PLAN DE CAPACITACIÓN EN CIBERSEGURIDAD PARA LA FORMACIÓN DE PERSONAL EN EL CENTRO DE OPERACIONES DE SEGURIDAD SOC DE LA EMPRESA DATASEC SAS

FERNANDO SERRANO TOVAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

PLAN DE CAPACITACIÓN EN CIBERSEGURIDAD PARA LA FORMACIÓN DE PERSONAL EN EL CENTRO DE OPERACIONES DE SEGURIDAD SOC DE LA EMPRESA DATASEC SAS.

FERNANDO SERRANO TOVAR

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

MIGUEL ANDRES AVILA GUALDRON
Tutor de Curso

MANUEL ANTONIO SIERRA RODRIGUEZ
Director Proyecto de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 20 de mayo de 2024

DEDICATORIA

Con amor, este proyecto aplicado lo dedico a ti, mi querido hijo, que llegaste al mundo con la promesa de un futuro lleno de retos y oportunidades.

AGRADECIMIENTOS

Quiero expresar mi agradecimiento a todas las personas que me han brindado su apoyo y colaboración en la elaboración de este proyecto aplicado.

En primer lugar, agradezco a la empresa Datasec SAS por brindarme la oportunidad de trabajar en un proyecto de tal envergadura y permitirme trabajar en el maravilloso mundo de la ciberseguridad.

También quiero agradecer a los Ingenieros Eduard Mantilla, Miguel Andrés Avila y Manuel Antonio Sierra, por su orientación, apoyo y retroalimentación constante, lo que me permitió mejorar este proyecto aplicado de manera significativa.

Finalmente, quiero agradecer a mi familia por su apoyo incondicional y su paciencia durante todo el proceso de elaboración del proyecto.

¡Muchas gracias a todos!

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AMENAZA: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

CIBERDELINCUENTE: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.

CIBERATAQUE: Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

HACKER: Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.

NGFW: Término proveniente del inglés New Generation Firewall, es un cortafuegos de nueva generación, llamado así por estar formado por diferentes elementos, cada uno de los cuales ofrecerá una característica distinta, lo que permite una mejor capacidad de procesamiento, y ante la caída de uno de los servicios, el resto puede seguir funcionando con normalidad.

RIESGO: Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado.

SANDBOX: Se define como un entorno de pruebas aislado que permite ejecutar aplicaciones peligrosas o dudosas sin riesgo de poner en peligro otros sistemas de la organización empresarial.

SIEM: Acrónimo de las siglas en inglés Security Information and Event Management; en español, gestión de eventos e información de seguridad. Se trata de un software con el que se intenta detectar y prevenir amenazas para atajarlas antes de que ocurran. El término comprende, por un lado, el almacenamiento y análisis de eventos en tiempo real SEM; y por otro, el almacenaje para su posterior análisis SIM. De la unión de los dos nace el SIEM, su objetivo es recopilar, identificar

y analizar los eventos de seguridad de forma rápida para prevenir posibles ataques y vulnerabilidades.

SOC: Del inglés Security Operations Center; en español, centro de operaciones en seguridad. Se trata de un equipo cualificado específicamente en ciberseguridad con las herramientas necesarias para poder analizar, investigar y dar soporte convenientemente a posibles eventos de ciberseguridad corporativos. Un SOC puede ser externo o interno, y su objetivo es evitar y mitigar posibles ataques en la empresa, constituyendo lo que podríamos llamar contramedidas ante un ciberataque

VULNERABILIDAD: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

Las anteriores definiciones, fueron tomadas en su totalidad del glosario de términos de ciberseguridad, una guía de aproximación para el empresario, patrocinado por el INCIBE (Instituto nacional de ciberseguridad de España).[1]

[1] INCIBE. (2021). Protege tu empresa - Glosario de términos de ciberseguridad, una guía de aproximación para el empresario. Recuperado el 5 de abril de 2023 Disponible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

RESUMEN

El objetivo principal de este proyecto es diseñar un plan de capacitación en fundamentos de ciberseguridad dirigido tanto al personal activo en su centro de operaciones de seguridad SOC como a aquellos individuos con interés en el campo de la seguridad informática y que aspiran a ingresar a este ámbito. La iniciativa, autorizada por Datasec SAS, busca no solo mantener actualizado a su personal, sino también identificar y capacitar a estudiantes que puedan potencialmente incorporarse a la empresa en el futuro, ocupando roles relacionados con el centro de operaciones de seguridad, SOC.

Para lograr este objetivo, se deben identificar las habilidades y conocimientos técnicos que son esenciales para desempeñarse en el campo de la ciberseguridad, y a su vez, guiados en modelos de competencias, se busca consolidar estas habilidades de manera alineada con las necesidades específicas de la organización, posibilitando un desempeño efectivo en el campo de la seguridad informática, especialmente como miembro de un Centro de Operaciones de Seguridad SOC. La elaboración de este plan de capacitación involucra la utilización de cursos de reconocidas marcas en ciberseguridad, como Fortinet, Cisco e ISC2, además de la organización de conferencias y talleres de capacitación junto con la implementación de un sistema de seguimiento y evaluación que permita medir el éxito de este.

El propósito de esta iniciativa es fomentar el desarrollo de personal en el ámbito de la ciberseguridad, a la vez que se proporciona a la empresa Datasec SAS una vía para identificar y seleccionar potenciales candidatos para futuros empleos en el campo de la seguridad informática, específicamente cargos en el centro de operaciones de seguridad SOC. Así, se busca contribuir al fortalecimiento de la seguridad informática en la compañía y a la formación de una fuerza laboral especializada en ciberseguridad que pueda hacer frente a los desafíos tecnológicos del futuro en el campo de la ciberseguridad.

Palabras Claves: Amenazas cibernéticas, Ciberseguridad, SOC, Firewall, SIEM.

ABSTRACT

The main objective of this project is to design a training plan in the fundamentals of cybersecurity, targeting both active personnel in its Security Operations Center (SOC) and individuals interested in the field of computer security, aspiring to enter this domain. Led by Datasec SAS, the initiative aims not only to keep its personnel updated but also to identify and train students who could potentially join the company in the future, taking on roles related to the Security Operations Center, SOC.

To achieve this objective, it is necessary to identify the skills and technical knowledge that are essential to perform in the field of cybersecurity. Guided by competency models, the goal is to consolidate these skills in alignment with the specific needs of the organization, enabling effective performance in the field of computer security, especially as a member of a Security Operations Center, SOC. The development of this training plan involves the use of courses from renowned cybersecurity brands such as Fortinet, Cisco, and ISC, as well as the organization of conferences and training workshops, along with the implementation of a monitoring and evaluation system to measure its success.

The purpose of this initiative is to promote the development of personnel in the field of cybersecurity, while providing Datasec SAS with a way to identify and select potential candidates for future jobs in the field of computer security, specifically positions in the Security Operations Center, SOC. Thus, it seeks to contribute to strengthening cybersecurity within the company and to the formation of a specialized workforce in cybersecurity capable of addressing future technological challenges in the field of cybersecurity.

Keywords: Cyber threats, Cybersecurity, CSOC, Firewall, SIEM.

INTRODUCCIÓN

La ciberseguridad se ha convertido en un tema de gran relevancia en la actualidad, dadas las constantes amenazas que existen en el mundo digital. La alta demanda de profesionales capacitados en ciberseguridad contrasta con la escasez de personal especializado en este campo, lo que dificulta enormemente la selección de candidatos para cubrir estas posiciones. Además, la rotación de personal en este campo también es alta debido a la constante evolución de las amenazas cibernéticas y la necesidad de mantenerse actualizado con las últimas tecnologías y herramientas de seguridad. Ante esta problemática, se requiere una solución efectiva para reclutar y retener personal en ciberseguridad, y para cubrir la brecha entre la demanda laboral y la oferta de personal calificado en este campo. En este sentido, la empresa Datasec SAS se plantea el desafío de diseñar un plan de capacitación en fundamentos de ciberseguridad dirigido tanto al personal activo en su centro de operaciones de seguridad SOC como a aquellos individuos con interés en el campo de la seguridad informática y que aspiran a ingresar a este ámbito. El propósito es formar y capacitar individuos que puedan ser considerados para futuros empleos dentro de la empresa especialmente como integrantes del Centro de Operaciones de Ciberseguridad SOC.

Para lograr este objetivo, es necesario identificar las habilidades y conocimientos técnicos necesarios para desempeñarse en estos cargos. Para ello, es importante que la empresa Datasec SAS realice una evaluación de las habilidades y conocimientos técnicos que se requieren para desempeñarse en el campo de la ciberseguridad como profesional de un equipo SOC. Esta evaluación debe considerar las competencias necesarias para proteger la información, datos y sistemas informáticos de una organización contra amenazas internas y externas. También se deben tener en cuenta los estándares de seguridad de la información y las mejores prácticas en ciberseguridad.

Una vez identificadas las habilidades y conocimientos técnicos necesarios, guiados en modelos de competencias, se pueden consolidar estas habilidades de manera alineada con las necesidades específicas de la organización, en busca de un desempeño efectivo del personal de su Centro de Operaciones de Seguridad SOC. De esta manera, se puede elaborar el plan de capacitación en ciberseguridad cuidando de incluir en él los elementos necesarios para formar personal que cuente con bases sólidas para adoptar las competencias requeridas para integrarse exitosamente en un equipo SOC.

Es importante también establecer una propuesta clara y definida que pueda presentarse a instituciones educativas, como la UNAD. Esta propuesta busca crear un espacio de intercambio y aprendizaje entre los profesionales de Datasec SAS y los estudiantes. De esta manera, se facilita la invitación a aquellos estudiantes interesados para que participen en el plan de capacitación en ciberseguridad ofrecido por Datasec SAS.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La creciente amenaza de ciberataques y la necesidad de proteger los datos y sistemas de información en las organizaciones, ha aumentado la demanda de profesionales especializados en ciberseguridad en el campo laboral. No cabe duda, que en Colombia los ataques cibernéticos vienen en crecimiento. Así lo demuestra el informe de seguridad de Fortinet [2], el líder mundial en ciberseguridad; Colombia recibió 20 mil millones de intentos de ciberataques en 2022, un crecimiento del 80% frente a 2021. Sin embargo, existe una escasez de personal capacitado en ciberseguridad, lo que dificulta la selección de candidatos para cubrir estas posiciones. Según el experto Santiago Rangel, Ingeniero de Gestión de Incidentes de Ciberseguridad de Netdata Networks, "es un hecho que nuestra industria necesita más especialistas y por eso es importante que desde las universidades se reconozca esta necesidad y se sienten las bases para fomentar las especializaciones en ciberseguridad"[3]. Además, la rotación de personal en este campo también es alta debido a la constante evolución de las amenazas cibernéticas y la necesidad de mantenerse actualizado con las últimas tecnologías y herramientas de seguridad. Una encuesta de ISACA informó que "el 60 % de las empresas experimentaron dificultades para retener profesionales calificados en seguridad cibernética."[4] En el caso de la empresa Datasec SAS, esta se ha visto afectada por dicho problema, ya que ha enfrentado dificultades para encontrar y contratar a candidatos adecuados para cubrir posiciones críticas en áreas de ciberseguridad, específicamente, para cargos de entrada, en su centro de operaciones de seguridad (SOC), lo que ha llevado en ocasiones a una mayor carga de trabajo para los colaboradores existentes, aumentando así el riesgo de errores y la probabilidad de fallas en procedimientos de seguridad. Esto es altamente critico en la empresa, porque incrementa la probabilidad de no poder satisfacer las necesidades de sus clientes y mantenerse competitiva en el mercado. Por lo tanto, se requiere una solución efectiva para reclutar y retener personal en ciberseguridad, y para cubrir la brecha entre la demanda laboral y la oferta de personal calificado.

