Diseño De Un Modelo De Consultoría Enfocado A La Importancia De La Ciberseguridad En Pymes.

Edna M. Torres, Juan S. Pardo y Norman A. Molina

Director: Ing. Annuar de la Barrera Padilla

Trabajo De Grado Para Optar Por El Título De Ingeniero De Telecomunicaciones.

Corporación Universitaria UNITEC

Bogotá, 2023

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Justificación

Desde el punto de vista práctico, este proyecto responde a la necesidad que tienen las pequeñas y medianas empresas de poder visibilizar y darle la importancia adecuada a la ciberseguridad para así evitar la pérdida de información, suplantación de identidad, secuestro de datos, entre otros.

Se enfocará en concientizar a los colaboradores de las empresas pequeñas y medianas en la importancia de un buen manejo de las herramientas desde el punto de vista de la seguridad informática, creando lineamientos y buenas prácticas de manejo de la información y del aseguramiento de esta que permitan al colaborador actuar con responsabilidad al momento del tratamiento de la información en cualquiera de los medios usuales virtuales como correos electrónicos, páginas web, aplicaciones, etc.

Para hacer frente a esta creciente amenaza, es importante que las empresas y organizaciones de la región inviertan en medidas de seguridad informática, como el cifrado de datos, el monitoreo constante de redes y sistemas, la formación de empleados en seguridad informática y la implementación de políticas de seguridad adecuadas.

Por lo tanto, este proyecto busca mejorar la seguridad informática de estas empresas a través de la concientización y la formación en seguridad informática, para que puedan identificar y mitigar los riesgos y amenazas potenciales. También busca mejorar la implementación de políticas y procedimientos de seguridad, incluyendo la actualización de software y sistemas, la configuración adecuada de redes y la formación de empleados en prácticas seguras.

Objetivos

Objetivo General:

Generar un modelo de consultoría y servicio especializada en ciberseguridad que brinde asesoría y acompañamiento a pequeñas y medianas empresas.

Objetivos Específicos:

- Clasificar activos según criticidad, riesgos y responsable.
- Evaluar el nivel de seguridad de las empresas acorde al sector de la industria en el que se desarrolla.
- Valorar el nivel de conocimiento de ciberseguridad a los colaboradores de cada empresa o recurso humano.
- Desarrollar campañas de concientización interna sobre los riesgos a los que se exponen las empresas.
- Crear lineamientos de seguridad y buenas prácticas de las herramientas de seguridad.

Marco Teórico y Estado del Arte.

Marco Referencial

La ciberseguridad se ha convertido en un tema crucial para las empresas de todo el mundo y con el creciente número de ataques cibernéticos y la cada vez mayor sofisticación de estos, las empresas de todos los tamaños están en riesgo. Las pequeñas y medianas empresas (PYMEs), en particular, pueden estar más expuestas a las amenazas cibernéticas debido a su falta de recursos para implementar medidas de seguridad adecuadas y la falta de conocimiento sobre las mejores prácticas de ciberseguridad.

De acuerdo con los estudios que se han ido realizan se encontró que coexisten investigaciones relevantes a trabajos que tratan la misma problemática identificada, los cuales citamos a continuación:

El artículo del investigador Felipe Gonzalez (Gonzalez, 2023) cuenta como una de las principales razones hace que las Pymes sean el foco principal de los ciberataques y esto se debe a la no implementación de sistemas que protejan su información; el 43% de los casos de ciberataques a nivel global tienen como objetivo a una pyme, es un porcentaje significativo el cual se debe tener en consideración.

En el proyecto (Ortega & Javier, 2022) encontramos similitudes y comentan que las Pymes cuando presentan un ciberataque optan por no denunciar para no afectar su reputación, debido a esto este proyecto propone protocolos básicos de ciberseguridad para pymes, como herramientas fundamentales y principal estrategia de defensa frente a un ciberataque.

Como hablan en el artículo (Semana, 223) de la revista semana explican la importancia al realizar unas buenas prácticas en ciberseguridad, el robo de información por medio de ransomware o software malicioso puede hacer que a la empresa le soliciten un rescate y esto

no garantiza que los delincuentes restablezcan los documentos confidenciales por ende la importancia de generar unas buenas contraseñas, realizar las respectivas copias de seguridad, actualización de software importantes para la compañía y generar restricciones en la accesibilidad de la información.

Hablando de teorías y buenas prácticas encontramos el proyecto (Martinez, s.f.) “Herramientas de para la prevención de fugas de información a través del correo electrónico en un entorno corporativo”, como bien sabemos el correo electrónico es el medio que genera mayor vulnerabilidad en las empresas o también al individuo en general. Gracias a las buenas prácticas propuestas por esta ponencia el ingeniero Ruben Marroig propone una serie de recomendaciones como, por ejemplo: Cifrar el correo electrónico, uso de contraseñas correctas y cambiarlas regularmente, no abrir correos provenientes de desconocidos, no responder correos spam, entre otros.

En el artículo de la universidad de Alfonso X (Javier Santiago & Sanchez Allende, 2017, pág. 4) el sabio que trabaja el tema de la ciberseguridad en las empresas nos muestra los principales riesgos de las empresas en el siglo XXI, donde los activos de información son principalmente lo que atacan en las empresas, se relacionan también las principales amenazas que afectan en las empresas de diferentes sectores, hace también énfasis en la capacidad que tienen los empleados de muchas empresas para poder detectar un intruso en la información.

Marco Conceptual

A continuación, se mencionarán algunas definiciones importantes para una mejor comprensión de este proyecto:

La ciberseguridad se apoya en una serie de medidas y herramientas para lograr su objetivo, es muy importante tener en cuenta los conceptos más relevantes que nos logran aclarar un poco el tema y comprender ciertas medidas que se pueden tener en cuenta en el momento de realizar alguna tarea.

Glosario de ciberseguridad

Amenaza cibernética: Es una acción o evento malicioso que tiene como objetivo comprometer la seguridad de los sistemas informáticos y la información que contienen.

Ataque de phishing: Es una técnica de ingeniería social en la que los atacantes intentan engañar a los usuarios para obtener información confidencial, como contraseñas o datos bancarios, haciéndose pasar por una entidad legítima.

Malware: Es software malicioso diseñado para dañar, acceder o tomar el control de un sistema informático sin el consentimiento del propietario. Incluye virus, gusanos, troyanos, ransomware, entre otros.

Firewall: Es una barrera de seguridad que controla el tráfico de red, filtrando y bloqueando las conexiones no autorizadas y protegiendo los sistemas contra intrusiones externas.

Autenticación de dos factores: Es un método de seguridad que requiere dos formas diferentes de autenticación, generalmente una contraseña y un código temporal enviado a través de un dispositivo móvil, para verificar la identidad de un usuario.

VPN (Red Privada Virtual): Es una tecnología que establece una conexión segura y encriptada entre un dispositivo y una red privada a través de Internet, permitiendo el acceso remoto seguro a recursos de la red.

Vulnerabilidad: Es una debilidad en un sistema o aplicación que puede ser explotada por un atacante para comprometer su seguridad.

Análisis de riesgos: Es el proceso de identificar, evaluar y priorizar los riesgos de seguridad informática, determinando las amenazas potenciales y las posibles consecuencias para la organización.

Auditoría de seguridad: Es una evaluación sistemática de los sistemas, redes y políticas de seguridad de una organización para verificar el cumplimiento de las mejores prácticas de seguridad e identificar posibles vulnerabilidades.

Política de seguridad de la información: Es un conjunto de directrices y reglas establecidas por una organización para proteger la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos.

Ingeniería social: Es una táctica en la que los atacantes manipulan a las personas para obtener información confidencial o persuadirlos a realizar acciones que puedan comprometer la seguridad.

Copia de seguridad: Es una réplica de los datos almacenados en un sistema, realizada con el fin de proteger la información en caso de pérdida, corrupción o eliminación accidental.

Incidente de seguridad: Es un evento que indica una posible violación de la seguridad informática, como un ataque exitoso, una intrusión no autorizada o la exposición de información confidencial.

Parche de seguridad: Es una actualización o corrección de software diseñada para solucionar vulnerabilidades conocidas y mejorar la seguridad de un sistema o aplicación.

Criptografía: Es el proceso de codificación y decodificación de información con el objetivo de asegurar su confidencialidad, integridad y autenticidad.

Política de gestión de contraseñas: Es un conjunto de reglas y mejores prácticas establecidas por una organización para garantizar contraseñas seguras y su correcta gestión.

Auditoría de cumplimiento: Es una evaluación independiente de los sistemas y procesos de una organización para verificar el cumplimiento de leyes, regulaciones y estándares relacionados con la seguridad de la información.

Token de seguridad: Es un dispositivo físico o una aplicación móvil que genera códigos únicos y temporales utilizados para la autenticación de dos factores y el acceso seguro a sistemas y servicios.

Marco Legal

Dentro de la legislación colombiana se encuentra varias leyes que regulan el manejo la protección de los datos así mismo como la penalización de delitos informáticos reconocidos en el País. Las siguientes son las principales leyes que rigen este este tema.

Tabla 1

Principales leyes que rigen en Colombia sobre el cibercrimen

NOMBRE DEL ARTICULO O TRABAJO	RESUMEN	REFERENCIA
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del	Ley 527 de 1999 - Gestor Normativo. (s/f). Gov.co. Recuperado el 10 de abril de 2023, de https://www.funcionpublica.g

	comercio electrónico y de las firmas digitales.	ov.co/eva/gestornormativo/norma.php?i=4276
Ley 594 de 2000	"Por medio de la cual se dicta la ley general de archivos y se dictan otras disposiciones". regulan la función archivística del estado. diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por la presente ley	LEY 594 DE 2000. (s/f). Gov.co. Recuperado el 10 de abril de 2023, de https://normativa.archivogeneral.gov.co/ley-594-de-2000/
Ley 679 de 2001	Tiene por objeto dictar medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad.	Ley N° 679/2001. Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores. (s/f). Unesco.org. Recuperado el 10 de abril de 2023, de https://siteal.iiep.unesco.org/bdnp/622/ley-ndeg-6792001-estatuto-
Ley 1581 de 2012	Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.	Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012]. (s/f). Senado de la República de Colombia. Recuperado el 10 de abril de 2023, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
El Decreto 338 de marzo de 2022	Establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital y crea el modelo y las instancias de gobernanza de seguridad digital entre otras disposiciones.	Technology, C. B. (10 de marzo de 2022). Cross Border Technology. Obtenido de https://www.crossbordertech.com/decreto-338-de-marzo-de-2022-ciberseguridad-en-colombia/#:~:text=El%20Decreto%20338%20de%20marzo,seguridad%20digital%20entre%20otras%20disposiciones.

