos y reputacionales.

Estos son los incidentes provenientes de ContabilidadSegura basado en el esquema del Framework.

Incidente 1: Phishing

Se detecta un correo electrónico sospechoso enviado a múltiples empleados, que intenta obtener credenciales de acceso a los sistemas contables de la empresa.

Mitigación:

- Notificar al Gerente de Ciberseguridad inmediatamente para analizar el correo sospechoso.
- Instruir a los empleados que hayan recibido el correo para que no hagan clic en enlaces ni descarguen adjuntos.
- Bloquear el remitente sospechoso en el servidor de correo electrónico.
- Realizar una verificación del sistema de contraseñas para identificar posibles accesos comprometidos.
- Informar a todos los empleados sobre el ataque para aumentar la precaución.

Responsable:

El Gerente de Ciberseguridad liderará la respuesta al incidente y coordinará las acciones necesarias, con el apoyo del Director de Ciberseguridad.

Incidente 2: Malware en un Equipo de Contabilidad

Un equipo del departamento de contabilidad muestra comportamiento anómalo (lentitud extrema y ventanas emergentes) y se sospecha que está infectado con malware.

Mitigación:

- Desconectar inmediatamente el equipo afectado de la red para evitar la propagación del malware.
- Analizar el equipo afectado utilizando un software antivirus y herramientas de detección de malware.
- Realizar una limpieza completa del sistema o reinstalar el sistema operativo si es necesario.
- Restaurar los datos afectados desde una copia de seguridad segura.
- Implementar medidas adicionales para prevenir infecciones similares, como actualizar el software y reforzar el firewall.

Responsable:

El Gerente de Ciberseguridad supervisará la limpieza del sistema, mientras que el empleado afectado será instruido para reportar cualquier comportamiento anómalo.

Incidente 3: Fuga de Información en Correo Electrónico

Un empleado envía accidentalmente datos sensibles de un cliente a un destinatario incorrecto.

Mitigación:

- Contactar al destinatario para pedir que elimine el correo y confirme la eliminación.
- Notificar al cliente afectado sobre el incidente, garantizando la transparencia.
- Revisar las políticas de envío de correos electrónicos y capacitar a los empleados sobre el manejo adecuado de información sensible.
- Implementar un sistema de verificación en correos electrónicos para alertar sobre posibles envíos a destinatarios externos no habituales.

Responsable:

El Gerente de Ciberseguridad gestionará la comunicación con el destinatario y cliente afectado, mientras el empleado responsable recibe capacitación adicional.

Mejora continua

Auditoria

Se realizo una auditoria para verificar el cumplimiento de las estrategias de ciberseguridad, estos son los resultados.

Práctica	Perfil Actual	Perfil Objetivo	Avance	Avance Por Fase
Definir PYME	Nivel 5	Nivel 5	100%	100%
Definir perfil actual y objetivo	Nivel 5	Nivel 5	100%	
Inventariar Infraestructura: activos hardware y software	Nivel 5	Nivel 5	100%	
Gestionar las comunicaciones	Nivel 5	Nivel 5	100%	
Definir las políticas de ciberseguridad de la organización	Nivel 5	Nivel 5	100%	100%
Definir los roles y las responsabilidades de seguridad	Nivel 5	Nivel 5	100%	
Desarrollar un plan de riesgos a través de una evaluación	Nivel 5	Nivel 5	100%	100%
Implementar medidas de protección de los datos	Nivel 5	Nivel 5	100%	
Implementar medidas de protección de la red	Nivel 5	Nivel 5	100%	
Implementar una cultura de ciberseguridad	Nivel 5	Nivel 5	100%	
Desarrollar un plan para mitigar incidentes	Nivel 5	Nivel 5	100%	
Realizar auditoría de ciberseguridad	Nivel 5	Nivel 5	100%	100%
Actualizar las estrategias de seguridad	Nivel 5	Nivel 5	100%	

Avance General	**100%**

Las prácticas de ciberseguridad del Framework se han implementado, sin embargo, se realizarán más auditorías con la implementación de nuevas estrategias de ciberseguridad en base a las nuevas amenazas e incidentes.

Actualizar las estrategias de ciberseguridad

Se realizo un plan para mantener y reforzar la ciberseguridad de ContabilidadSegura mediante la revisión periódica y actualización de políticas, herramientas, y prácticas, con el fin de adaptarse a nuevas amenazas y tecnologías.

Etapas del Plan

Evaluación Inicial

Objetivo: Identificar las áreas que necesitan actualización en las estrategias de seguridad existentes.

- Revisar el cumplimiento de las políticas de ciberseguridad actuales.
- Analizar incidentes de seguridad pasados para determinar vulnerabilidades recurrentes.
- Evaluar el estado actual de la infraestructura de seguridad (hardware, software, red).
- Realizar una encuesta entre empleados para identificar áreas de mejora en capacitación y herramientas.

Responsable: Gerente de Ciberseguridad.

Investigación de Nuevas Amenazas

Objetivo: Conocer las últimas tendencias y ataques cibernéticos que puedan afectar a la empresa.

- Consultar informes actualizados de amenazas cibernéticas (ejemplo: ransomware, phishing avanzado).
- Revisar boletines de seguridad de proveedores de software y hardware usados en la empresa.
- Participar en foros, webinars o cursos especializados en ciberseguridad.

Responsable: Gerente de Ciberseguridad con apoyo del Director de Ciberseguridad.

Actualización de Políticas

Objetivo: Modificar las políticas de ciberseguridad para reflejar las nuevas necesidades y amenazas detectadas.

- Revisar las políticas de contraseñas y acceso remoto.
- Actualizar el plan de respuesta ante incidentes para incorporar lecciones aprendidas de simulaciones o ataques previos.
- Implementar nuevos controles de acceso si es necesario (como autenticación multifactor).

Responsable: Director de Ciberseguridad.

Implementación de Nuevas Herramientas y Tecnologías

Objetivo: Incorporar herramientas modernas que refuercen la seguridad de los sistemas y datos.

- Evaluar e implementar actualizaciones de software existentes (ejemplo: nuevas versiones del software contable o de NordPass).
- Incorporar nuevas herramientas de ciberseguridad.
- Reforzar el servidor con actualizaciones de sistema operativo y el IDS/IPS snort.

Responsable: Gerente de Ciberseguridad con apoyo del personal técnico.