1.2 FORMULACIÓN DEL PROBLEMA

De lo anterior, se desprende la siguiente pregunta: ¿De qué manera el diseño de un plan de capacitación en ciberseguridad facilita enfrentar la demanda de profesionales en el centro de operaciones de seguridad de Datasec SAS, empresa que opera en la ciudad de Bogotá?

---

[2] Fortinet. (2023). FortiGuard Labs reports destructive wiper malware increases over 50 percent. Recuperado el 5 de abril de 2023, disponible en https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent

[3] Lozano, D. (2022). Ciberseguridad en Colombia: hay casi 3 millones de vacantes. Pulzo. https://www.pulzo.com/tecnologia/ciberseguridad-colombia-hay-casi-3-millones-vacantes-PP2130987A

[4] Casallas, D. (2023). Tendencias de seguridad cibernética "no técnicas" para 2023. Play Marketing. https://playmarketing.net/tendencias-de-seguridad-cibernetica-no-tecnicas-para-2023

2. JUSTIFICACIÓN

El proyecto de capacitación en fundamentos de ciberseguridad es una iniciativa muy necesaria y relevante para satisfacer la creciente demanda de profesionales especializados en este campo. En la actualidad, la seguridad informática se ha convertido en una preocupación primordial para las organizaciones y gobiernos, debido a la creciente amenaza de ciberataques y la necesidad de proteger los datos y sistemas de información.

Sin embargo, la escasez de personal capacitado en ciberseguridad realmente es un problema, no solo en Colombia, sino en todo el mundo, que enfrentan muchas organizaciones. Esto se debe en parte a la falta de programas de capacitación en ciberseguridad aplicada en las universidades y centros educativos y en la educación en general, así como a la constante evolución de las amenazas cibernéticas que requieren que los profesionales en ciberseguridad estén siempre actualizados y en constante formación.

En este sentido, el proyecto propuesto es una solución efectiva para fomentar el desarrollo de personal en ciberseguridad, al mismo tiempo que se provee a la empresa Datasec SAS, una vía para identificar y seleccionar potenciales candidatos para futuros cargos en el campo de la seguridad informática, específicamente, para cargos de entrada en su centro de operaciones de seguridad SOC. La capacitación y formación de individuos interesados en la seguridad informática es una forma de ampliar el campo de candidatos, al tiempo que contribuye a que el personal del centro de operaciones de seguridad de la empresa se mantenga actualizado y adquiera conocimientos en las últimas tecnologías, procesos y herramientas de ciberseguridad.

Este proyecto también posibilita promover la inclusión de mujeres y minorías en la industria de la ciberseguridad y así contribuir al desarrollo económico y tecnológico del país al aumentar la disponibilidad de personal capacitado en ciberseguridad, lo que daría un valor agregado a la iniciativa.

En definitiva, el proyecto propuesto es una iniciativa necesaria y relevante para abordar el problema de la escasez de talento en ciberseguridad y para satisfacer la creciente demanda laboral en este campo.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar un plan de capacitación basado en la identificación de habilidades y competencias necesarias en el área de la ciberseguridad, para la formación de candidatos y personal activo del centro de operaciones de seguridad de la empresa DATASEC SAS, ubicada en la ciudad de Bogotá.

3.2 OBJETIVOS ESPECÍFICOS

1. Realizar el diagnóstico del perfil de los cargos ocupados por el personal del Centro de Operaciones de Seguridad en Datasec SAS.

2. Determinar las habilidades y conocimientos necesarios para desempeñarse en el área de la ciberseguridad con base en un modelo de competencias de este campo.

3. Elaborar un programa de capacitación en fundamentos de ciberseguridad, que incluya material teórico actualizado, talleres de práctica y evaluaciones de seguimiento, que facilite la trasferencia de conocimiento y el desarrollo de habilidades tanto en candidatos como en el personal activo del centro de operaciones de seguridad de la empresa Datasec SAS.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

El mercado laboral de ciberseguridad a nivel mundial y por supuesto, en Colombia está experimentando una escasez de personal capacitado en ciberseguridad, lo que dificulta la selección de candidatos para cubrir estas posiciones. Se identifica el problema tanto en cantidad como en calidad,[5] ya que cuando hay candidatos para un puesto concreto, menos del 25% de ellos está realmente cualificado para el empleo.[6] La rotación de personal en este campo también es alta debido a la constante evolución de las amenazas cibernéticas y la necesidad de mantenerse actualizado con las últimas tecnologías y herramientas de seguridad. Por lo tanto, las organizaciones, enfrentan un desafío en la contratación y retención de talentos en ciberseguridad. Los ejecutivos de seguridad deben desarrollar espacios para anticiparse y observar atentamente los entornos cambiantes y superpuestos, en busca siempre de la protección de la información y los nuevos activos digitales.[7]

Es esencial contar con personal capacitado y disponible en área de la ciberseguridad. Para poder decir que una persona está capacitada en ciberseguridad, por lo menos debe tener una comprensión clara los componentes básicos de la ciberseguridad. Los componentes incluyen la identificación de vulnerabilidades, la prevención de intrusiones, la detección de intrusiones y la respuesta a incidentes.

La identificación de vulnerabilidades se refiere a la identificación de posibles vulnerabilidades en los sistemas de información y la eliminación o mitigación de estos riesgos. La prevención de intrusiones se refiere a la implementación de medidas de seguridad para evitar que los atacantes accedan a los sistemas de información. La detección de intrusiones se refiere a la identificación temprana de los ataques cibernéticos para minimizar los daños. La respuesta a incidentes se refiere a la gestión de los incidentes cibernéticos una vez que se han identificado.

Alguien que desee empezar por adquirir estos conocimientos base, haría bien en seguir la ruta de estudio de Fortinet. Por ejemplo, el curso de NSE1[8] está abierto a cualquier persona que desee aprender sobre el panorama de las amenazas y la seguridad de la información. El curso describe las ciberamenazas actuales y brinda consejos sobre cómo puede proteger su información.

[5] Pastor Acosta, Ó. (2017). Capacitación profesional y formación especializada en ciberseguridad. Cuadernos de Estrategia, . 185, 291–350. https://dialnet.unirioja.es/servlet/articulo?codigo=6115627

[6] WINICK, E. (2018). La falta de expertos en ciberseguridad obliga a recurrir a estudiantes. Revista Istmo, 359, 18–20. https://www.technologyreview.es/s/10614/la-falta-de-expertos-en-ciberseguridad-obliga-recurrir-estudiantes

[7] Andres R. Almanza J. (2021). Resiliencia digital: La nueva frontera para las organizaciones del siglo XXI. Sistemas, Núm. 159, 105-120. https://doi.org/10.29236/sistemas.n159a4

[8] Fortinet. (2023). NSE1 Instituto de entrenamiento Fortinet Network Security Associate. Recuperado el 5 de abril de 2023, de https://training.fortinet.com/local/staticpage/view.php?page=nse_1

NSE2[9] brinda conocimientos sobre los tipos de productos de seguridad que existen, para abordar las amenazas cibernéticas. La ciberseguridad debe ser un tema que se enseñe desde la educación básica. Lamentablemente la mayoría de las personas no son conscientes de los riesgos digitales a los que se enfrente y esto hace que, en su mayoría, las personas no conozcan lo que involucra el tema de la ciberseguridad. Con esto en mente, es importante identificar las habilidades clave que los estudiantes deben adquirir. Estas habilidades incluyen la capacidad de identificar vulnerabilidades en los sistemas de información, la capacidad de implementar medidas de seguridad para prevenir intrusiones, la capacidad de identificar y responder a incidentes de seguridad, y la capacidad de trabajar en equipo y comunicar eficazmente las soluciones de seguridad.

Cisco, empresa que fabrica dispositivos para redes locales y externas, y que presta el servicio de soluciones de red, cuenta con rutas de estudio especializadas para abordar lo anterior. En el curso de Introducción a la ciberseguridad,[10] se puede aprender acerca de las amenazas, los ataques y las vulnerabilidades más comunes y obtener información sobre cómo las empresas protegen sus operaciones de los ataques, además de conocer las últimas tendencias laborales y el contante crecimiento del campo de la ciberseguridad.

Además de ello, se tiene a disposición gran cantidad de software libre especializado en el campo de la ciberseguridad. Por ejemplo, se puede crear un sistema para la correlación de eventos (SIEM) de bajo coste, basado en ElasticSearch[11] y ElastAlert, marco que permite generar, mediante el uso de intervalos temporales, diferentes reglas, alertas y acciones en tiempo real. Hay un artículo excelente que ejemplifica su desarrollo, llevado a cabo en la universidad de Castilla.[12] Estas plataformas son propicias para desarrollar ejercicios y actividades de simulación. Por ejemplo, se pueden realizar talleres de respuesta a incidentes que permiten entrenar personas en habilidades relativas a reacciones y procesos ante situaciones ficticias de ataques y crisis, labores propias que debe desempeñar un profesional que se desempeñe en el cargo de analista de un centro de operaciones de ciberseguridad (CSOC). En un trabajo enfocado a la simulación de respuesta ante incidentes de ciberseguridad para aprendizaje en organizaciones, se encontró que los ejercicios realizados en entornos educativos mejoran los aprendizajes de las temáticas.[13]

---

[9] Fortinet. (2023). NSE2 Instituto de entrenamiento Fortinet Network Security Associate. Retrieved from https://training.fortinet.com/local/staticpage/view.php?page=nse_2.

[10] Cisco Networking Academy. (n.d.). Introduction to Cybersecurity. Retrieved from https://www.netacad.com/es/courses/cybersecurity/introduction-cybersecurity.

[11] Elastic. (2023). ¿Qué es Elasticsearch? [Webpage]. Retrieved from https://www.elastic.co/es/what-is/elasticsearch.