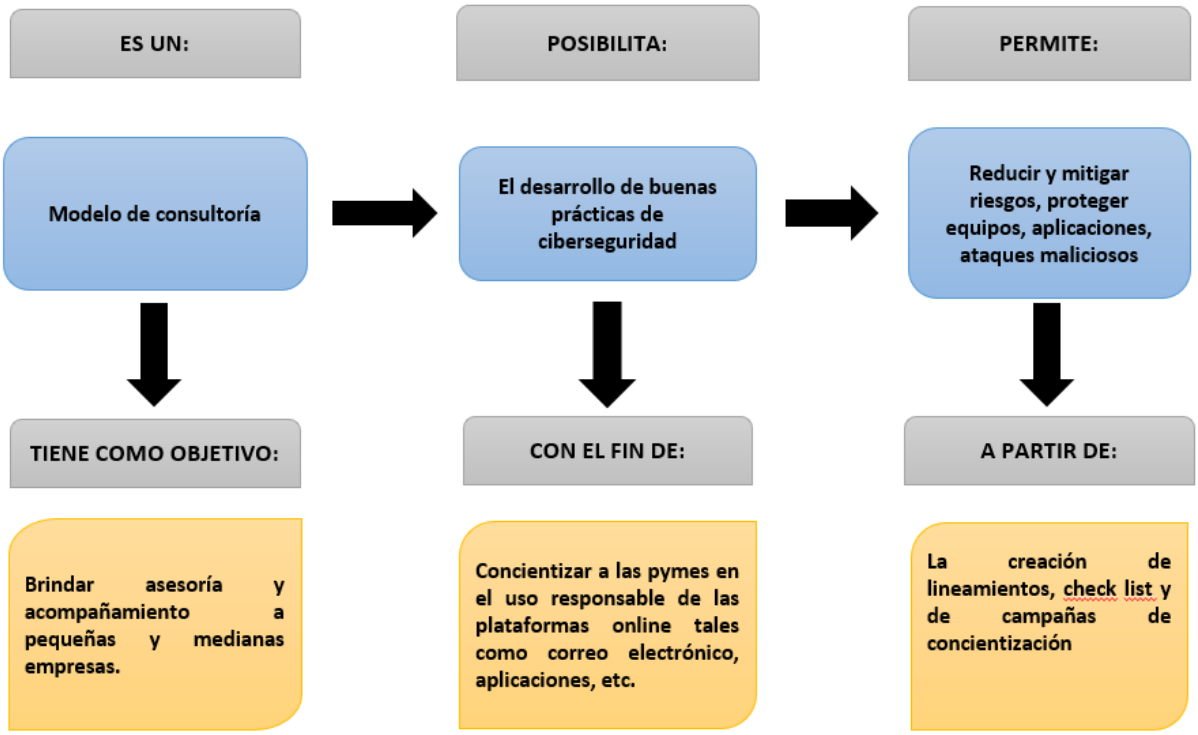
Ley 1928 de 24 de Julio de 2018	Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest. El Congreso de Colombia Visto el texto del “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.	Legis.xparta (s/f). Legis.co. Recuperado el 10 de abril de 2023, de https://xperta.legis.co/visor/legcol/legcol_84eb23248dd34877ac28f04ef2343074/coleccion-de-legislacion-colombiana/ley-1928-de-julio-24-de-2018

Estado del arte

Esta imagen (**Diagrama del estado del arte**) muestra de manera resumida la importancia de nuestro proyecto, dando como mayor valor e impacto el desarrollo de las buenas prácticas de ciberseguridad en una empresa, ayudando a reducir riesgos en la perdida de información o ataques cibernéticos de las Pymes.

Figura 1

Diagrama del estado del arte.



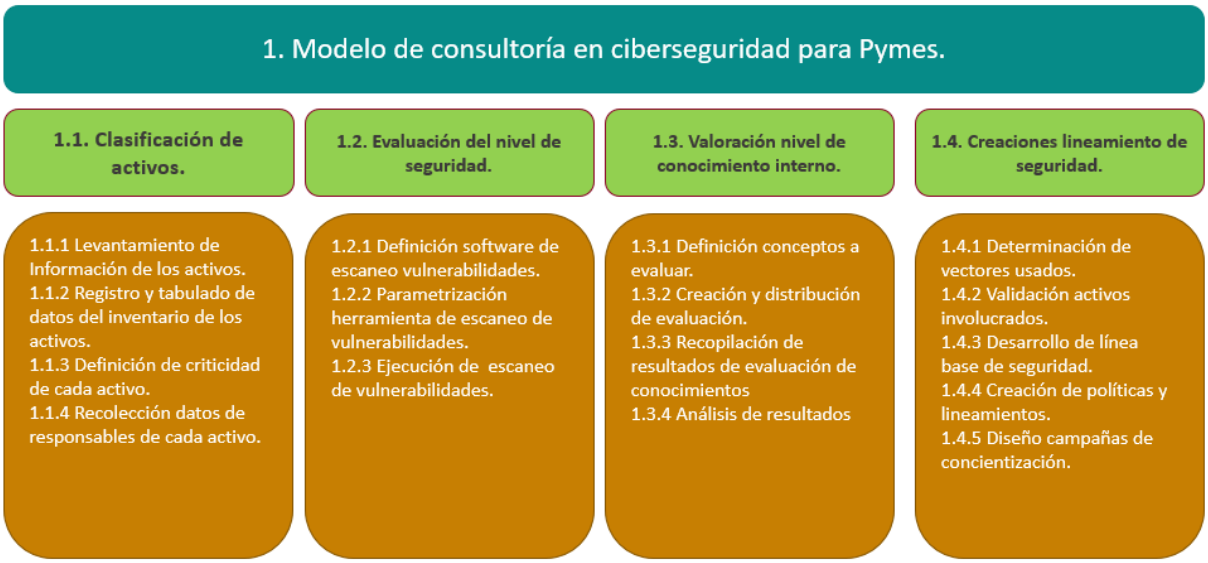
Método (aplicación de la gerencia de proyectos bajo lineamiento PMI)

Estudio y Análisis

A partir de las 4 fases del proyecto se crea el diccionario de actividades de trabajo en cada una de estas fases en el cual se generan 16 paquetes de trabajo divididas en cada uno de los bloques que se ilustra en la Figura 2.

Figura 2

Mapa de actividades del proyecto.



Nota. El diagrama se describen las diferentes fases del proyecto junto con el paquete de tareas correspondiente a cada fase.

Estructura de desglose de trabajos (EDT)

De la anterior definición del mapa de actividad se genera el documento de la Estructura de Desglose del Trabajo (EDT), la cual está plasmado en la figura 3, 4 y 5. En este formato se relacionan el paquete de actividades con los responsables, fechas de inicio y fin de cada actividad, posibles riesgos, recursos utilizados entre otras variables.

Figura 3

Formato EDT (Estructura de descomposición de trabajo) de actividades.

I. Datos del Proyecto

Proyecto	Nombre			Sigla
	Modelo de consultoría enfocado a concientizar la importancia de la ciberseguridad en Pymes.			MCIP01
Datos ficha	**Nombre**	**Cargo**	**Dependencia**	**Fecha (dd/mm/aaaa)**
Elaborado por:	Juan Sebastian Pardo	Lider técnico	Servcios	6/02/2023
Revisado por:	Norman Alberto Molina	Cordinador Servicios	Servicios	10/02/2023
Aprobado por	Edna Margarita Torres	Analista de riesgos	Servicios	15/02/2023
Registro Modificaciones	**Versión**	**Descripción**	**Autor**	**Fecha (dd/mm/aaaa)**
1	1.0	Primera Versión	Juan Sebastian Pardo Ramirez	6/02/2023

II. Diccionario EDT

Código paquete trabajo	Descripción Paquete trabajo	Descripción trabajo	Asignación de responsabilidades	Fechas programadas	Criterios Aceptación	Supuestos	Riesgos	Recursos asignados	Dependencias del paquete
1.1.1	Levantamiento de Información de los activos.	Investigación y entrevistas con directores y/o coordinadores de área de la empresa para la identificación de los posibles activos críticos de interés	Edna Torres, Norman Molina	06/02/2023 03/03/2023	Sebastian Pardo, Recibirá las hoja de vida de los activos con las descripción y campos completos necesarios para su inventario y clasificación en formato en linea de Microsoft Forms		Dejar por fuera de la matriz áreas y activos de importancia en la empresa	8H de Recurso humano, 8 horas de equipo ofimático	N/A
1.1.2	Registro y tabulado de datos del inventario de los activos.	Recolección de los datos de los activos presentes en las áreas criticas de la empresa en una matriz de activos	Sebastian Pardo, Norman Molina	06/03/2023 08/03/2023	Edna Torres: Revisara y validara la matriz entregada en formato de Excel		El formato no sea claro al momento de hacer la creación y queden puntos importantes por fuera	Equipo Ofimático y Software Ofimático, Recursos Humano 8 H	Actividades predecesoras: 1.1.1
1.1.3	Definición de criticidad de cada activo.	Ponderación de la criticidad de los activos según su importancia y área de negocio en la matriz de activos	Sebastian Pardo, Edna torres	09/03/2023 29/03/2023	Norman Molina: Deberá validar los datos suministrados y asegura que todos los activos cuenten con su nivel de criticada registros en al matriz		No se pueda establecer de manera clara o fácil el nivel de criticidad de los activos a falta de información de los mismos.	4H de recuso humano	Actividades predecesoras: 1.1.2
1.1.4	Recolección datos de responsables de cada activo	Se deberá definir el responsable de cada activo o grupo de activos y documentar su información de contacto y alcances en la matriz de	Sebastian Pardo, Norman Molina	30/03/2023 07/04/2023	Edna Torres: Valida la información de las personas responsables y la relación con los activos inventariados		Falta de información en las áreas o claridad de los responsables de los activos, que dificulten el levantamiento de la información	24H Recurso humano , 24H Equipo de computo	Actividades predecesoras: 1.1.3
1.2.1	Definición software de escaneo vulnerabilidades.	Desarrollo de comparativa de herramientas de escaneo y pruebas de las herramientas de escaneo documentadas	Edna Torres, Norman Molina	06/02/2023 08/02/2023	Norman Molina: Deberá validar resultados de las pruebas de las diferentes herramientas y ponderal los		No se encuentre una herramienta adecuada o el costo de la solución este fuera del presupuesto.	Ambientes de pruebas, Sofware de Escaneo de vulnerabilidades, 8H recurso Humano	N/A
1.2.2	Parametrización herramienta de escaneo de vulnerabilidades.	Se deberá configura los parámetros necesarios de la herramienta acorde a el enfoque del escaneo.	Sebastian Pardo, Norman Molina	09/02/2023 13/02/2023	Edna Torres: Deberá hace el analisis de y check de verificación de las configuración realizadas en la herramienta		No se cuente con los parámetros necesarios en la herramienta, no se cuente con suficiente información para parametrizar la herramienta	Casos de uso, Set de Pruebas, Recurso Humano 4H	Actividades predecesoras: 1.2.1
1.2.3	Ejecución de escaneo de Vulnerabilidades	Se deberá lanzar el proceso de escaneo sobre los activos objetivo obtenido un informde de vulnerabilidades	Sebastian Pardo	30/03/2023 19/04/2023	Norman Molina: Deberá validar que los activos escaneados responda en el escaneo y consola de la		Falta de permios para alcanzar los activos del Inventariados listasdos o que estos esten fuera de servcio o apagados	Inventario de Activos	Actividad predesesoras 1.1.3 y 1.2.2