[12] Esteban-Navarro B, Larriva-Novo XA, Villagrá VA. 13 Diseño de Un Sistema de Correlación Basado En Software Libre Para La Detección de Anomalías En El Campo de La Ciberseguridad. Ediciones de la Universidad de Castilla-La Mancha; 2021. doi:10.18239/jornadas_2021.34.13

[13] Pacheco F. Simulación de respuesta ante incidentes de ciberseguridad para aprendizaje en organizaciones y en el aula. 2022 IEEE Biennial Congress of Argentina (ARGENCON), Biennial Congress of Argentina (ARGENCON), 2022 IEEE. September 2022:1-8. doi:10.1109/ARGENCON55245.2022.9939841

Ahora bien, lo anterior, puede encontrar acogida en un marco especializado para la seguridad informática. El marco NICE[14] (National Initiative for Cybersecurity Education) puede ser muy útil para ayudar a diseñar y ejecutar un plan de capacitación en ciberseguridad para las organizaciones del sector. El marco NICE proporciona un marco común de referencia para la ciberseguridad, que puede ser utilizado para identificar y definir las habilidades, conocimientos y tareas necesarias para los profesionales de la ciberseguridad. Inclusive, el marco NICE ofrece una serie de recursos, como el NICE Cybersecurity Workforce Framework[15] y la NICE Cybersecurity Workforce Development Toolkit,[16] que pueden ser utilizados para diseñar y ejecutar programas de capacitación y formación. Al utilizar el marco NICE, las organizaciones pueden comparar los perfiles de los cargos que buscan, con las habilidades y conocimientos necesarios para desempeñarse en el campo de la ciberseguridad y construir un plan de capacitación práctico, que incluya material teórico, laboratorios prácticos y evaluaciones de conocimiento. También se puede utilizar el marco NICE para evaluar el éxito del plan de capacitación, mediante el seguimiento y evaluación de los estudiantes, incluyendo su desempeño en las actividades y su posterior inserción laboral si así se desea. No cabe duda pues, que el marco NICE puede ser un recurso valioso para diseñar y ejecutar un plan de capacitación efectivo en ciberseguridad para que las organizaciones puedan implementarlo.

En conclusión, la ciberseguridad se ha convertido en una preocupación cada vez más importante para las organizaciones, especialmente en el contexto actual de trabajo remoto y digitalización. La escasez de personal capacitado en ciberseguridad a nivel mundial y en Colombia, junto con la constante evolución de las amenazas cibernéticas, representa un desafío para las organizaciones en la contratación y retención de talentos en este campo. Es esencial contar con personal capacitado en ciberseguridad, y existen diversas rutas de estudio y herramientas disponibles para adquirir los conocimientos necesarios. Además, es importante destacar la necesidad de educar sobre ciberseguridad desde la educación básica para concientizar a toda la población acerca de los riesgos digitales y fomentar el desarrollo de habilidades clave en este campo. En resumen, la ciberseguridad es fundamental para proteger la información y los sistemas de las organizaciones y garantizar la continuidad del negocio.

[14] National Institute of Standards and Technology (NIST). (2023). NICE Framework Resource Center. Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center.
[15] National Institute of Standards and Technology (NIST). (2023). NICE Cybersecurity Workforce Framework Revisions. NICE Framework Resource Center. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-framework-revisions
[16] Petersen, R. (2019). Workforce Development Toolkit It's all on NICCS. Presented at the FISSEA 32nd Annual Conference. Retrieved from https://csrc.nist.gov/CSRC/media/Events/FISSEA-32nd-Annual Conference/documents/Track_3/FISSEA%20Presentation_Anderson%20EA%20approved.pdf

4.2 MARCO CONCEPTUAL

Ciberseguridad

La ciberseguridad es el conjunto de prácticas, tecnologías y herramientas diseñadas para proteger los datos, las redes, y los sistemas en las organizaciones, de amenazas cibernéticas, como, por ejemplo, virus, malware, hackers y ciberataques. Como se menciona en el libro Ciberseguridad, un enfoque desde la ciencia de datos, se trata "del área de las ciencias de la computación encargada del desarrollo y la implementación de los mecanismos de protección de la información y la infraestructura tecnológica."[17]

En la actualidad, la ciberseguridad se ha convertido en una preocupación importante para las organizaciones, debido al aumento de la cantidad y la complejidad de los ciberataques. Desde la reciente de pandemia, el trabajo remoto se ha vuelto más común de lo habitual, pues se argumenta que el trabajo remoto llegó para quedarse, o por lo menos una solución hibridad es latente[18]; y esto hace que el tema de la seguridad sea aún más pertinente ya que ahora, las organizaciones deben garantizar ya no solo sus infraestructuras, sino la forma en la que sus empleados se conectan a ellas. Para hacer frente a esta problemática, las organizaciones requieren personal altamente capacitado en ciberseguridad para proteger sus sistemas de información y garantizar la continuidad del negocio.

Amenazas Cibernéticas

Las amenazas cibernéticas abarcan una amplia gama de posibles ataques dirigidos hacia sistemas, dispositivos y redes conectados tanto a Internet como a otras infraestructuras de comunicación. Estas amenazas pueden surgir de individuos o grupos con intenciones maliciosas, como ciberdelincuentes, pero también pueden originarse de eventos fortuitos, como desastres naturales, fallos técnicos o errores humanos involuntarios. Dentro de las amenazas cibernéticas se encuentran diversos tipos de ataques, manifestándose a través de intrusiones, malware, phishing y otras tácticas perjudiciales que buscan comprometer la integridad, confidencialidad y disponibilidad de la información digital. La creciente interconexión de sistemas y la evolución constante de la tecnología destacan la importancia de abordar proactivamente la seguridad cibernética para mitigar estos riesgos y garantizar un entorno digital seguro. A continuación, se describen algunos de las amenazas cibernéticas más comunes, basados en la información suministrada por el líder mundial en ciberseguridad Fortinet.[19]

[17] Urcuqui López, C. C., García Peña, M., Osorio Quintero, J. L., & Navarro Cadavid, A. (2018). Ciberseguridad. Un enfoque desde la ciencia de datos. Editorial Universidad Icesi. Recuperado de https://www.icesi.edu.co/editorial/ciberseguridad/

[18] David, D. (2021). 5 Models for the Post-Pandemic Workplace. Harvard Business Review. https://hbr.org/2021/06/5-modelsfor-the-post-pandemic-workplace

[19] Fortinet Latin-American. (2023) https://www.fortinet.com/lat

Malware

Software malicioso diseñado para dañar[20], alterar o tomar el control de un sistema informático sin el conocimiento o consentimiento del propietario. El malware se puede propagar a través de correos electrónicos, sitios web infectados, dispositivos USB infectados y otros medios. Los efectos del malware pueden ser variados y peligrosos, como el robo de información personal o financiera, la toma de control del sistema informático, el cifrado de datos y la extorsión. Los usuarios deben tomar medidas de seguridad, como la instalación de software de protección contra malware y el mantenimiento de copias de seguridad regulares de los datos, para proteger sus sistemas contra el malware.

Phishing

Ataque cibernético que usualmente llega a los usuarios a través de correo electrónico, mensaje de texto o social media[21]. El atacante intenta engañar a un usuario haciéndose pasar por un contacto de confianza para que revele información confidencial, como contraseñas, información financiera o datos personales. Los correos electrónicos y mensajes de texto suelen incluir enlaces o archivos adjuntos que parecen legítimos, pero que en realidad llevan a sitios web falsificados o descargan malware en el sistema del usuario. Los sitios web falsificados también pueden parecerse a sitios web legítimos, como los de bancos o redes sociales, pero su objetivo es recopilar información confidencial de los usuarios. Los usuarios pueden protegerse contra el phishing mediante la educación sobre cómo detectar los intentos de phishing, la instalación de software de seguridad y la verificación de la autenticidad de los sitios web antes de ingresar información confidencial.

Ransomware

Código malicioso que hace que los dispositivos atacados no estén disponibles[22], hasta que se realiza un pago al ciberdelincuente. El ransomware, una forma insidiosa de malware, opera al cifrar los archivos cruciales de la víctima, tornándolos inaccesibles y restringiendo el acceso al sistema. La infiltración de este software malicioso ocurre mediante múltiples vías, entre las que se incluyen archivos adjuntos perjudiciales en correos electrónicos engañosos o mediante enlaces a sitios web infectados. Una vez que ha logrado encriptar los archivos, los perpetradores detrás del ataque demandan un rescate económico, instando a la víctima a efectuar el pago correspondiente para obtener la clave de desencriptación necesaria.

---

[20] Fortinet. (2023). Malware. https://www.fortinet.com/lat/resources/cyberglossary/malware

[21] Fortinet. (2022). Reconocer, reportar y prevenir el phishing. https://www.fortinet.com/lat/blog/industry-trends/reconocer-reportar-y-prevenir-el-phishing#:~:text=%C2%BFQu%C3%A9%20es%20el%20phishing%3F,de%20texto%20o%20social%20media.

[22] Fortinet. (2023). How to Prevent Ransomware. https://www.fortinet.com/lat/resources/cyberglossary/how-to-prevent-ransomware.

DDoS

Ataque de denegación de servicio distribuido (DDoS[23], por sus siglas en inglés) es un tipo de ciberataque en el que se intenta inundar un servidor o red con un gran número de solicitudes de conexión simultáneas para abrumar sus recursos, es decir, hacer que se saturen y se vuelvan inaccesibles para los usuarios legítimos. Los atacantes utilizan técnicas como el envío masivo de tráfico malicioso desde múltiples dispositivos infectados, lo que hace que sea difícil identificar y bloquear las fuentes del ataque. Estos ataques pueden tener graves consecuencias, como la interrupción del servicio para los usuarios legítimos, la pérdida de ingresos y reputación para las empresas afectadas, y la posibilidad de que se utilicen como distracción para otros ataques más avanzados. Estas amenazas pueden afectar a empresas, organizaciones gubernamentales y personas individuales, y pueden tener consecuencias graves como pérdida de datos, robo de información personal o financiera, pérdida de ingresos, daño a la reputación y, en casos extremos, daño físico. Es importante tomar medidas de seguridad cibernética para prevenir y mitigar las amenazas cibernéticas. El establecimiento de un CSOC puede proporcionar una mayor visibilidad y control sobre la infraestructura de TI de una organización, permitiendo una detección y respuesta más efectiva a los incidentes de seguridad.

Csoc

Centro de operaciones de ciberseguridad, CSOC[24] es un equipo de profesionales en ciberseguridad, dedicado a monitorear analizar y responder a las amenazas de seguridad informática en una organización. En este centro se monitorean los sistemas de información que una empresa usa para su infraestructura de TI. Esto puede incluir todo, desde sitios web, bases de datos, servidores, aplicaciones, redes, escritorios, centros de datos y una variedad de puntos finales de la empresa. Una configuración de seguridad cibernética SOC monitorea cada elemento de la infraestructura, evalúa su estado actual, incluidas las amenazas potenciales y existentes, y responde a las amenazas. El SOC también establece medidas y protocolos de seguridad de la información diseñados para prevenir futuras amenazas. El objetivo principal del CSOC es proteger los sistemas y redes de la organización de ataques cibernéticos mediante la detección temprana, la respuesta rápida y la prevención proactiva de futuros ataques. Un CSOC puede ayudar a identificar y priorizar las amenazas a medida que se producen, lo que permite una respuesta rápida y eficaz a los incidentes de seguridad. Además, el CSOC puede ayudar a una organización a identificar las vulnerabilidades en su infraestructura y tomar medidas para mitigarlas antes de que puedan ser explotadas por los atacantes.