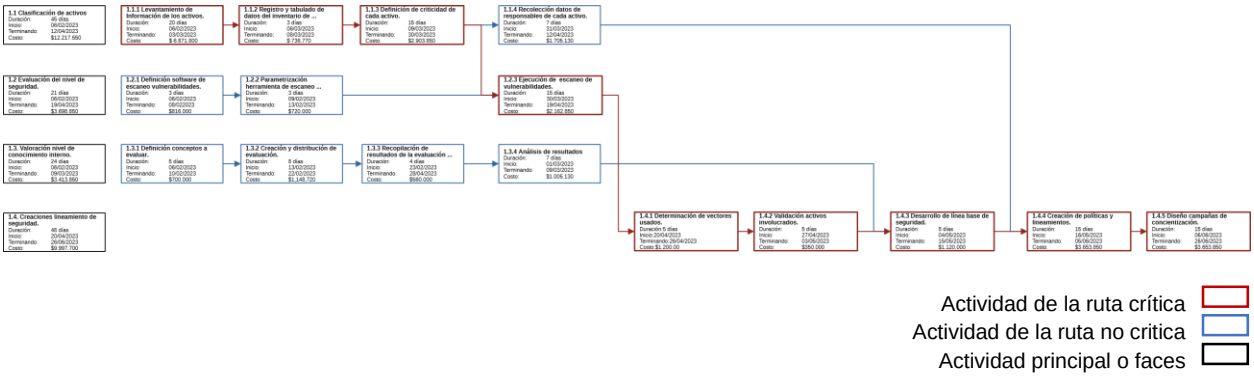
1.3.1	Definición conceptos a evaluar.	Se debe definir los conceptos a tratar en la evaluación y registrarlos en und documento de indice tematico.	Norman Molina, Sebastian Pardo	06/02/2023 10/02/2023	Norman Molina: Debera definir los conceptos principales para la cracion de la E.T		Falta de manejo del tema por parte de los responsabels de la evaluación	Base de datos de conceptos más de ciberseguridad, Software de Ofimatica, 4H de Recurso Humano	N/A
1.3.2	Creación y distribucion de evaluación.	Se crearа evaluación de conocimiento basada en documento de indice mestro en modo de encuesta en linea como	Edna Torres, Sebastian Pardo	13/02/2023 22/02/2023	Sebastian Pardo: Se validara que todos los temas del indice se encuentren incuidos en al encuensta o medio de evaluación.		Perdida de la informacion recopilada	Set de preguntas y ejercisios software de encuestas, 8H de recurso humano, equipode computo 8H	Actividades predesesoras: 1.3.1
1.3.3	Recolección y tabulación de resultados.	Se recompilación todos los resultados de la evaluación de conocimientos y se generara la tabulación de la información	Edna Torres	23/02/2023 28/02/2023	Edna Torres: Verificará la informacion recopilada despues que hayan presentado la E.T		Que se pierda información en todo el proceso de recopilación	Plantilla en Excel, 4H Recurso humano	Actividades predesesoras: 1.3.2
1.3.4	Análisis de resultados	Se generaran indicadores de los resultados según líneas y áreas de falencia de los colaboradores en un informe técnico de resultados	Sebastian Pardo, Norman Molina	01/03/2023 09/03/2023	Sebastián Pardo, Norman Molina: Se revisaran y detallaran los resultados en el informe de resultados tecnicos del documento final.			PC del proyecto, plantilla en software excel, 2H recurso humano	Actividades predesesoras: 1.3.3
1.4.1	Determinación de vectores de informacion usados.	Genera listado de posibles vectores ataques implicados	Norman Molina, Edna Torres	20/04/2023 26/04/2023	Sebastian Pardo: Validara que los todos lo vectores esten documentados		No se tenga encuenta todos los vectores asosiadoas a la linea de negocio	Software de ofimatica, Computador, 8H Recurso humano	Actividades predesesoras: 1.2.3
1.4.2	Validación activos involucrados.	Creacion de matriz de activos por vector de ataque	Edna Torres	27/04/2023 03/05/2023	Norman Molina: Verificando cruce de activos con vectores estimados		Activos no inventariados	Software de ofimatica, Computador, 8H Recurso humano	Actividades predesesoras: 1.4.1
1.4.3	Desarrollo de línea base de seguridad.	Creacion de lineamientos	Edna Torres	04/05/2023 15/05/2023	Edna Torres: Realizará en un documento la linea base de seguridad que se aplicará en la empresa determinada		Escape de información	Software de offimatica, Computador, 48H Recurso humano	Actividades predesesoras: 1.3.4 y 1.4.2
1.4.4	Creación de políticas y lineamientos.	Genera listado de politicas a implementar y por ende los lineamientos que deben seguir para evitar brechar de ciberseguridad en la empresa	Norman Molina, Juan Pardo R	16/05/2023 05/06/2023	Norman Molina: Recibira el documento con políticas y lineamientos definidos		Falta de información en base a los diferentes tipos de buenas prácticas en ciberseguridad	Software de ofimatica, Computador, 56H Recurso humano	Actividades predesesoras: 1.1.4 y 1.4.3
1.4.5	Diseño campañas de concientización.	Desarrollo campañas internas para la concientización de los colaboradores sobre los riesgo de ciberseguridad	Norman Molina, Juan Pardo R	06/06/2023 26/06/2023	Edna Torres: Revisara los documentos de las campañas de concientizacion y porpuestas de las mismas en en mdedio		Perdida de documentos o información base para el diseño de las campañas de concientización	Software de ofimática, Computador, 24H Recurso humano	Actividades predesesoras: 1.4.4

Ruta critica

La ruta crítica generada a partir del cronograma de actividades nos permitió establecer las actividades principales y priorizarlas para el desarrollo oportuno del proyecto, al igual que el tiempo máximo dedicado presupuestado de todas las fases.

Figura 4

Diagrama de la ruta crítica de las actividades.



Planeación

Cronograma

Para el desarrollo del proyecto se estima un total de 141 días desde su inicio el 02 de febrero del 2023 y finalizado el 26 de junio del 2023, además se cuenta con un tiempo total efectivo en las ejecuciones de las actividades de 101 días hábiles. Dicho cronograma se generó partir de la estructura de desglose de actividades de la anterior actividad (Figura 3).

Figura 5

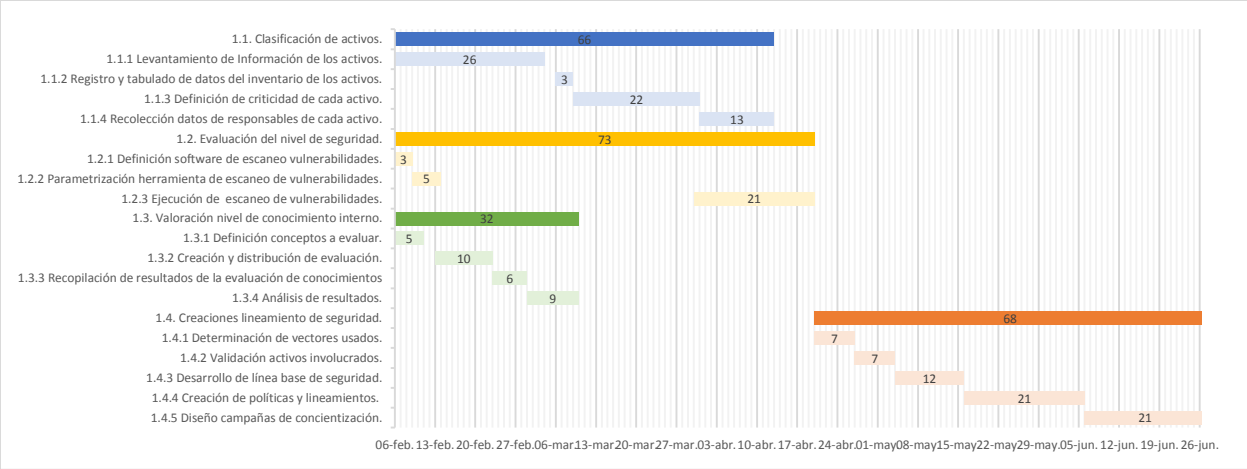
Cronograma de actividades basado en el diccionario EDT.

N	Nombre de la actividad o fase	Duración actividad (Días)	Tiempo Total (Días)	Fecha Inicio	Fecha Fin	Actividad Predecesora
1	**1. Modelo de consultoría enfocado a la importancia de la ciberseguridad e**	**101**	**141**	**6/02/2023**	**26/06/2023**	
2	**1.1. Clasificación de activos.**	**45**	**66**	**6/02/2023**	**12/04/2023**	
3	1.1.1 Levantamiento de Información de los activos.	20	26	6/02/2023	3/03/2023	
4	1.1.2 Registro y tabulado de datos del inventario de los activos.	3	3	6/03/2023	8/03/2023	3
5	1.1.3 Definición de criticidad de cada activo.	15	22	9/03/2023	30/03/2023	4
6	1.1.4 Recolección datos de responsables de cada activo.	7	13	31/03/2023	12/04/2023	5
7	**1.2. Evaluación del nivel de seguridad.**	**21**	**73**	**6/02/2023**	**19/04/2023**	
8	1.2.1 Definición software de escaneo vulnerabilidades.	3	3	6/02/2023	8/02/2023	
9	1.2.2 Parametrización herramienta de escaneo de vulnerabilidades.	3	5	9/02/2023	13/02/2023	8
10	1.2.3 Ejecución de escaneo de vulnerabilidades.	15	21	30/03/2023	19/04/2023	5, 9
11	**1.3. Valoración nivel de conocimiento interno.**	**24**	**32**	**6/02/2023**	**9/03/2023**	
12	1.3.1 Definición conceptos a evaluar.	5	5	6/02/2023	10/02/2023	
13	1.3.2 Creación y distribución de evaluación.	8	10	13/02/2023	22/02/2023	12
14	1.3.3 Recopilación de resultados de la evaluación de conocimientos	4	6	23/02/2023	28/02/2023	13
15	1.3.4 Análisis de resultados.	7	9	1/03/2023	9/03/2023	14
16	**1.4. Creaciones lineamiento de seguridad.**	**48**	**68**	**20/04/2023**	**26/06/2023**	
17	1.4.1 Determinación de vectores usados.	5	7	20/04/2023	26/04/2023	10
18	1.4.2 Validación activos involucrados.	5	7	27/04/2023	3/05/2023	17
19	1.4.3 Desarrollo de línea base de seguridad.	8	12	4/05/2023	15/05/2023	15, 18
20	1.4.4 Creación de políticas y lineamientos.	15	21	16/05/2023	5/06/2023	6, 19
21	1.4.5 Diseño campañas de concientización.	15	21	6/06/2023	26/06/2023	15, 20

A partir de del desarrollo de del cronograma de actividades se genera el respectivo diagrama de Gantt acorde los tiempos y fechas de estipulados en el cronograma.