[23] Fortinet. (2023). Ataques de DoS y Ataque DDoS. Types of Cyber Attacks. https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks

[24] Fortinet. (2023) ¿Qué es un SOC? Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/what-is-soc

Modelo de Competencias

Estructura que identifica las habilidades, conocimientos, comportamientos y capacidades necesarias para tener éxito en una función o rol específico dentro de una organización. Según el sistema regional de cooperación para la vigilancia de la seguridad operacional[25], es un "modelo de gestión que se basa en las características personales de los ocupantes más exitosos de ciertos cargos, para establecer los elementos requeridos en las personas que forman parte de una organización y que permiten un buen desempeño organizacional."

El modelo de competencias define claramente las habilidades y características que un individuo debe tener para realizar de manera efectiva su trabajo y ayudar a alcanzar los objetivos de la organización. Además, el modelo de competencias se utiliza a menudo en la evaluación del desempeño, el desarrollo de planes de capacitación y desarrollo, la selección de personal y la toma de decisiones sobre promociones y ascensos en la empresa.

Soluciones SIEM

SIEM son las siglas de Security Information and Event Management (Administración de Eventos e Información de Seguridad, en español). Es una solución de seguridad que se utiliza para recopilar, correlacionar, analizar y visualizar datos de diferentes fuentes en tiempo real con el fin de detectar y responder a amenazas de seguridad informática. El SIEM de Fortinet. FortiSIEM [26] está diseñado para ser la columna vertebral del equipo de operaciones de ciberseguridad seguridad, pues ofrece capacidades que van desde la creación automática de inventario de activos hasta la aplicación de análisis de comportamiento de vanguardia para detectar y responder rápidamente a las amenazas.

Los sistemas SIEM permite la recopilación de datos de diferentes dispositivos y sistemas, como firewalls, servidores, sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusiones (IPS), entre otros, para analizarlos y correlacionarlos en tiempo real. Esto ayuda a los equipos de seguridad a identificar patrones y anomalías que podrían indicar una amenaza, y a tomar medidas para prevenir o mitigar el impacto de un posible ataque. Además, también se utiliza para generar informes de cumplimiento y auditoría de seguridad, lo que lo hace una herramienta muy útil para cumplir con las regulaciones y normativas de seguridad.

---

[25] Diaz D. (2012) Definición y control de competencias Presentación realizada en la Conferencia de la Región SAM de la OACI. https://www.icao.int/SAM/Documents/2012/DSOSYMP12/Definici%C3%B3n%20y%20control%20de%20Competencias%20.pdf

[26] Fortinet Información de seguridad y administración de eventos (SIEM) https://www.fortinet.com/lat/products/siem/fortisiem

5. DISEÑO METODOLÓGICO

La metodología utilizada es Cuantitativa.

- Proceso investigativo:

El proceso investigativo se llevará a cabo en tres etapas interrelacionadas.

En la primera etapa, se estudiarán las necesidades y expectativas específicas de la empresa DATASEC SAS en cuanto al perfil de seguridad que busca para cargos vinculados al SOC. Se validará con el equipo de seguridad de la empresa para comprender las habilidades y conocimientos que consideran importantes en un candidato y así evaluar la adecuación del plan de capacitación propuesto. Es importante destacar que el puesto de entrada para las posiciones en su SOC es el de Analista SOC N1.

En la segunda etapa, se identificarán las habilidades y competencias necesarias para desempeñarse de manera efectiva en el campo de la ciberseguridad. Se revisarán los marcos de referencia y los estándares internacionales de ciberseguridad para compilar una lista de habilidades clave, y, posteriormente, adaptarla a las necesidades específicas de DATASEC SAS.

Finalmente, en la tercera etapa, teniendo en cuenta la información se procederá a desarrollar un programa de formación base en ciberseguridad para estudiantes talentos que permita no solo aborda la escasez de talento en ciberseguridad, sino que también establezca una vía para identificar y cultivar futuros especialistas en seguridad cibernética.

Este enfoque garantiza que el plan de capacitación base sea completo y esté actualizado, asegurando que los estudiantes adquieran las habilidades fundamentales necesarias para enfrentar los desafíos actuales y futuros en el campo de la ciberseguridad.

- Selección de la muestra:

Se seleccionará una muestra de mínimo un candidato que cumplan con los criterios de selección establecidos por Datasec.

- Recopilación de datos:

Se diseñará un cuestionario estructurado que permita medir el nivel de conocimiento técnico y las habilidades en ciberseguridad de los estudiantes antes y después del plan de capacitación. Los datos serán recopilados antes del inicio del programa y al finalizar el mismo.

- Análisis de datos:

Los datos recopilados serán analizados mediante estadística descriptiva e inferencial para determinar si existe una mejora significativa en el desempeño de los estudiantes en términos de conocimiento y habilidades en ciberseguridad.

- Conclusiones y recomendaciones:

Se elaborarán conclusiones y recomendaciones basadas en los resultados del análisis de datos. Estas recomendaciones serán utilizadas para mejorar el plan de capacitación y aumentar su eficacia en el futuro.

- Implementación:

Finalmente, el plan de capacitación será implementado en Datasec y se establecerá un sistema de seguimiento y evaluación para medir su impacto en el desempeño de los estudiantes y en la empresa.

6. PERFIL DE CARGOS DEL CENTRO DE OPERACIONES DE SEGURIDAD SOC DATASEC

La ciberseguridad es una de las áreas de mayor crecimiento y relevancia en el mundo empresarial actual, en donde la protección de la información se ha convertido en una preocupación primordial. Las organizaciones buscan constantemente profesionales especializados en ciberseguridad que puedan garantizar la protección de sus sistemas y datos, y a su vez, asegurar la continuidad de sus operaciones y el cumplimiento de sus objetivos.

La elevada demanda y escasa oferta de profesionales en ciberseguridad han desencadenado una competencia por el talento, complicando la contratación de personal calificado en este campo. Datasec SAS, una empresa líder en ciberseguridad en el mercado colombiano, ofrece una amplia gama de soluciones y servicios de seguridad para sus clientes. Sin embargo, enfrenta un desafío al identificar la dificultad para encontrar candidatos que ocupen posiciones dentro de su Centro de Operaciones de Seguridad SOC. Normalmente, el puesto de entrada en el SOC de la compañía es el de Analista SOC N1, siendo esencial que el titular de este cargo posea fundamentos sólidos en ciberseguridad, ya que constituye la base de la proyección laboral en la empresa. Se espera que, a partir de este rol inicial, se seleccionen recursos para asumir posiciones de mayor responsabilidad.

Por esta razón, a través de este capítulo, se llevará a cabo un diagnóstico no solo del perfil específico del Analista N1 SOC de Datasec, sino también de la diversidad de perfiles que conforman los roles dentro del Centro de Operaciones de Seguridad de la empresa. El propósito principal es la recopilación de las habilidades y conocimientos técnicos esenciales para el desempeño efectivo de funciones dentro del SOC. A través de este análisis, se pretende identificar de las aptitudes, técnicas y conocimientos fundamentales, al tiempo que se profundizará en la evaluación de los requisitos necesarios para ocupar cada uno de estos puestos estratégicos en la organización.

Con el fin de alcanzar este objetivo, iniciaremos con una panorámica integral de Datasec SAS, una empresa con su centro de operaciones ubicado en la ciudad de Bogotá. En este contexto, se abordarán aspectos clave como su misión, gama de servicios, las distintas áreas que conforman su estructura organizativa, y las colaboraciones estratégicas establecidas con diversos aliados. Este enfoque preliminar proporcionará un marco contextual esencial antes de sumergirnos en el análisis actual de los perfiles necesarios por parte de Datasec para cubrir los puestos cruciales dentro de su Centro de Operaciones de Seguridad SOC.

6.1 LA EMPRESA

DATASEC SAS destaca como una destacada empresa de servicios tecnológicos, especializada en la implementación, administración, soporte, monitoreo y gestión

de plataformas de seguridad informática y redes. Originaria de Colombia, DATASEC ha forjado un sólido historial al desarrollar proyectos significativos en el ámbito de la ciberseguridad y conectividad, atendiendo tanto a entidades públicas como privadas.

La especialización de la compañía se concentra en diversas áreas de vanguardia, entre las que se incluyen:

- Servicios Gestionados de Seguridad: Ofreciendo soluciones integrales para la gestión eficaz de la seguridad de la información.

- Servicios de Ciberseguridad SOC: Destacándose en el establecimiento y operación de Centros de Operaciones de Seguridad Cibernética para una defensa proactiva contra amenazas.

- Implementación de Tecnologías de Ciberseguridad: Desplegando innovadoras soluciones tecnológicas para fortalecer la seguridad digital de sus clientes.

- Soporte a Dispositivos y Tecnologías de Ciberseguridad: Brindando un respaldo técnico especializado para garantizar el óptimo rendimiento y funcionamiento de los sistemas de seguridad cibernética implementados.

El área en la empresa en la que se centra este proyecto es su centro de operaciones de Seguridad SOC. Esta área se propone como objetivo principal desempeñar una función centralizada dedicada a la vigilancia, análisis continuo, prevención y mitigación constante de amenazas cibernéticas. Fundamentado en el uso de herramientas que cuentan con el respaldo del modelo de arquitectura de seguridad adaptable de Gartner, su finalidad es abordar y contrarrestar eficazmente el delito cibernético en el actual panorama de amenazas digitales. Dentro del Centro de Operaciones de Ciberseguridad de Datasec SAS, se lleva a cabo una supervisión constante de los sistemas y redes de organizaciones, tanto públicas como privadas, que han contratado los servicios de la empresa. Esta actividad se realiza con el propósito de detectar proactivamente posibles amenazas o incidentes de seguridad. Es responsabilidad del personal del SOC recopilar meticulosamente la información y llevar a cabo un análisis exhaustivo para identificar posibles intrusiones, malware, ataques de denegación de servicio (DDoS), entre otras amenazas cibernéticas.

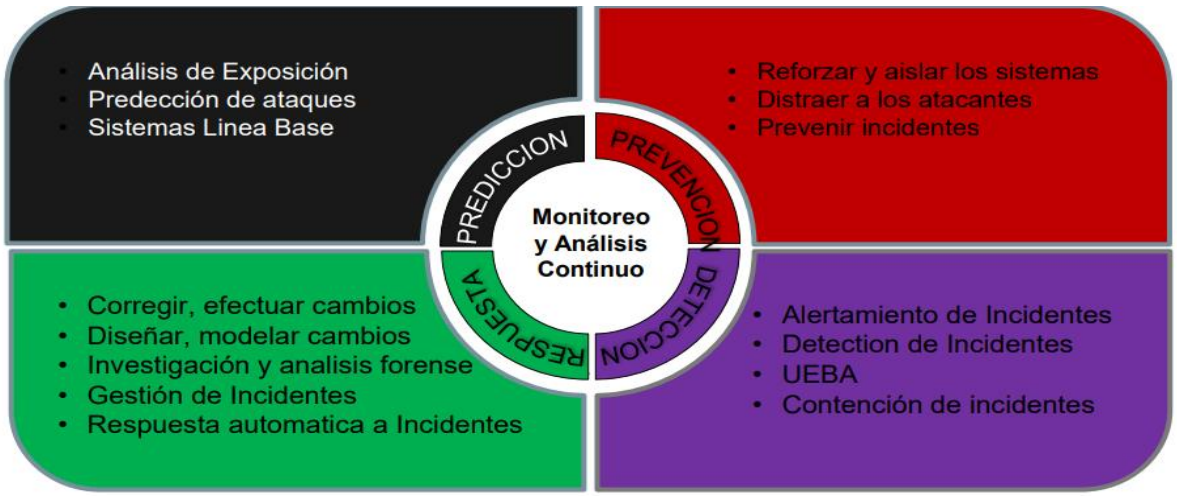
Una vez que se identifica una amenaza, se activan medidas de respuesta con el objetivo de mitigar el riesgo. Este proceso implica el despliegue de acciones que permiten emitir una alerta temprana, acompañada de recomendaciones pertinentes para la gestión eficaz de los incidentes de seguridad. Esta labor incluye la documentación detallada de los incidentes, la investigación profunda de sus causas, la implementación de medidas correctivas y preventivas, así como la comunicación

efectiva con las partes interesadas en cada organización afectada. Además, el Centro de Operaciones de Seguridad SOC de Datasec también asume la responsabilidad de elaborar informes detallados y presentar recomendaciones estratégicas destinadas a mejorar la seguridad de las organizaciones. En resumen, los colaboradores que ocupan cargos dentro del Centro de Operaciones de Seguridad (SOC) de Datasec SAS desempeñan una función crucial al encargarse de salvaguardar y gestionar la ciberseguridad de las organizaciones que han depositado su confianza en los servicios ofrecidos. Este enfoque proactivo y multidimensional contribuye significativamente a la fortaleza y resiliencia digital de sus clientes.

6.1.1 Alcance servicio SOC

El alcance del servicio SOC en la empresa Datasec, es detectar intrusiones que comprometan la información en los servicios, aplicativos y activos tecnológicos de los clientes. Además, se enfoca en proporcionar los mecanismos necesarios para responder y recuperar los activos afectados en el menor tiempo posible y con el mínimo impacto. El objetivo principal del servicio SOC es brindar respuestas efectivas para la resolución de incidentes de seguridad. Esto implica el desarrollo e implementación de planes de solución que neutralicen las amenazas, teniendo en cuenta la criticidad del ataque, la importancia de los activos comprometidos y el impacto que puedan tener sobre los mismos. En la Figura 1 se puede ver un resumen del alcance del servicio SOC en Datasec.

Figura 1 Monitoreo y análisis continuo



Fuente: Datasec SAS (2023). Monitoreo y análisis continúo adaptado Fortinet.

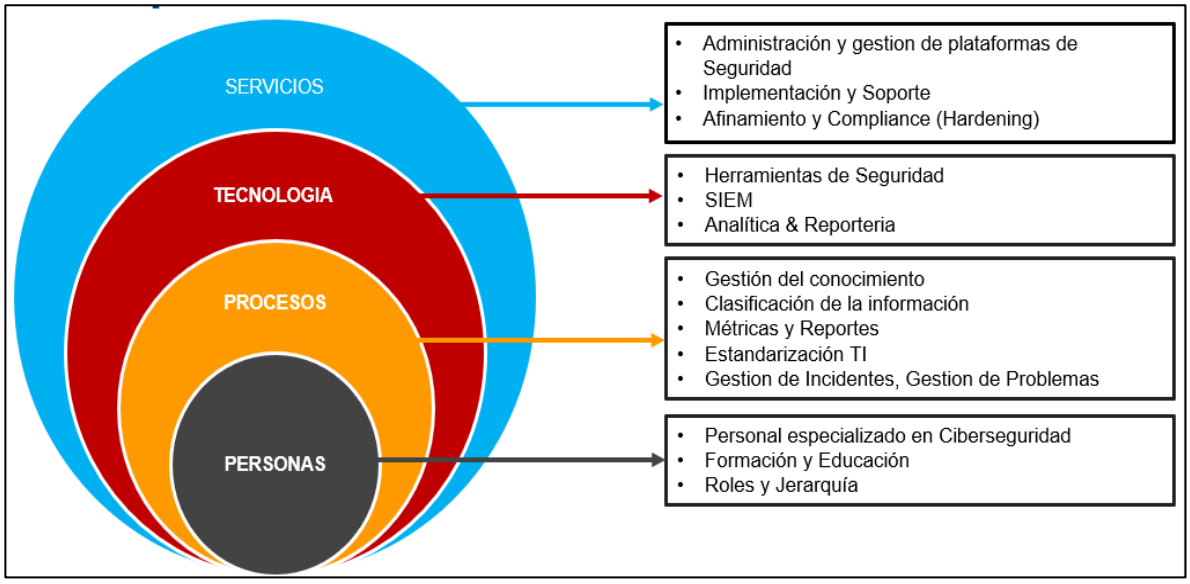
6.1.2 Arquitectura del servicio SOC

La columna vertebral de la arquitectura del servicio SOC reside en el recurso humano, es decir, en individuos especializados en ciberseguridad con una formación educativa en este ámbito. Este equipo de trabajo se organiza en diversos roles y jerarquías, conformando así un conjunto robusto y eficiente. Además, la implementación de procesos por parte de Datasec SAS facilita la gestión del conocimiento, la clasificación de la información, la ejecución de casos de uso, así como la creación de métricas y reportes. Estos procesos se llevan a cabo bajo modelos estandarizados de tecnologías de la información, que permiten la eficaz gestión de incidentes y problemas.

En el siguiente nivel de la arquitectura, se encuentran las herramientas tecnológicas de seguridad, como dispositivos tipo FIREWALL, SIEM, SOAR, SANDBOX, además de gestores de vulnerabilidades, así como servicios de monitoreo de marca. Estas herramientas desempeñan un papel clave en la detección y respuesta a amenazas cibernéticas. Finalmente, en el último componente, se destacan los servicios que abarcan desde la administración y gestión de plataformas de seguridad hasta la implementación, soporte, ajuste y cumplimiento normativo de las mismas.

El resumen visual de esta arquitectura se presenta de manera esquemática en la Figura 2.

Figura 2 Arquitectura del servicio



Fuente: Datasec SAS (2023). Arquitectura del servicio adaptada Fortinet.

6.1.3 Aliados estratégicos

La compañía Datasec cuenta con aliados estratégicos para dar alcance a sus objetivos y poder fundamentar su arquitectura de servicio. Algunos de ellos son:

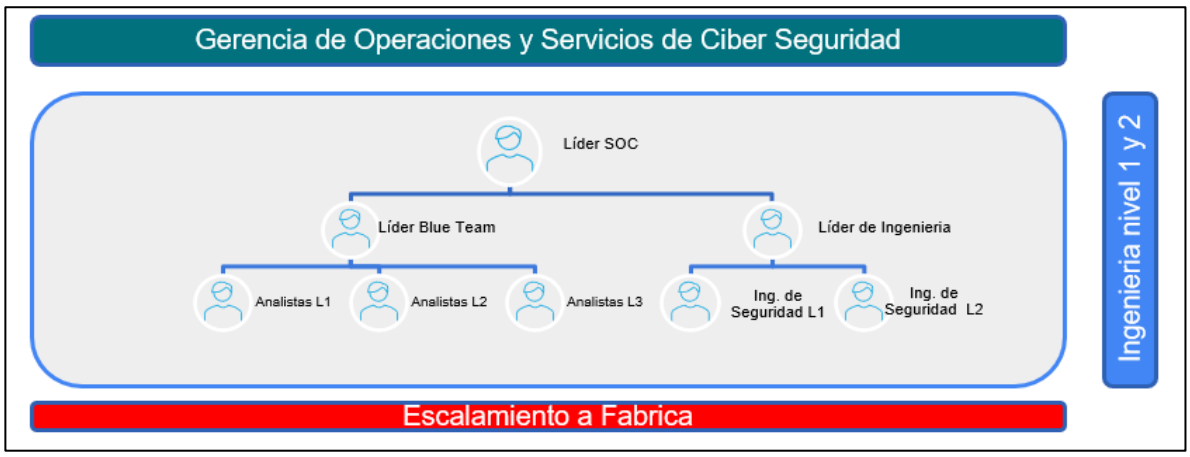
- FORTINET
- TENABLE
- AXUR
- DARKTRACE
- STELLAR

6.1.4 Estructura equipo de trabajo

El servicio SOC de Datasec se configura mediante un equipo de profesionales que opera de forma ininterrumpida en modalidades 7x24 y 8x5. Este equipo se especializa en llevar a cabo actividades de monitoreo y gestión de eventos e incidentes relacionados con el rendimiento y la disponibilidad de los dispositivos en la infraestructura tecnológica de diversos clientes.

Para ofrecer una visión detallada de la estructura organizativa de este servicio, se presenta en la Figura 3 el organigrama que representa el equipo de trabajo del Centro de Operaciones de Seguridad Cibernética (CSOC) en Datasec SAS.

Figura 3 Estructura equipo de trabajo SOC



Fuente: Datasec SAS (2023). Estructura equipo de trabajo SOC.

Es precisamente, la base de la anterior estructura, la que atañe a la propuesta de este proyecto aplicado. Por lo general, para iniciar carrera en la compañía, en el área de ciberseguridad, se empieza por al cargo de Analista SOC N1. En este nivel, Datasec SAS ha experimentado retos notables al buscar profesionales capacitados que se ajusten a las demandas de este puesto específico. Un desafío recurrente ha sido la constatación de una marcada carencia de conocimientos especializados en ciberseguridad entre los profesionales graduados en disciplinas como ingeniería de sistemas, electrónica o telecomunicaciones.