Figura 6

Diagrama de Gantt de las actividades



Presupuesto

Para el costo presupuestado del proyecto se contemplaron los costos individuales de cada tarea y se diligenciar el documento de Excel de inversión y costos discriminando el valor de cada recuso asignado.

Figura 7

Documento de Inversión y costos de los paquetes de las tareas.

PRESUPUESTO

CORPORACIÓN UNIVERSITARIA UNITEC

Proyecto	Nombre			Sigla
	Diseño De Un Modelo De Consultoría Enfocado A La Importancia De La Ciberseguridad En Pymes.			*DMCECICP*
Datos ficha	**Nombre**	**Cargo**	**Dependencia**	**Fecha (dd/mm/aaaa)**
Elaborado por:	Norma A. Molina	Cordinador Servicios	Servicios	*2/20/2023*
Revisado por:	Sebastian Pardo	Lider tecnico	Servcios	*3/1/2023*
Aprobado por	Edna Torres	Analista de riesgos	Servcios	*3/2/2023*
Duracion	*101 dias*			

OBJETIVO DEL PROYECTO

Generar un modelo de consultoría y servicio especializada en ciberseguridad que brinde asesoría y acompañamiento a pequeñas y medianas empresas

ELEMENTOS QUE COMPONEN LOS COSTOS

ITEM	DESCRIPCIÓN PAQUETE ACTIVIDAD	RECURSOS ASIGNADOS	DIAS ACTIVIDAD	COSTO RECURSOS ASIGNADO
1.1.1	Levantamiento de Información de los activos. (documento excel)	Servicio de Internet	20	$ 200,000
		Alquiler de tres computadores	20	$ 600,000
		Pepeleria	20	$ 71,800
		Recurso humano (3 personas)8h	20	$ 6,000,000
		TOTAL		**$ 6,871,800**
1.1.2	Registro y tabulado de datos del inventario de los activos.	Servicio de Internet	3	$ 30,000
		Alquiler de tres computadores	3	$ 300,000
		Pepeleria	3	$ 10,770
		Sofware infomatico	3	$ 96,000
		Recurso humano (3 personas)8h	3	$ 300,000
		TOTAL		**$ 736,770**
1.1.3	Definición de criticidad de cada activo.	Servicio de Internet	15	$ 150,000
		Alquiler de tres computadores	15	$ 450,000
		Pepeleria	15	$ 53,850
		Recurso humano (3 personas) 4h	15	$ 2,250,000
		TOTAL		**$ 2,903,850**
1.1.4	Recolección datos de responsables de cada activo.	Servicio de Internet	7	$ 70,000
		Alquiler de tres computadores	7	$ 210,000
		Pepeleria	7	$ 25,130
		Recurso humano (2 personas)	7	$ 1,400,000
		TOTAL		**$ 1,705,130**
1.2.1	Definición software de escaneo vulnerabilidades.	Servicio de Internet	3	$ 30,000
		Alquiler de dos computadores	3	$ 90,000
		Sofware infomatico	3	$ 96,000
		Recurso humano (2 personas)	3	$ 600,000
		TOTAL		**$ 816,000**
1.2.2	Parametrización herramienta de escaneo de vulnerabilidades.	Servicio de Internet	3	$ 30,000
		Alquiler de un computador	3	$ 90,000
		Recurso humano (2 persona)	3	$ 600,000
		TOTAL		**$ 720,000**
1.2.3	Ejecución de escaneo de Vulnerabilidades	Servicio de Internet	15	$ 150,000
		Licencia Paquete Office	15	$ 9,000
		Papeleria	15	$ 53,850
		Alquiler de un computador	15	$ 450,000
		Recurso humano (1 persona)	15	$ 1,500,000
		TOTAL		**$ 2,162,850**
1.3.1	Definición conceptos a evaluar.	Servicio de Internet	5	$ 50,000
		Alquiler de un computador	5	$ 150,000
		Recurso humano (2 personas)	5	$ 500,000
		TOTAL		**$ 700,000**
1.3.2	Creación y distribución de evaluación.	Servicio de Internet	8	$ 80,000
		Alquiler de un computador	8	$ 240,000
		Pepeleria	8	$ 28,720
		Recurso humano (1 persona)	8	$ 800,000
		TOTAL		**$ 1,148,720**
1.3.3	Recopilación de resultados de evaluación de conocimientos	Recurso humano (1 persona)	4	$ 400,000
		Alquiler de un computador	4	$ 120,000
		Servicio de Internet	4	$ 40,000
		TOTAL		**$ 560,000**
1.3.4	Análisis de resultados	Recurso humano (1 persona)	7	$ 700,000
		Pepeleria	7	$ 25,130
		Alquiler de un computador	7	$ 210,000
		Servicio de Internet	7	$ 70,000
		TOTAL		**$ 1,005,130**

1.4.1	Determinación de vectores de informacion usados.	Servicio de Internet	5	$ 50,000
		Alquiler de dos computadores	5	$ 150,000
		Recurso humano (2 personas)	5	$ 1,000,000
		TOTAL		**$ 1,200,000**
1.4.2	Validación activos involucrados.	Servicio de Internet	5	$ 50,000
		Alquiler de un computador	5	$ 150,000
		Recurso humano (1 persona)	5	$ 150,000
		TOTAL		**$ 350,000**
1.4.3	Desarrollo de línea base de seguridad.	Servicio de Internet	8	$ 80,000
		Alquiler de un computador	8	$ 240,000
		Recurso humano (1 persona)	8	$ 800,000
		TOTAL		**$ 1,120,000**
1.4.4	Creación de políticas y lineamientos.	Servicio de Internet	15	$ 150,000
		Papeleria	15	$ 53,850
		Alquiler de dos computadores	15	$ 450,000
		Recurso humano (2 personas)	15	$ 3,000,000
		TOTAL		**$ 3,653,850**
1.4.5	Diseño campañas de concientización.	Servicio de Internet	15	$ 150,000
		Papeleria	15	$ 53,850
		Alquiler de dos computadores	15	$ 450,000
		Recurso humano (2 personas)	15	$ 3,000,000
		TOTAL		**$ 3,653,850**
COSTO NETO DEL PROYECTO				$ 29,307,950
IMPREVISTOS (10%)				$ 2,930,795
COSTO TOTAL				**$ 32,238,745**

Ejecución

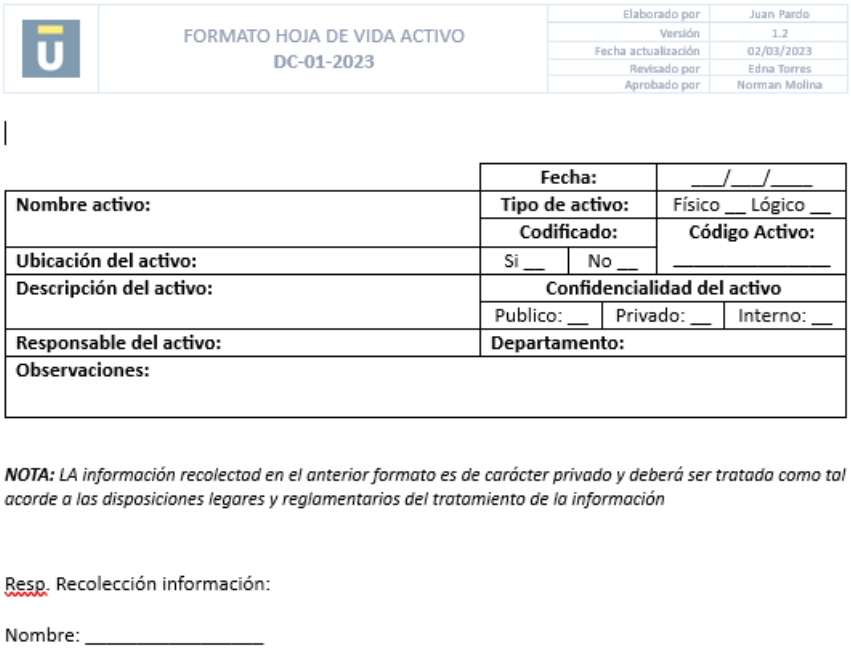
Durante la ejecución del proyecto se llevan a cabo las actividades según tiempos y orden establecidos en el cronograma y ruta crítica, siendo están las descritas a continuación.

Evidencia Actividades

1.1.1 Levantamiento de Información de los activos (Formato Word). Se realiza la recolección de información de todos los activos de la empresa a través del formato que se observa en la Figura 5, el cual se diligencia personalmente en cada área y en la compañía del responsable de cada activo.

Figura 8

Formato de recolecciones de información de los activos.



FORMATO HOJA DE VIDA ACTIVO
DC-01-2023

Elaborado por	Juan Pardo
Versión	1.2
Fecha actualización	02/03/2023
Revisado por	Edna Torres
Aprobado por	Norman Molina

	Fecha:		___/___/____
Nombre activo:	**Tipo de activo:**		Físico __ Lógico __
	Codificado:		**Código Activo:**
Ubicación del activo:	Si __	No __	_____
Descripción del activo:	**Confidencialidad del activo**		
	Publico: __	Privado: __	Interno: __
Responsable del activo:	**Departamento:**		
Observaciones:			

NOTA: *LA información recolectad en el anterior formato es de carácter privado y deberá ser tratada como tal acorde a las disposiciones legares y reglamentarios del tratamiento de la información*

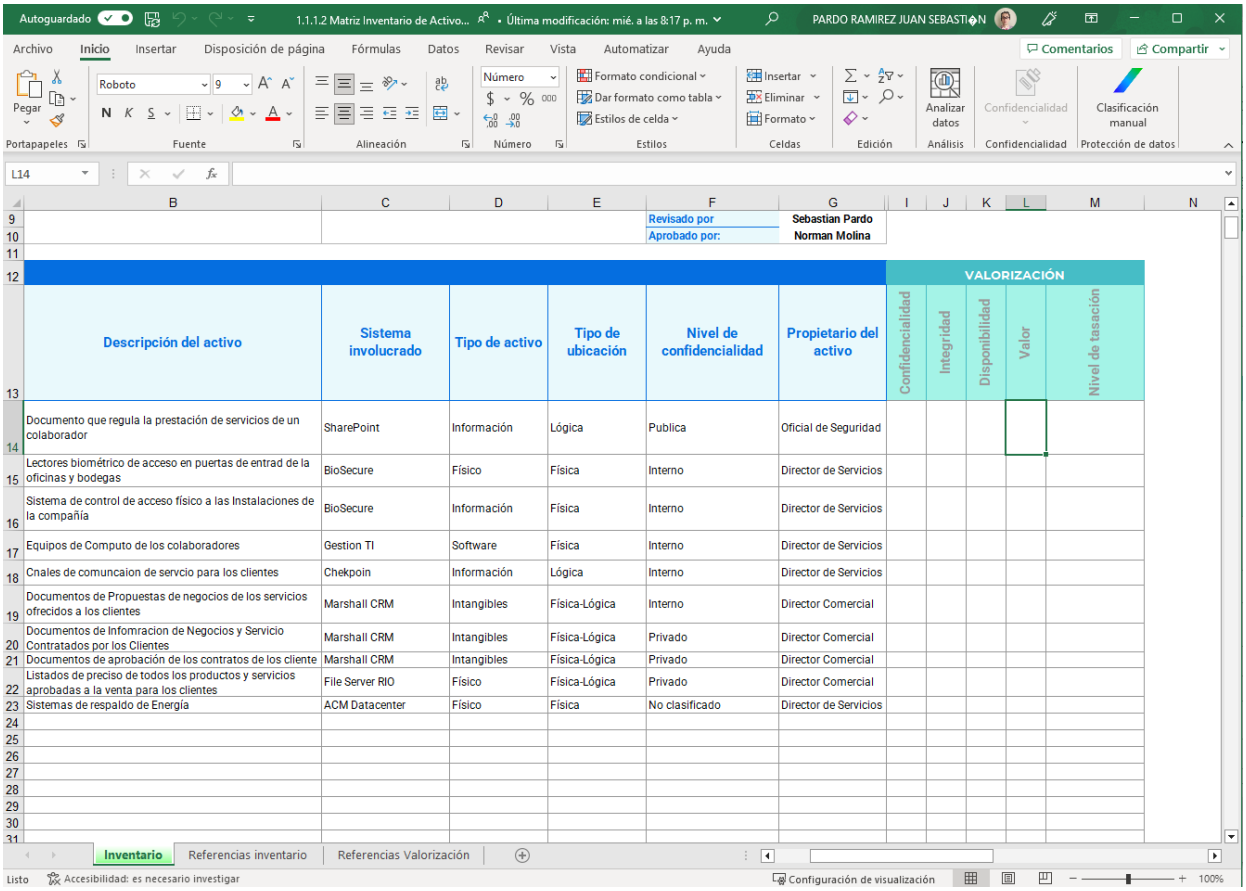
Resp. Recolección información:

Nombre: _____

1.1.2 Matriz Inventario de Activos - (Inventario). Una vez recolectada toda la información correspondiente a los activos a inventariar se procederá a tabular en a la matriz de activos la información de estos.

Figura 9

Matriz de activos de la entidad diligenciada con información de los activos.



	B	C	D	E	F	G	I	J	K	L	M	N
9					Revisado por	Sebastian Pardo						
10					Aprobado por:	Norman Molina						
11												
12							VALORIZACIÓN					
13	Descripción del activo	Sistema involucrado	Tipo de activo	Tipo de ubicación	Nivel de confidencialidad	Propietario del activo	Confidencialidad	Integridad	Disponibilidad	Valor	Nivel de tasación	
14	Documento que regula la prestación de servicios de un colaborador	SharePoint	Información	Lógica	Publica	Oficial de Seguridad						
15	Lectores biométrico de acceso en puertas de entrad de la oficinas y bodegas	BioSecure	Físico	Física	Interno	Director de Servicios						
16	Sistema de control de acceso físico a las Instalaciones de la compañía	BioSecure	Información	Física	Interno	Director de Servicios						
17	Equipos de Computo de los colaboradores	Gestion TI	Software	Física	Interno	Director de Servicios						
18	Cnales de comuncaion de servcio para los clientes	Chekpoin	Información	Lógica	Interno	Director de Servicios						
19	Documentos de Propuestas de negocios de los servicios ofrecidos a los clientes	Marshall CRM	Intangibles	Física-Lógica	Interno	Director Comercial						
20	Documentos de Infomracion de Negocios y Servicio Contratados por los Clientes	Marshall CRM	Intangibles	Física-Lógica	Privado	Director Comercial						
21	Documentos de aprobación de los contratos de los cliente	Marshall CRM	Intangibles	Física-Lógica	Privado	Director Comercial						
22	Listados de preciso de todos los productos y servicios aprobadas a la venta para los clientes	File Server RIO	Físico	Física-Lógica	Privado	Director Comercial						
23	Sistemas de respaldo de Energía	ACM Datacenter	Físico	Física	No clasificado	Director de Servicios						
24												
25												
26												
27												
28												
29												
30												
31												

Nota. Tomado y adaptado de "*Creando un inventario de activos en 4 sencillos pasos",* Adriel Araujo, 2021, Hackmetrix (https://blog.hackmetrix.com/inventario-de-activos-seguridad-de-la-informacion/).

1.1.3 Matriz Inventario de Activos - (Definición Criticidad). La definiendo criticidad se define en base a valores enteros de 1 a 5 teniendo en cuenta los factores de integridad, disponibilidad y confidencialidad del activo.

Tabla 2

Definición de los valores de ponderación de niveles según factor de análisis.

VALOR	CONFIDENCIALIDAD
5 (Muy Alto)	La información asociada al activo es solo accedida por el personal de alto rango, pues su divulgación afectaría irreversiblemente a la organización.
4 (Alto)	La información asociada al activo es restringida y solo personal de un proyecto específico puede acceder a ella, pues su divulgación afectaría gravemente a la organización.
3 (Medio)	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la organización.
2 (Bajo)	La información asociada al activo es de uso interno y solo personal de ABC puede acceder a ella, pues su divulgación afectaría parcialmente a la organización.
1 (Muy Bajo)	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la organización.
VALOR	**INTEGRIDAD**
5 (Muy Alto)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 0%, pues la vulneración de su integridad afectaría irreversiblemente a la organización.
4 (Alto)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 15%, pues la vulneración de su integridad afectaría gravemente a la organización.
3 (Medio)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 50%, pues la vulneración de su integridad afectaría considerablemente a la organización.
2 (Bajo)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 85%, pues la vulneración de su integridad afectaría parcialmente a la organización.
1 (Muy Bajo)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 100%, pues la vulneración de su integridad no impacta a la organización.
VALOR	**DISPONIBILIDAD**
5 (Muy Alto)	Se requiere que el activo nunca se encuentre indisponible, pues su carencia afectaría irreversiblemente a la organización.
4 (Alto)	Se considera que como máximo el activo puede estar indisponible por una hora, pues su carencia afectaría gravemente a la organización.
3 (Medio)	Se considera que como máximo el activo puede estar indisponible por un día, pues su carencia afectaría considerablemente a la organización.
2 (Bajo)	Se considera que como máximo el activo puede estar indisponible por una semana, pues su carencia afectaría parcialmente a la organización.
1 (Muy Bajo)	Se considera que como máximo el activo puede estar indisponible por tiempo indefinido, pues su carencia no impacta a la organización.

Nota. Tomado y adaptado de "*Creando un inventario de activos en 4 sencillos pasos",* Adriel Araujo, 2021, Hackmetrix (https://blog.hackmetrix.com/inventario-de-activos-seguridad-de-la-informacion/).

Dada la anterior definición de ponderación de los tres factores para tener en cuenta en la determinación del nivel de criticada del activo se completa la matriz de activos con el cruce de datos resultantes acorde a la tabla 2 como se evidencia en la figura 8.

Tabla 3

Valoración para nivel de criticidad de los activos

Valor del Activo	Nivel de Criticidad	Color
4.001 – 5.000	Muy Alto	Rojo
3.001 – 4.000	Alto	Naranja
2.001 – 3.000	Medio	Amarillo
1.001 – 2.000	Bajo	Verde
0.000 – 1.000	Muy Bajo	Azul

Nota. Tomado y adaptado de Creando un inventario de activos en 4 sencillo, Adriel Araujo pasos, 2021, Hackmetrix (https://blog.hackmetrix.com/inventario-de-activos-seguridad-de-la-informacion/).

Figura 10

Matriz de Activos diligenciada con los datos de Valorización y Criticidad.

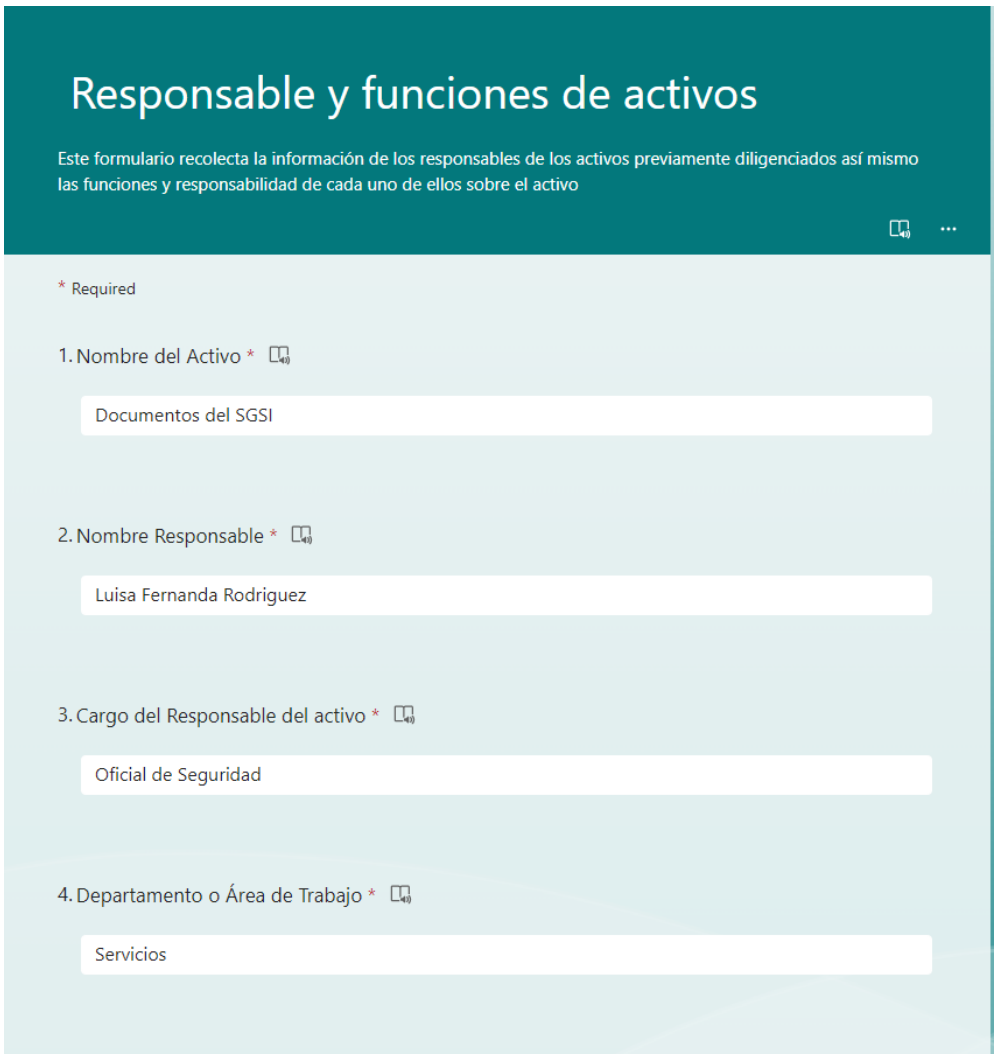
	DC-10-021A	INVENTARIO DE ACTIVOS	Versión:	1.0
			Fecha última actualización:	2/11/2023
			Revisado por	Sebastian Pardo
			Aprobado por:	Norman Molina