Esta observación se convierte en un punto crítico que justifica la necesidad de intervenir mediante el proyecto propuesto. La falta de conocimientos específicos en ciberseguridad entre los recién graduados en áreas técnicas relacionadas representa una brecha significativa en la formación de los Analistas SOC N1. Al enriquecer y adaptar las oportunidades de formación y desarrollo profesional, se busca cerrar la brecha de conocimiento identificada y cultivar un potencial equipo de Analistas SOC N1 más capacitado y preparado para enfrentar los desafíos emergentes en el ámbito de la seguridad cibernética

6.2 POSICIONES VINCULADAS AL SOC DATASEC

El Centro de Operaciones de Seguridad SOC de Datasec SAS desempeña un papel fundamental en la salvaguardia de la información y los sistemas de las organizaciones clientes. La eficacia de sus servicios radica en la presencia de un equipo altamente capacitado y dotado de habilidades en seguridad informática, dado que los ciberdelincuentes perpetuamente buscan innovar sus tácticas de ataque contra las organizaciones. En este contexto, la ciberseguridad demanda conocimientos técnicos específicos y habilidades especializadas para la configuración, administración y mantenimiento efectivos de los sistemas de seguridad. En Datasec, se reconoce y valora la importancia de contar con profesionales que estén a la vanguardia en las últimas tendencias y amenazas cibernéticas, garantizando así un SOC que responda de manera proactiva y eficiente a los desafíos en constante evolución del panorama de seguridad digital.

A continuación, se explorarán las diferentes posiciones vinculadas al SOC de Datasec. Este análisis abarcará desde los Analistas SOC N1, N2 y N3, el Líder Blue Team, hasta los Ingenieros de Seguridad N1 y N2, así como los roles de Líder de Ingeniería y Líder de SOC. Se llevará a cabo un diagnóstico de las competencias actuales y habilidades esenciales requeridas para cada una de estas funciones. A pesar de que la atención inicial se centra en el cargo de entrada, Analista SOC N1, resulta fundamental realizar un diagnóstico de todos los perfiles del SOC. Este enfoque integral nos permitirá comprender a fondo las diversas actividades relacionadas con la operatividad del Centro de Operaciones de Seguridad SOC de Datasec.

6.2.1 ANALISTA SOC N1

OBJETIVO DEL CARGO

Esta posición, de nivel inicial, se encarga de llevar a cabo diversas actividades fundamentales, entre las que se incluyen el monitoreo, la gestión, el soporte y la generación de informes de incidentes. Asimismo, implica el manejo competente de múltiples plataformas de seguridad, como SIEM y SOAR. Además, el rol abarca el respaldo de todas las actividades adicionales necesarias para garantizar una prestación de servicio de monitoreo efectiva y cumplir con las expectativas de los clientes en términos de calidad y oportunidad, asegurando así su plena satisfacción.

PERFIL

El perfil técnico profesional para el cargo de Analista SOC N1 en Datasec SAS, actualmente consta de las siguientes características:

- Formación como Técnico Profesional, Tecnólogo o Ingeniero en formación (últimos semestres) en electrónica, informática, telecomunicaciones, sistemas o afines.

- Experiencia de al menos 6 meses en monitoreo y análisis de eventos de seguridad en entornos de seguridad operacional SOC.

- Conocimiento en sistemas operativos (Windows, Linux), bases de datos, redes de comunicaciones y protocolos de seguridad.

- Conocimiento en herramientas de seguridad de la información como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, entre otros.

- Conocimientos en metodologías de análisis de incidentes de seguridad, gestión de incidentes y respuesta a incidentes.

- Capacidad para generar informes técnicos y comunicar de forma clara y efectiva los hallazgos de seguridad encontrados.

- Habilidad para realizar análisis de incidentes de seguridad.

- Conocimientos básicos en lenguajes de programación y scripting.

HABILIDADES

El desempeño del cargo de Analista SOC N1 en Datasec SAS exige la posesión de habilidades técnicas específicas en áreas clave de seguridad informática. Es fundamental contar con conocimientos en sistemas operativos (Windows, Linux), bases de datos, redes de comunicaciones y protocolos de seguridad, así como en herramientas de seguridad de la información como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, entre otros. También debe poseer fluidez en tecnologías clave de ciberseguridad y metodologías de ataque.[27]

COMPETENCIAS

Además de contar con las habilidades técnicas el perfil del analista debe estar enriquecido con las siguientes competencias:

- Capacidad de análisis: el analista SOC N1 debe tener la capacidad de analizar moderadas cantidades de datos y utilizar herramientas de seguridad para identificar amenazas y vulnerabilidades. También debe ser capaz de resolver problemas y tomar decisiones en situaciones de presión.

- Comunicación efectiva: el analista SOC N1 debe ser capaz de comunicar claramente los resultados de su análisis de seguridad a otros miembros del equipo para compartir información y colaborar en la identificación y mitigación de amenazas.

- Pensamiento crítico: el analista SOC N1 debe tener la capacidad de analizar y evaluar la información para identificar patrones y tendencias, y utilizar esta información para prevenir futuros ataques.

- Trabajo en equipo: el analista SOC N1 debe ser capaz de trabajar en equipo y colaborar con otros miembros del equipo de seguridad de la información para identificar y mitigar las amenazas de seguridad de las organizaciones clientes de Datasec.

- Innovación y Mejora Continua: el Analista SOC N1 debe demostrar una disposición constante para explorar nuevas soluciones y métodos, contribuyendo así a la evolución continua de las prácticas de seguridad. La capacidad de proponer mejoras significativas en los procesos y sistemas, así como la disposición para adoptar enfoques innovadores en la resolución de problemas, son aspectos fundamentales.

[27] CIO México (2022) Cinco habilidades que un analista SOC debe poseer (Redacción CIO México Disponible en https://cio.com.mx/cinco-habilidades-que-un-analista-de-soc-debe-poseer/

DIAGNOSTICO DEL PERFIL

El cargo de Analista SOC N1 en Datasec refleja un perfil técnico-profesional cuidadosamente diseñado para responder a las exigencias del entorno de seguridad cibernética. La formación académica en electrónica, informática, telecomunicaciones o afines, junto con una experiencia mínima de 6 meses en monitoreo y análisis de eventos de seguridad en entornos SOC, establece una base sólida. Se espera que el analista demuestre conocimientos en sistemas operativos, bases de datos, redes de comunicaciones y protocolos de seguridad, así como en herramientas esenciales de ciberseguridad.

El listado de habilidades resalta la importancia de la fluidez en tecnologías clave de ciberseguridad y la capacidad para aplicar metodologías de ataque. Además de las habilidades técnicas, se subraya la necesidad de competencias específicas, como la capacidad analítica para abordar moderadas cantidades de datos y la toma de decisiones bajo presión. La habilidad para comunicar claramente hallazgos de seguridad, el pensamiento crítico para identificar patrones y tendencias, y la colaboración efectiva en equipos de seguridad de la información son elementos cruciales. La inclusión de la competencia en Innovación y Mejora Continua destaca la importancia de fomentar un enfoque proactivo hacia la evolución continua de las prácticas de seguridad.

6.2.2 ANALISTA SOC N2

OBJETIVO DEL CARGO

Esta posición demanda una experiencia más avanzada en comparación con el Analista N1, y conlleva mayores responsabilidades. Los Analistas N2 desempeñan un papel fundamental al investigar y gestionar respuestas a incidentes de seguridad, al mismo tiempo que colaboran en el desarrollo y la mejora continua de los procesos de seguridad en la organización. Por lo general, este cargo es asumido por Analistas N1 que han demostrado un destacado desempeño en sus responsabilidades anteriores.

PERFIL

El perfil técnico profesional para el cargo de Analista SOC N2 en Datasec SAS, actualmente consta de las siguientes características:

- Formación académica en ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica, seguridad informática o carreras afines.

- Experiencia de al menos año en resolución y análisis de eventos de seguridad en entornos de seguridad operacional SOC.

- Conocimiento en sistemas operativos (Windows, Linux, AIX), bases de datos, redes de comunicaciones y protocolos de seguridad y redes.

- Conocimiento en herramientas de seguridad de la información como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, SANDBOX y SOAR.

- Conocimientos en metodologías de análisis de incidentes de seguridad, gestión de incidentes y respuesta a incidentes.

- Conocimiento práctico de los datos relevantes para la seguridad, incluidos los protocolos de red, los puertos y los servicios estándar, como los protocolos de red TCP/IP y los protocolos de la capa de aplicación.

- Habilidad para realizar análisis de malware y técnicas de ingeniería inversa.

- Conocimientos básicos en lenguajes de programación y scripting.

- Habilidad en Forense Digital.

HABILIDADES

Se espera que el analista de Nivel 2 cuente con habilidades destacadas al identificar qué datos o sistemas han sido comprometidos, así como la capacidad para proponer acciones de mitigación, respuesta a incidentes y estrategias preventivas. En este sentido, el rol del Analista SOC N2 demanda un conjunto específico de habilidades técnicas y prácticas, esenciales para ejecutar eficientemente las funciones de monitoreo, detección y respuesta a incidentes de seguridad.

Una competencia crucial es la formación académica en disciplinas como ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica, seguridad informática o áreas afines. Estos programas educativos proporcionan la base de conocimientos necesaria para comprender los sistemas y aplicaciones complejas en el entorno de seguridad operacional SOC. Es importante destacar que esta formación no solo fortalece las capacidades del profesional, sino que también suele ser un requisito demandado por los clientes de Datasec.

Otra habilidad esencial requerida para este puesto implica poseer un conocimiento intermedio en sistemas operativos, bases de datos, redes de comunicaciones y protocolos de seguridad. Estos conocimientos son fundamentales para identificar los riesgos potenciales y evaluar de manera efectiva el impacto de posibles ataques.

El Analista SOC Nivel 2 debe estar familiarizado con metodologías de análisis de incidentes de seguridad, gestión de incidentes y respuesta a incidentes, para poder tomar decisiones rápidas y precisas en situaciones críticas. Asimismo, es importante que cuente con habilidades en análisis de datos relevantes para la seguridad, lo que permitirá al analista SOC Nivel 2 identificar patrones y tendencias en los eventos de seguridad. Adicionalmente es deseable que cuente con conocimientos en técnicas forenses[28], específicamente en recolección y manejo de evidencia.

COMPETENCIAS

Se espera que el analista SOC N2 cuente con competencias tales como:

- Capacidad de análisis: el analista SOC N2 debe tener la capacidad de analizar grandes cantidades de datos y utilizar herramientas avanzadas de seguridad para identificar amenazas y vulnerabilidades. También debe ser capaz de resolver problemas y tomar decisiones en situaciones de alta presión.

- Comunicación efectiva: el analista SOC N2 debe ser capaz de comunicar claramente los resultados de su análisis de seguridad a otros miembros del equipo y a los líderes de Datasec. También debe ser capaz de comunicarse eficazmente con clientes para compartir información y colaborar en la identificación y mitigación de amenazas.

- Pensamiento crítico: el analista SOC N2 debe tener la capacidad de analizar y evaluar la información para identificar patrones y tendencias, y utilizar esta información para prevenir futuros ataques y crear estrategias de mitigación.

- Trabajo en equipo: el analista SOC N2 debe ser capaz de trabajar en equipo y colaborar con otros miembros del equipo de seguridad de la información para identificar y mitigar las amenazas de seguridad de las organizaciones clientes de Datasec.

- Resolución de problemas, el analista SOC N2 debe ser capaz de enfrentar situaciones complejas y desarrollar soluciones efectivas en un ambiente de alta presión.