INVENTARIO							VALORIZACIÓN				
Nombre de activo	Descripción del activo	Sistema involucrado	Tipo de activo	Tipo de ubicación	Nivel de confidencialidad	Propietario del activo	Confidencialidad	Integridad	Disponibilidad	Valor	Nivel de Criticidad
Documentos del SGSI	Documento que regula la prestación de servicios de un colaborador	SharePoint	Información	Lógica	Publica	Oficial de Seguridad	4	3	2	3.00	Medio
Lectores de Acceso Biometrico	Lectores biométrico de acceso en puertas de entrad de la oficinas y bodegas	BioSecure	Físico	Física	Interno	Director de Servicios	5	1	1	2.33	Medio
Sistema Biométrico	Sistema de control de acceso físico a las Instalaciones de la compañía	BioSecure	Información	Física	Interno	Director de Servicios	1	3	3	2.33	Medio
Estaciones de trabajo	Equipos de Computo de los colaboradores	Gestion TI	Software	Física	Interno	Director de Servicios	2	4	5	3.67	Alto
Canales de VPNs con clientes	Cnales de comuncaion de servcio para los clientes	Chekpoin	Información	Lógica	Interno	Director de Servicios	2	4	5	3.67	Alto
Propuestas Comerciales	Documentos de Propuestas de negocios de los servicios ofrecidos a los clientes	Marshall CRM	Intangibles	Física-Lógica	Interno	Director Comercial	1	2	1	1.33	Bajo
Aprobaciones de Negocio	Documentos de Infomracion de Negocios y Servicio Contratados por los Clientes	Marshall CRM	Intangibles	Física-Lógica	Privado	Director Comercial	5	5	3	4.33	Muy Alto
Aprobaciones de Servicios	Documentos de aprobación de los contratos de los cliente	Marshall CRM	Intangibles	Física-Lógica	Privado	Director Comercial	2	3	3	2.67	Medio
Listas de precios	Listados de preciso de todos los productos y servicios aprobadas a la venta para los clientes	File Server RIO	Físico	Física-Lógica	Privado	Director Comercial	2	1	5	2.67	Medio
UPS	Sistemas de respaldo de Energía	ACM Datacenter	Físico	Física	No clasificado	Director de Servicios	3	4	4	3.67	Alto

1.1.4 Recolección datos de responsables de cada activo. Para la recolección de los datos de los responsables de cada activo se realiza mediante formularios en línea en plataforma de Microsoft Forms.

Figura 11

Formulario de recolecciones datos



Nota. URL de acceso a formulario Forms (https://forms.office.com/r/8zR1467Zxn)

1.2.1 Definición software de escaneo vulnerabilidades. Para la definición de la solución de escaneo a usar se realiza una tabla comparativa de dos softwares diferentes comparando sus capacidades y características.

Tabla 4

Tabla comparativa de las soluciones de escaneo seleccionadas

Característica	Open VAS	Nessus
Precio	Gratuito	$2,700/año
Software Libre	Si	No
Cobertura de CVE	26000	47000
Plataforma	Multi OS	Multi OS
Etiquetado de activos	Si	No
Administración de Políticas	No	Si
Descubrimiento de activos	No	Si
Fragmentación de activos	Si	No
Escaneo en Red	Si	Si
Gestión de Parches de seguridad	No	No
Priorización	Si	Si
gestión de Riesgo	Si	No
Evaluación de Vulnerabilidad	Si	Si

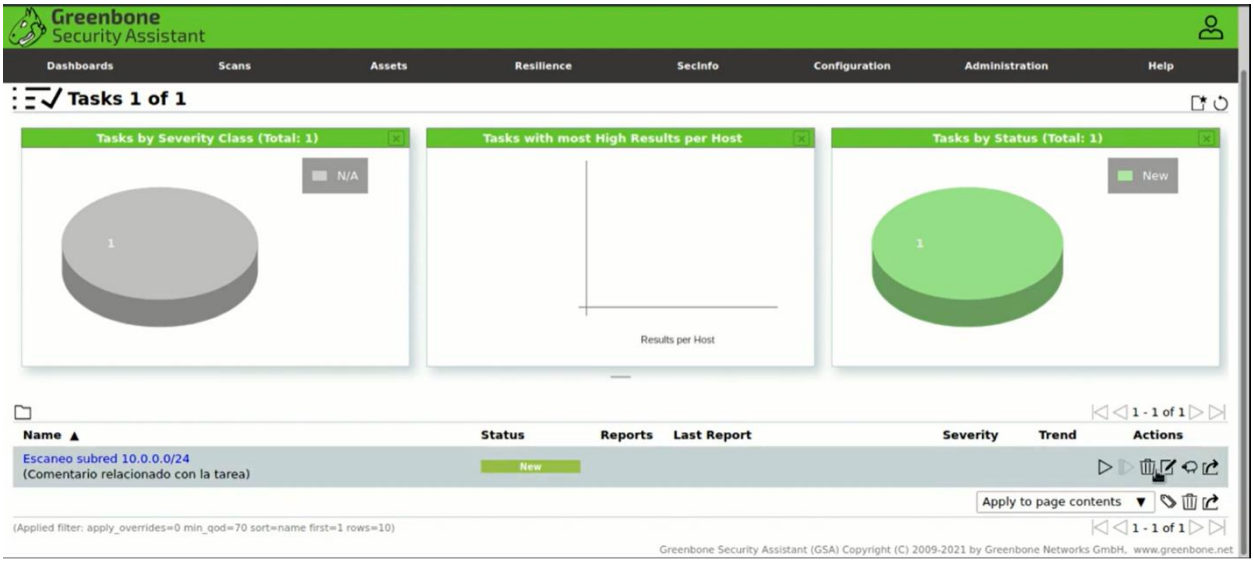
Escaneo web	Si	Si
Soporte	Foro comunitario para comunicación activa y un equipo de respuesta de seguridad separado para errores	Soporte técnico las 24 horas, los 7 días de la semana a través de una variedad de opciones como chat, comunidad y por teléfono.
Funciones principales	Interfaz web, escaneo de vulnerabilidades, descubrimiento de activos, gestión de riesgos, gestión de políticas, etiquetado de activos	Perfilado de activos, auditoría de seguridad, análisis de vulnerabilidades, recuperación de datos confidenciales
Característica destacable	La configuración del proceso de escaneo es fácil de usar y altamente configurable	Administración de configuración de documento e informes.

De la anterior comparación se opta por seleccionar como software de Escaneo OpenVAS dado el alcance de del proyecto y las limitaciones presupuesto existentes se hace esta la más viable.

1.2.2 Parametrización herramienta de escaneo de vulnerabilidades. Se realiza configuración de la herramienta de escaño para la ejecución de escaño de forma programada sobre el segmento de red 10.0.0.0/24 en donde se encuentra todos los activos a escanear definidos previamente.

Figura 12

Consola de configuración de escaneos OpenVAS

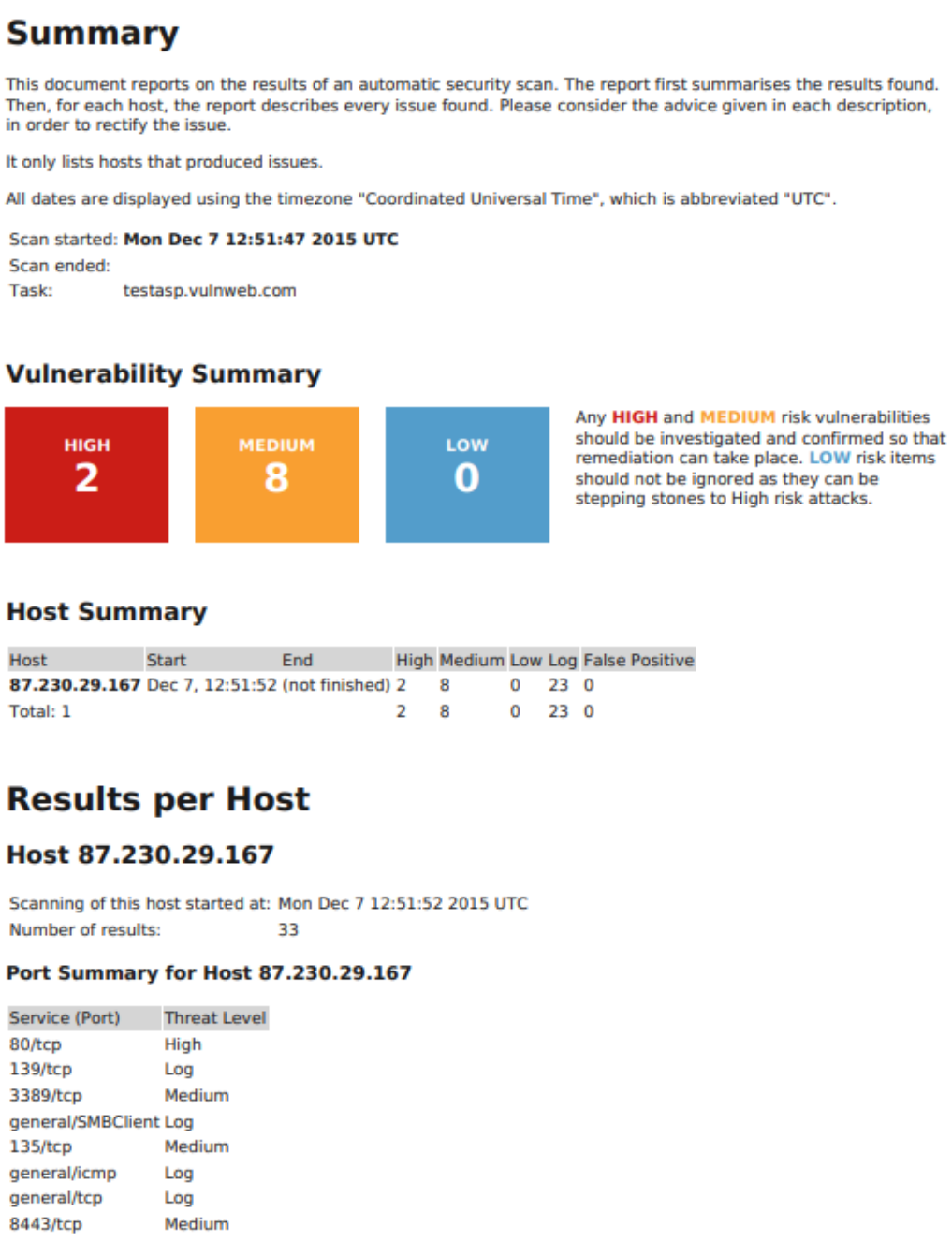


Nota. Configuración realizada en con base a la guía y documentación del fabricante Greenbone (https://greenbone.github.io/docs/latest/index.html)

1.2.3. Ejecución de escaneo de vulnerabilidades. Una vez configurado la tarea de escaneo de vulnerabilidad se procede a ejecutarse sobre los activos seleccionados y al final de este nos la herramienta nos entrega el informe correspondiente del escaneo en formato pdf.