- Capacidad Multitarea: el analista SOC N2 debe ser capaz de realizar tareas tipo multitask y trabajar de manera oportuna y efectiva en la correlación y respuesta ante eventos de seguridad.

[28] MinTic (2016) Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

DIAGNOSTICO DEL PERFIL

El rol de Analista SOC N2 en Datasec se presenta como una posición avanzada que demanda experiencia y habilidades especializadas en seguridad cibernética. Este cargo, con formación académica en disciplinas clave, como ingeniería de sistemas, telecomunicaciones o seguridad informática, debe poseer al menos un año de experiencia en la resolución y análisis de eventos de seguridad en entornos SOC. Las habilidades técnicas requeridas abarcan un espectro amplio, desde el conocimiento profundo en sistemas operativos, bases de datos, redes y protocolos de seguridad, hasta la habilidad para realizar análisis de malware, técnicas de ingeniería inversa y forense digital. Además, se espera que el Analista SOC N2 cuente con competencias avanzadas en análisis de datos y la capacidad para proponer acciones de mitigación, respuesta a incidentes y estrategias preventivas. En términos de competencias, se destaca la necesidad de habilidades analíticas avanzadas, comunicación efectiva tanto con el equipo interno como con los clientes, pensamiento crítico para identificar patrones y tendencias, trabajo colaborativo en equipo, resolución de problemas en entornos de alta presión y capacidad multitarea para gestionar eventos de seguridad de manera oportuna y efectiva.

6.2.3 ANALISTA SOC N3

OBJETIVO DEL CARGO

Es una posición de alto nivel que requiere una amplia experiencia en ciberseguridad. Los Analistas N3 se encargan de liderar la respuesta a incidentes de seguridad críticos y de proporcionar orientación y apoyo técnico a los Analistas N1 y N2. Por lo general, este cargo es asumido por Analistas N2 que han demostrado un destacado desempeño en sus responsabilidades anteriores.

PERFIL

El perfil técnico profesional para el cargo de Analista SOC N3 en Datasec SAS, actualmente consta de las siguientes características:

- Formación académica en ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica, seguridad informática o carreras afines con especialización en seguridad informática.

- Experiencia de al menos 2 años en el área de la ciberseguridad.

- Experiencia en liderazgo de equipos de centro de control, monitoreo, SOC.

- Amplio conocimiento en sistemas operativos (Windows, Linux, AIX), bases de datos, redes de comunicaciones y protocolos de seguridad.

- Conocimiento en herramientas especializadas de seguridad de la información como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, SANDBOX, SOAR, DECEPTORS, NDR.

- Habilidad para realizar análisis de malware y técnicas de ingeniería inversa.

- Conocimientos avanzados en lenguajes de programación y scripting.

- Análisis avanzado forense.

- Certificaciones en Ethical Hacking. NSE5 – NS6.

HABILIDADES

La posición de Analista SOC N3 en Datasec SAS demanda un conjunto avanzado de habilidades técnicas en diversas áreas de la seguridad informática. Se requiere una sólida experiencia previa en liderazgo de equipos de centros de control, monitoreo y SOC. Es esencial poseer un profundo conocimiento en sistemas operativos, bases de datos, redes de comunicaciones y protocolos de seguridad, así como en herramientas especializadas, como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, SANDBOX, SOAR, DECEPTORS y NDR.

Además, se espera que el Analista SOC N3 cuente con habilidades avanzadas para realizar análisis de malware y técnicas de ingeniería inversa, así como conocimientos profundos en lenguajes de programación y scripting. Se valora la experiencia en análisis forense en Host, Incident Handler, Análisis de malware, Threat Intelligence, Detección avanzada de intrusiones, Ethical Hacking avanzado y un sólido dominio de los conocimientos de CISSP.

COMPETENCIAS

Se espera que el analista SOC N3 cuente con competencias tales como:

- Capacidad de análisis: el analista SOC N3 debe tener la capacidad de analizar grandes cantidades de datos y utilizar herramientas avanzadas de seguridad para identificar amenazas y vulnerabilidades. También debe ser capaz de resolver problemas y tomar decisiones en situaciones de alta presión.

- Comunicación efectiva: el analista SOC N3 debe ser capaz de comunicar claramente los resultados de su análisis de seguridad a otros miembros del equipo y a los líderes de Datasec. También debe ser capaz de comunicarse

eficazmente con clientes para compartir información y colaborar en la identificación y mitigación de amenazas.

- Pensamiento crítico: el analista SOC N3 debe tener la capacidad de analizar y evaluar la información para identificar patrones y tendencias, y utilizar esta información para prevenir futuros ataques y crear estrategias de mitigación.

- Trabajo en equipo: el analista SOC N3 debe ser capaz de trabajar en equipo y colaborar con otros miembros del equipo de seguridad de la información para identificar y mitigar las amenazas de seguridad de las organizaciones clientes de Datasec.

- Resolución de problemas, el analista SOC N3 debe ser capaz de enfrentar situaciones complejas y desarrollar soluciones efectivas en un ambiente de alta presión.

- Capacidad Multitarea: el analista SOC N3 debe ser capaz de realizar tareas tipo multitask y trabajar de manera oportuna y efectiva en la correlación y respuesta ante eventos de seguridad.

- Liderazgo y habilidades para la gestión de equipos: el analista SOC N3 debe ser capaz de liderar y supervisar procesos y técnicas en su equipo de trabajo, por lo que es necesario contar con habilidades de liderazgo, comunicación y trabajo en equipo colaborativo.

- Capacidad para tomar decisiones: el analista SOC N3 debe ser capaz de responsabilizarse de la toma decisiones importantes en relación con la ciberseguridad de las organizaciones clientes, por lo que es necesario contar con habilidades de análisis y resolución de problemas para tomar decisiones efectivas.

DIAGNOSTICO DEL PERFIL

El perfil de Analista SOC N3 en Datasec SAS demanda un profesional altamente experimentado en ciberseguridad, con una sólida formación académica y al menos dos años de experiencia en el campo. Este analista se debe destacar por liderar la respuesta a incidentes críticos de seguridad, proporcionar orientación técnica a Analistas N1 y N2, y contribuir significativamente al desarrollo y mejora continua de los procesos de seguridad en la organización. Se espera que posea conocimientos avanzados en diversas áreas, desde sistemas operativos y bases de datos hasta herramientas especializadas como firewalls, IDS/IPS, SIEM, y habilidades avanzadas en análisis forense y técnicas de ingeniería inversa. Además, debe contar con certificaciones en Ethical Hacking y habilidades demostradas en liderazgo, gestión de equipos, toma de decisiones y resolución de problemas en

entornos de alta presión. Este analista desempeña un papel crucial en la identificación y mitigación de amenazas, contribuyendo significativamente a la seguridad de las organizaciones clientes de Datasec.

6.2.4 LIDER BLUE TEAM

OBJETIVO DEL CARGO

Es el líder del equipo de seguridad defensiva de la organización. Se encarga de llevar a cabo pruebas de penetración y simulaciones de ataques para identificar vulnerabilidades en los sistemas y mejorar las defensas de la organización. Si se requiere una persona para dicho cargo, se buscaría entre los Analistas N3 que hayan demostrado un destacado desempeño en sus responsabilidades anteriores.

PERFIL

El perfil técnico profesional para el cargo de Líder Blue Team en Datasec SAS, actualmente consta de las siguientes características:

- Formación académica en ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica, seguridad informática o carreras afines con especialización en seguridad informática.

- Experiencia de al menos 3 años en el área de la ciberseguridad.

- Amplio conocimiento en sistemas operativos (Windows, Linux), bases de datos, redes de comunicaciones y protocolos de seguridad.

- Experiencia en dirección y liderazgo de equipos de centro de operaciones de ciberseguridad, CSOC.

- Conocimiento en implementación y configuración de soluciones de seguridad, tales como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), herramientas de Correlación de eventos, SIEM, SOAR, SANDBOX, DECEPTORS.

- Habilidad para realizar análisis de malware y técnicas de ingeniería inversa.

- Experiencia en auditoria, exploración de vulnerabilidades de la red interna o externa.
- Conocimientos en metodologías de análisis de incidentes de seguridad, gestión de incidentes y respuesta a incidentes.

- Certificación vigente como auditor SGSI ISO 27001 – NS6 - NSE7.

HABILIDADES

Es necesario que el líder Blue Team, sea un profesional que tenga una amplia experiencia en seguridad de la información y en la gestión de equipos de trabajo, habilidades propias de un líder Blue Team. Entre las habilidades técnicas, el candidato debe tener un conocimiento profundo y muy avanzado de las tecnologías de seguridad y las herramientas de monitoreo y análisis de amenazas. Debe conocer las técnicas de ataque y defensa, así como las vulnerabilidades y amenazas más comunes en las redes y sistemas informáticos. También debe tener conocimiento en la implementación y configuración de soluciones de seguridad, tales como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) y tener experiencia en análisis forense en Host, Incident Handler, Análisis de malware, Threat Intelligence, Detección avanzada de intrusiones, Ethical Hacking avanzado, y dominios de conocimiento de CISSP. Además, debe tener habilidades en procesos de auditorías de seguridad en una organización para verificar que los sistemas de información y procesos siempre cumplan con los estándares de ciberseguridad establecidos.

COMPETENCIAS

Se espera que el líder Blue Team cuente con competencias tales como:

- Comunicación efectiva: el líder Blue Team debe ser capaz de comunicar claramente los objetivos a alcanzar a todo el equipo de trabajo.

- Resolución de problemas, el líder Blue Team debe ser capaz de enfrentar situaciones estratégicas y desarrollar soluciones efectivas para satisfacer las necesidades de las organizaciones demandantes de servicios de ciberseguridad.

- Liderazgo y habilidades para la gestión de equipos: el líder Blue Team debe ser capaz de liderar y supervisar procesos y técnicas en su equipo de trabajo, por lo que es necesario contar con habilidades de liderazgo, comunicación y trabajo en equipo colaborativo.

- Capacidad para tomar decisiones: el líder Blue Team debe ser el responsable de la toma decisiones importantes en relación con las metas y objetivos del centro de operaciones de ciberseguridad y velar por el cumplimiento de los ANS comprometidos con las organizaciones clientes, por lo que es necesario contar con habilidades de análisis y resolución de problemas para tomar decisiones efectivas.

- Motivador nato: el líder Blue Team debe ser capaz de mantener al equipo comprometido y enfocado en los objetivos de seguridad. Debe ser capaz de

inspirar y motivar a los miembros del equipo para que se sientan involucrados y comprometidos en el trabajo que realizan.