Figura 13

Página de resumen del reporte de escaneo de vulnerabilidad generado.



Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

It only lists hosts that produced issues.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started: **Mon Dec 7 12:51:47 2015 UTC**
Scan ended:
Task: testasp.vulnweb.com

Vulnerability Summary

HIGH 2 | MEDIUM 8 | LOW 0

Any **HIGH** and **MEDIUM** risk vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be stepping stones to High risk attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
87.230.29.167	Dec 7, 12:51:52	(not finished)	2	8	0	23	0
Total: 1			2	8	0	23	0

Results per Host

Host 87.230.29.167

Scanning of this host started at: Mon Dec 7 12:51:52 2015 UTC
Number of results: 33

Port Summary for Host 87.230.29.167

Service (Port)	Threat Level
80/tcp	High
139/tcp	Log
3389/tcp	Medium
general/SMBClient	Log
135/tcp	Medium
general/icmp	Log
general/tcp	Log
8443/tcp	Medium

1.3.1 Definición conceptos a evaluar. Para la evaluación de conceptos interna dirigida a los colaboradores se define los siguientes temas de conocimiento para el desarrollo de la encuesta de conocimiento.

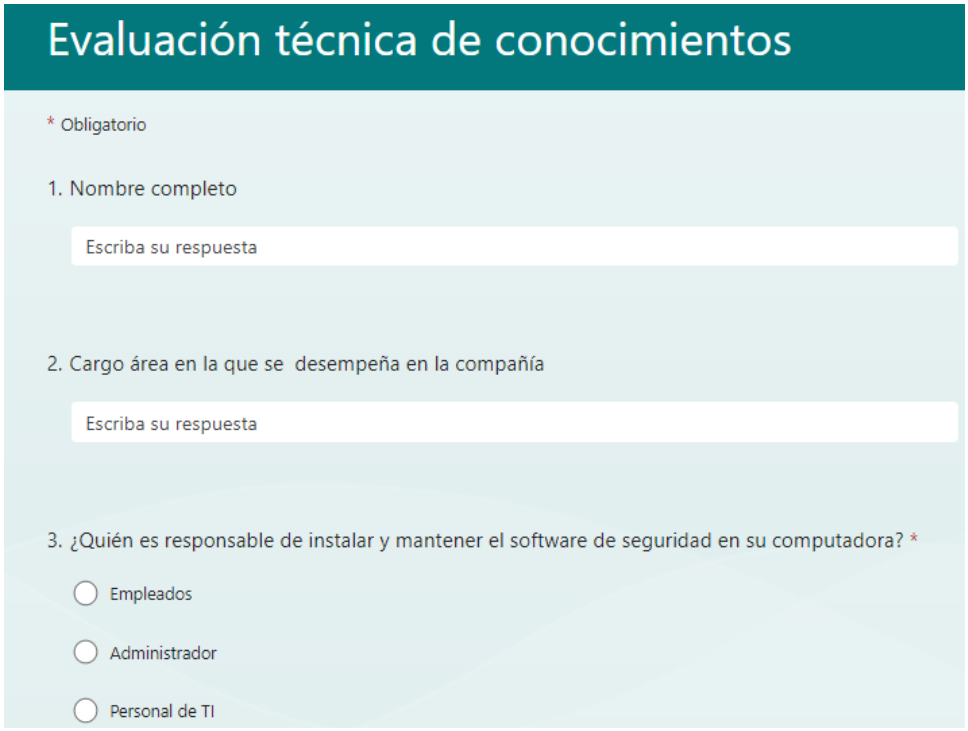
- Software
- Seguridad
- Navegadores Web
- Antivirus
- Monitoreo de PC
- Actualización de Antivirus
- Llevar el propio dispositivo suele ser...
- Contraseña segura
- Malware
- Responsable TI
- Ordenador
- VPN
- Ciberseguridad

1.3.2 Creación y distribución de evaluación

Diseño y planteamiento de las preguntas técnicas realizadas a cada uno de los colaboradores

Figura 14

Formato de evaluación de conocimientos.



Nota. URL de acceso a formulario Forms [Microsoft Forms]

Preguntas realizadas a los colaboradores:

1. ¿Quién es responsable de instalar y mantener el software de seguridad en su computadora?
2. ¿Qué navegador web utilizas normalmente?
3. ¿Tiene software antivirus instalado en su computadora?
4. ¿Qué software antivirus utilizas?
5. ¿La administración está monitoreando tu computadora todo el tiempo?
6. ¿Con qué frecuencia actualizas un software antivirus?
7. Complete la frase: "Llevar el propio dispositivo suele ser..."
8. ¿Cuál cree usted que es la contraseña más segura?

9. El servicio externo de gestión de recursos humanos de su empresa sufre una filtración de datos cuando un nuevo empleado descarga malware por accidente. Como resultado, se roba información de su empresa. ¿Quién es el responsable? Seleccione la opción que corresponda.
10. Un mensaje emergente le dice que hay disponible una nueva actualización para una aplicación de confianza que descargó y que sirve para comprobar la gramática. Seleccione la afirmación que crea correcta
11. Verdadero o falso: Un ordenador no puede sufrir una infección o un ataque en línea si el usuario tiene una VPN activa
12. Seleccione la afirmación que considere más precisa.
13. ¿Se ha nombrado un responsable de ciberseguridad en su empresa?
14. ¿Su empresa habla de ciberseguridad con sus clientes y proveedores?

1.3.3 Recopilación de resultados de evaluación de conocimientos. Recolección de prueba técnica para posteriormente realizar el análisis correspondiente para determinar nivel de conocimiento de cada uno de los colaboradores.

Figura 15

Tabla de resultado de encuesta realizadas

8 Respuestas

ID ↑	Nombre	Respuestas
1	anonymous	Leidy Bolivar
2	anonymous	Vanessa Florez
3	anonymous	Laura Rodriguez
4	anonymous	Jaime Carlos González
5	anonymous	Camila Gómez
6	anonymous	Andrés rincón Rodríguez
7	anonymous	Luisa Cardenas
8	anonymous	Camilo Andrés Molano

Figura 16

Detalle de las respuestas recolectadas en las encuestas de la evaluación

3. ¿Quién es responsable de instalar y mantener el software de seguridad en su computadora? (0 punto)

Más detalles

Empleados	1
Administrador	4
Personal de TI	3

4. ¿Qué navegador web utilizas normalmente? (0 punto)

Más detalles

Mozilla	1
Internet Explorer	1
Google Chrom	6
Opera	0

5. ¿Tiene software antivirus instalado en su computadora? (0 punto)

Más detalles

Si	4
No	0
No se	4

6. ¿Qué software antivirus utilizas? (0 punto)

Más detalles

McAfee	2
Avast	2
Avira	0
Microsoft	0
No se	4

7. ¿La administración está monitoreando tu computadora todo el tiempo? (0 punto)

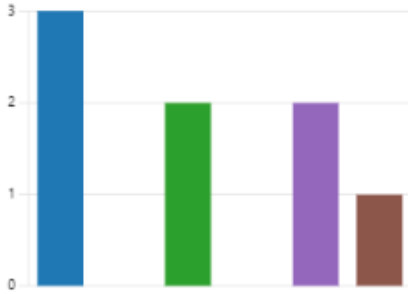
Más detalles

Si	0
No	4
No se	4

8. ¿Con qué frecuencia actualizas un software antivirus? (0 punto)

Más detalles

Se realiza automaticamente	3
2 veces por semana	0
De vez en cuando	2
Siempre	0
No se	2
Nunca	1



9. Complete la frase: "Llevar el propio dispositivo suele ser..." (0 punto)

Más detalles

Más arriesgado que usar los qu...	3
Igual de arriesgado que usar los...	3
Menos arriesgado que usar los ...	2

10. ¿Cual cree usted que es la contraseña más segura? (0 punto)

Más detalles

123456	2
Abril67.*	4
1q2w3e4r	2
dragon	0

11. Un mensaje emergente le dice que hay disponible una nueva actualización para una aplicación de confianza que descargó y que sirve para comprobar la gramática. Seleccione la afirmación que crea correcta

Más detalles

- Si no hago clic, se actualizará ig... 2
- Solo actualizo cuando el depart... 4
- Las actualizaciones deben aplica... 1
- Es mejor no aplicar la actualizaci... 1

12. El servicio externo de gestión de recursos humanos de su empresa sufre una filtración de datos cuando un nuevo empleado descarga malware por accidente. Como resultado, se roba información de su empresa. ¿Quién es el responsable? Seleccione la opción que corresponda.

Más detalles

- Su empresa 1
- El servicio externo de gestión de... 0
- El empleado que hizo clic en el ... 3
- El personal cuyos datos fueron r... 4

13. Verdadero o falso: Un ordenador no puede sufrir una infección o un ataque en línea si el usuario tiene una VPN activa

Más detalles

- Verdadero 6
- Falso 2

14. Seleccione la afirmación que considere más precisa. (0 punto)

Más detalles

- Todo el personal debería tener f... 3
- Empleados determinados (por e... 4
- Si una empresa cuenta con un s... 1

Nota. URL de acceso a formulario Forms [Microsoft Forms]

1.3.4 Análisis de resultados. Logramos identificar que no tiene claridad de quien es la persona encargada de realizar actualizaciones o instalación de software en los computadores, adicional el navegador que más utilizan es Google Chrome, la mitad de las personas encuestada no tienen conocimiento si el pc cuenta con antivirus, tampoco esa misma mitad sabe que software de antivirus utiliza la compañía para proteger su información, se detecta que no tienen conocimiento si están siendo monitoreados por ende abren sin ningún problema cualquier página, validamos y se evidencio en historial de los pc que YouTube, Facebook, WhatsApp web, juegos en línea, son las páginas que más son frecuentas en las instalaciones de la compañía, un pequeño porcentaje indica que la actualización se realiza automáticamente, el resto no sabe o de vez en cuando, es algo preocupante porque es evidente que al no realizar estas actualizaciones la información de la empresa se encuentra más vulnerable a cualquier tipo de ataque cibernético, con respecto al tipo de contraseña que utilizarían, escogen la más acertada y segura, la prueba en general demuestra poco conocimiento en ciberseguridad y es

un problema que se debe remediar ya o sino seguirán expuesto en la red a que sea hackeados de una manera más agresiva, generando perdida de información importante, datos de cliente, dinero (transacciones) entre otros.

Control y Evaluación

Durante el proceso de ejecución se llevarán a cabo todas las actividades descritas en el cronograma a la fecha del 24 de abril del 2023 fecha de entrega del presente documento, a continuación, se describe dichas activad en comparación entre los tiempo y costos planeados y los realmente ejecutados para cada actividad.

Planeación vs Ejecución (Tiempos)

Tabla 5

Tabla de comparativa de tiempo ejecutado vs tiempo estimado.

Índice	Actividad	Planeado	Ejecución	Dif.	Análisis
1.1.1	Levantamiento de Información de los activos.	20 días	22 días	+2	No se puedo obtener toda información de las áreas propietarias de los activos a tiempo.
1.1.2	Registro y tabulado de datos del inventario de los activos.	3 días	2 días	-1	El registro de los activos iniciales fue menor al estimado
1.1.3	Definición de criticidad de cada activo.	15 días	18 días	+3	Debido a que algunos activos tenían más información de la estimada fue más complejo la validación de algunos activos.
1.1.4	Recolección datos de responsables de cada activo.	7 días	10 días	3	Dado la dificultad de acceso a las diferentes áreas no se logró ubicar todos los responsables en el tiempo previsto
1.2.1	Definición software de escaneo vulnerabilidades.	3 días	3 días	0	El tiempo que se previsto para la actividad fue el justo

1.2.2	Parametrización herramienta de escaneo de vulnerabilidades.	3 días	3 días	0	El tiempo que se previsto para la actividad fue el justo
1.2.3	Ejecución de escaneo de vulnerabilidades.	15 días	22 días	+7	Por restricciones de acceso a varios de los activos se debió solicitar permisos adicionales que generaron retrasos en la ejecución.
1.3.1	Definición conceptos a evaluar.	5 días	4 días	-1	Se logro reducir la cantidad de conceptos a evaluar de total considerado.
1.3.2	Creación y distribución de evaluación.	8 días	7 días	-1	Dado que ya existían una base da datos de los colaboradores, la distribución de la evaluación fue más eficiente.
1.3.3	Recopilación de resultados de evaluación de conocimientos	4 días	4 días	0	El tiempo estimado de la activad fue el justo a la actividad
1.3.4	Análisis de resultados	7 días	10 días	+3	Se tuvo dificultades de recursos humano para el análisis de los datos recopilados.
1.4.1	Determinación de vectores usados.	5 días	5 días	0	El tiempo que se previsto para la actividad fue el justo
1.4.2	Validación activos involucrados.	5 días	5 días	0	El tiempo que se previsto para la actividad fue el justo

Planeación vs Ejecución (Costo)

Tabla 6

Tabla de comparativa de costo de actividad ejecutada vs el costo estimado.

Índice	Actividad	Planeado	Ejecutado	Diferencia	Análisis
1.1.1	Levantamiento de Información de los activos.	$ 2.405.130	$ 2.645.643	$ 240.513	Se designo dos días adicional de recurso humano para la actividad.
1.1.2	Registro y tabulado de datos del inventario de los activos.	$ 736.770	$ 491.180	-$ 245.590	Se recupera sobre costo de la actividad anterior con la ganancia de esta activad.

1.1.3	Definición de criticidad de cada activo.	$ 174.360	$ 209.232	$ 34.872	El desface del costo está dentro del rango de imprevistos.
1.1.4	Recolección datos de responsables de cada activo.	$ 1.217.950	$ 1.739.929	$ 521.979	Se requirió asignar más días de trabajo de recurso humano.
1.2.1	Definición software de escaneo vulnerabilidades.	$ 544.000	$ 544.000	$ 0	No se generó sobre costo de la actividad
1.2.2	Parametrización herramienta de escaneo de vulnerabilidades.	$ 720.000	$ 720.000	$ 0	No se generó sobre costo de la actividad
1.2.3	Ejecución de escaneo de vulnerabilidades.	$ 703.000	$ 1.031.067	$ 328.067	Se dispuso un recurso adicional por 7 días.
1.3.1	Definición conceptos a evaluar.	$ 700.000	$ 560.000	-$ 140.000	Se ahorro un día de trabajo en a la actividad
1.3.2	Creación y distribución de evaluación.	$ 574.360	$ 502.565	-$ 71.795	Hubo un sobre costo la activad en la planeación
1.3.3	Recopilación de resultados de evaluación de conocimientos	$ 560.000	$ 560.000	$ 0	No se generó sobre costo de la actividad
1.3.4	Análisis de resultados	$ 574.360	$ 820.514	$ 246.154	Se pagaron horas extras para agilizar proceso de análisis
1.4.1	Determinación de vectores usados.	$ 1.200.00	$ 950.000	-$ 250.000	NO se realizó un proceso de análisis por solitud falta de información
1.4.2	Validación activos involucrados.	$ 350.000	$ 440.000	$ 90.000	Se generaron gastos adicionales en la compra de papelería faltante

Cierre

Acorde a los diferentes objetivos planteados inicialmente en el proyecto podemos concluir los siguientes indicadores del proceso ejecutada en cada una de sus fases:

Objetivo 1: Respecto al objetivo 1 "**Clasificación de activos"** Se logra completar de forma parcial el levantamiento de la información al 90%

Objetivo 2: Respecto al objetivo 2 "**Evaluación del nivel de seguridad**" Se ejecuto y cumplió de manera parcial, dado que durante el escaneo de los activos NO se cubrió la totalidad de los activos llegado solamente a un aproximado del 87%.

Objetivo 3: Para el objetivo 3 "**Valoración nivel de conocimiento interno**", Se lleva cabo las campañas de evaluaciones de forma a efectiva alcanzado y midiendo el conocimiento de más del 96% de la totalidad de los colaboradores encuestados acerca de la temática evaluada.

Objetivo 4: El objetivo 4 "**Creaciones lineamiento de seguridad.**" Se encuentra en ejecución dado que la fase a la fecha de entrega de este documento se encuentra al 39.71% de cumplimiento

Lecciones aprendidas:

- Se logró obtener la información necesaria del 90% de los activos dentro de los tiempos establecidos, el 10% faltante no se logra por la disponibilidad de las áreas encargas.
- Se evaluó el nivel de seguridad de la empresa a la que se le está realizando el estudio, encontrando los mayores riesgos de la información administradas por ellos.

- Se analiza el conocimiento que tienen los colaboradores en la empresa con respecto a ciberseguridad y se concluye que no cuentan con bases suficientes para saber proceder en un momento de vulnerabilidad.

Se presentan varios desfaces tanto en costos (algunos a favor) como en tiempo durante la ejecución que son difíciles de prever cuando algunas actividades dependen de terceros. Aunque en costos se estimó una reserva del 10% sobre el presupuesto inicial el cual ha sido suficiente. En cuanto a tiempos los retrasos de alguna actividad en algunos casos generan un retraso secuencial en las tareas subsecuentes.

Futuros Proyectos:

A partir de este proyecto de modelo de consultoría es posible crear otros proyectos de asesoría en área de ciberseguridad y la telecomunicación con un enfoque de servicio. Formalizando una empresa que presente servicios de consultoría, soporte, administración en enfocada en las áreas mencionadas.

Este proyecto también sierve como base a futuras investigación y/o comparaciones de modelos de asesorías y consultorías relacionadas con la temática plateada, pudiendo ser un buen punto de partida para el desarrollo de un trabajo más extenso o aplicado a un área particulares de la ciberseguridad.

Bibliografía

Basquecscentre; , EUSKALIT;. (2022). *Euskalit.net*.

Bustillos Ortega, l., & Rojas Segura, J. (2022 de Noviembre de 2). PROTOCOLO BÁSICO DE CIBERSEGURIDAD PARA PYMES. pág. 19.

Campo, L. M. (2020). *Ciberseguridad en la empresa moderna.*

Cano, J. J. (2021). *Ciberseguridad Empresarial.* LEMOINE.

Gonzales, F. (s.f.). *Ciberataques: por qué su pyme debería tener un plan de seguridad informática para empresas*. Obtenido de Py: https://www.pymas.com.co/ideas-para-crecer/mundo-pyme/seguridad-informatica-para-empresas

González, J. (2019). *La ciberseguridad y su impacto en la empresa.*

Javier Santiago, E., & Sanchez Allende, J. (2017). *Riesgos de Ciberseguridad en las Empresas.* Madrid.

Revista Semana. (3 de 01 de 2023). Pymes: esto deben tener en cuenta para su ciberseguridad. pág. 30. Obtenido de https://www.semana.com/economia/empresas/articulo/pymes-esto-deben-tener-en-cuenta-para-su-ciberseguridad/202355/

CARTA SESION DE DERECHOS

Por intermedio del presente documento en mi calidad de autor o titular de los derechos de propiedad intelectual de la obra que adjunto, titulada **Diseño De Un Modelo De Consultoría Enfocado A La Importancia De La Ciberseguridad En Pymes**, autorizo a la Corporación universitaria Unitec para que utilice en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador o titular de la obra objeto del presente documento.

La presente autorización se da sin restricción de tiempo, ni territorio y de manera gratuita. Entiendo que puedo solicitar a la Corporación universitaria Unitec retirar mi obra en cualquier momento tanto de los repositorios como del catálogo si así lo decido.

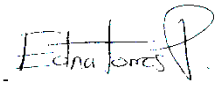
La presente autorización se otorga de manera no exclusiva, y la misma no implica transferencia de mis derechos patrimoniales en favor de la Corporación universitaria Unitec, por lo que podré utilizar y explotar la obra de la manera que mejor considere. La presente autorización no implica la cesión de los derechos morales y la Corporación universitaria Unitec los reconocerá y velará por el respeto a los mismos.

La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato electrónico, y en general para cualquier formato conocido o por conocer. Manifiesto que la obra objeto de la presente autorización es original y la realicé sin violar o usurpar derechos de autor de terceros, por lo tanto, la obra es de mi exclusiva autoría o tengo la titularidad sobre la misma. En caso de presentarse

cualquier reclamación o por acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión asumiré toda la responsabilidad, y saldré en defensa de los derechos aquí autorizados para todos los efectos la Corporación universitaria Unitec actúa como un tercero de buena fe. La sesión otorgada se ajusta a lo que establece la ley 23 de 1982.

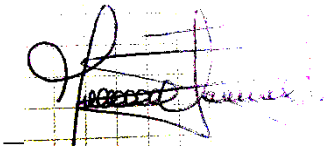
Para constancia de lo expresado anteriormente firmo, como aparece a continuación.

Firma



Nombre Edna Margarita Torres
CC. 103.6626.938

Nombre Juan Sebastian Pardo
CC. 1.073.236.579



Nombre Norman Alberto Molina
CC. 1.015.999.098