- Ética profesional: el líder Blue Team debe ser capaz de garantizar la integridad y confidencialidad de la información y los sistemas de la organización. Debe comprender la importancia de la privacidad y la seguridad de los datos, así como de la responsabilidad que tiene en el manejo de la información

DIAGNOSTICO DEL PERFIL

El perfil de Líder Blue Team en Datasec SAS demanda un profesional con una sólida formación académica en campos relacionados con la seguridad informática, respaldada por al menos 3 años de experiencia en ciberseguridad. Este líder es crucial para la organización, encabezando el equipo de seguridad defensiva y llevando a cabo pruebas de penetración y simulaciones de ataques para fortalecer las defensas. El perfil busca a individuos con conocimientos avanzados en sistemas operativos, bases de datos, redes y protocolos de seguridad, así como experiencia en liderar equipos de centro de operaciones de ciberseguridad SOC. La habilidad para realizar análisis de incidentes, técnicas de ingeniería inversa, y poseer certificaciones vigentes como auditor SGSI ISO 27001 – NS6 - NSE7 son esenciales. Además de las habilidades técnicas, se destaca la necesidad de habilidades de liderazgo excepcionales, fuertes capacidades comunicativas, resolución de problemas estratégicos, toma de decisiones, motivación del equipo y un fuerte compromiso con la ética profesional.

6.2.5 INGENIERO DE SEGURIDAD N1

OBJETIVO DEL CARGO

Este perfil se enfoca en la configuración y el mantenimiento de sistemas de seguridad, tales como firewalls y sistemas de detección de intrusiones. Asimismo, se encarga de llevar a cabo tareas de monitoreo, gestión, soporte y generación de informes sobre incidentes en diversas plataformas de seguridad, incluyendo SIEM, SOAR, así como plataformas de gestión de vulnerabilidades y evaluación de riesgos. Normalmente, este rol es asumido por Analistas N1 que han demostrado un rendimiento óptimo en sus responsabilidades anteriores.

PERFIL

El perfil técnico profesional para el cargo de Ingeniero de seguridad N1 en Datasec SAS, actualmente consta de las siguientes características:

- Formación académica en ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica, seguridad informática o carreras afines.

- Experiencia de al menos 1 años en el área de la ciberseguridad.

- Conocimiento en implementación y configuración de soluciones de seguridad, tales como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), herramientas de Correlación de eventos, SIEM, SOAR, SANDBOX, DECEPTORS.

- Conocimiento práctico de los datos relevantes para la seguridad, incluidos los protocolos de red, los puertos y los servicios estándar, como los protocolos de red TCP/IP y los protocolos de la capa de aplicación.

- Conocimientos en Linux y Power Shell.

- Análisis y control de vulnerabilidades.

- Conocimiento de esquemas de seguridad se manera Onpremise y Nube.

- Conocimientos básicos en plataformas en la nube.

- Certificaciones NSE4 e ITIL.

HABILIDADES

Para desempeñarse como Ingeniero de seguridad N1 en Datasec SAS, se requiere contar con habilidades técnicas en diversas áreas de la seguridad informática.

El ingeniero de seguridad N1 debe tener formación académica en áreas relacionadas con la seguridad informática, como ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica o carreras afines.

Es esencial que cuente con conocimientos técnicos en la implementación y configuración de soluciones de seguridad, como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS).

Además, debe poseer un conocimiento práctico de los protocolos de red, los puertos y los servicios estándar, como los protocolos de red TCP/IP y los protocolos de la capa de aplicación. Es importante que tenga habilidades en Linux y Power Shell para la automatización de tareas de seguridad y la gestión de grandes cantidades de datos.

Debe contar con experiencia en esquemas de seguridad Onpremise y Cloud, ademan de contar con habilidades en la gestión, configuración, administración y monitoreo de dispositivos de seguridad, de preferencia dispositivos FortiGate[29]

COMPETENCIAS

Se espera que el ingeniero de seguridad N1 cuente con competencias tales como:

- Resolución de problemas: el ingeniero de seguridad N1 debe ser capaz de enfrentar situaciones estratégicas y de utilizar las mejores prácticas en la implementación de soluciones de seguridad y demostrar destreza en las herramientas de seguridad relevantes.

- Trabajo en equipo: el ingeniero de seguridad N1 debe contar con competencias trabajando equipo y colaborar con otros miembros del equipo de seguridad de la información para identificar y mitigar las amenazas de seguridad de las organizaciones clientes de Datasec.

- Proactividad: además de responder a incidentes de seguridad, el ingeniero de seguridad N1 debe estar en la capacidad de idear soluciones para prevenir posibles amenazas, por lo que es importante que sea proactivo y demuestre anticipación en sus labores.

- Pensamiento crítico: el ingeniero de seguridad N1 debe tener la capacidad de analizar y evaluar la información para identificar patrones y tendencias, y utilizar esta información para prevenir futuros ataques.

- Innovación y Mejora Continua: el ingeniero de seguridad N1 debe demostrar una disposición constante para explorar nuevas soluciones y métodos, contribuyendo así a la evolución continua de las prácticas de seguridad. La capacidad de proponer de manera efectiva mejoras sustanciales en los procesos y sistemas existentes. Además, es esencial mostrar una disposición activa hacia la adopción de enfoques innovadores al abordar y resolver problemas. Este enfoque dinámico no solo implica identificar oportunidades de mejora, sino también estar abierto a la implementación de soluciones creativas y vanguardistas.

[29] Fortinet training institute Fortigate Security. Course description https://training.fortinet.com/local/staticpage/view.php?page=library_fortigate-security

DIAGNOSTICO DEL PERFIL

El perfil para Ingeniero de Seguridad N1 en Datasec debe destacar por su formación académica sólida en áreas fundamentales de la seguridad informática y una experiencia mínima de un año en el campo de la ciberseguridad. Posee conocimientos especializados en la implementación y configuración de soluciones de seguridad, abarcando desde firewalls hasta sistemas de detección de intrusiones, y demuestra habilidades prácticas en la gestión de datos relevantes para la seguridad. Su destreza técnica abarca protocolos de red, Linux, Power Shell, y certificaciones NSE4 e ITIL. Este perfil se distingue por su capacidad para abordar desafíos estratégicos, trabajar eficazmente en equipo y aplicar las mejores prácticas en la implementación de soluciones de seguridad. Además, muestra una actitud proactiva al anticiparse a amenazas potenciales y demuestra habilidades de pensamiento crítico para analizar patrones y tendencias. Su disposición constante hacia la innovación y mejora continua lo posiciona como un activo valioso para evolucionar las prácticas de seguridad en Datasec.

6.2.6 INGENIERO DE SEGURIDAD N2

OBJETIVO DEL CARGO

Es un puesto de nivel más alto que el Ingeniero de Seguridad N1 y tiene más responsabilidades. El Ingeniero de Seguridad N2 se encarga de diseñar e implementar soluciones de seguridad más complejas y de liderar proyectos de seguridad. Por lo general, este cargo es asumido por Ingenieros de Seguridad N1 que han demostrado un destacado desempeño en sus responsabilidades anteriores.

PERFIL

El perfil técnico profesional para el cargo de Ingeniero de seguridad N2 en Datasec SAS, actualmente consta de las siguientes características:

- Formación académica en ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica, seguridad informática o carreras afines.

- Experiencia de al menos 2 años en el área de la ciberseguridad.

- Conocimientos técnicos en la implementación y configuración de soluciones de seguridad, como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS).

- Conocimientos Linux, Python y Power Shell.

- Conocimiento de esquemas de seguridad se manera Onpremise y Nube
- Experiencia en seguridad en plataformas en la nube.
- Administración y personalización controles de eventos .
- Experiencia en gestión, configuración, administración y monitoreo de dispositivos Fortinet y Palo Alto.
- Habilidad para realizar análisis de malware y técnicas de ingeniería inversa.
- Certificaciones en NSE 7

HABILIDADES

Para desempeñarse como Ingeniero de seguridad N2 en Datasec SAS, se requiere contar con habilidades técnicas en diversas áreas de la seguridad informática.

El Ingeniero de seguridad N2 debe contar con formación académica en áreas relacionadas con la seguridad informática, como ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica o carreras afines, y poseer conocimientos certificados en Fortinet como NSE7.

Además, debe contar con habilidades avanzadas en la implementación y configuración de soluciones de seguridad, como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS). Conocimientos avanzados en redes, Ethical Hacking, habilidad en Forense Digital. Debe tener experiencia en la administración de protocolos de red, puertos y servicios estándar, así como en la automatización de tareas de seguridad y la gestión de grandes cantidades de datos.

También se requiere una capacidad demostrada para gestionar soluciones de prevención control de vulnerabilidades y conocimientos de esquemas de seguridad tanto Onpremise como en la nube y contar con habilidades técnicas en ingeniería inversa.

COMPETENCIAS

Se espera que el ingeniero de seguridad N2 cuente con competencias tales como:

- Comunicación efectiva: es importante que pueda comunicar de manera clara y concisa, tanto oralmente como por escrito, para poder transmitir información técnica a personas no especializadas en el área de la ciberseguridad.

- Trabajo en equipo: debe ser capaz de trabajar en equipo, colaborar y coordinar con otros miembros del equipo de seguridad, así como con otras áreas de la empresa para garantizar la implementación efectiva de las soluciones de seguridad.

- Adaptabilidad: debe ser capaz de adaptarse a cambios constantes en el entorno de la ciberseguridad, tales como nuevas amenazas, tecnologías emergentes y requisitos del cliente.

- Pensamiento crítico: debe ser capaz de analizar situaciones y problemas de manera crítica, identificando y evaluando alternativas de solución.

- Toma de decisiones: debe ser capaz de tomar decisiones rápidas y efectivas, basadas en datos y análisis de riesgos.

- Orientación al cliente: debe tener una actitud de servicio hacia el cliente, comprendiendo sus necesidades y expectativas y trabajando para satisfacerlas de manera efectiva.

- Responsabilidad: debe ser responsable y comprometido con su trabajo, cumpliendo con los plazos y entregables establecidos.

DIAGNOSTICO DEL PERFIL

El perfil del Ingeniero de Seguridad N2 en Datasec asume un papel estratégico con mayores responsabilidades, demostrando un sólido respaldo académico y una experiencia mínima de 2 años en ciberseguridad. Su enfoque se orienta hacia el diseño e implementación de soluciones de seguridad complejas, así como el liderazgo de proyectos en esta área. Con conocimientos técnicos certificados en Fortinet (NSE7), este profesional destaca por sus habilidades avanzadas en la configuración de firewalls, sistemas de detección de intrusiones y prevención de intrusiones, así como en el manejo de Linux, Python y Power Shell. Su competencia se extiende a la seguridad en entornos de nube, gestión de dispositivos Fortinet y Palo Alto, análisis de malware, ingeniería inversa y habilidades avanzadas en forense digital. Además, exhibe competencias en comunicación efectiva, trabajo en equipo, adaptabilidad a cambios, pensamiento crítico y toma de decisiones. Su orientación al cliente y responsabilidad son evidentes, lo que refleja su compromiso con la satisfacción del cliente y la entrega puntual de resultados. En conjunto, el perfil de Ingeniero de Seguridad N2 se presenta como un cargo altamente capacitado y comprometido con las demandas dinámicas del entorno de ciberseguridad en Datasec.

6.2.7 PERFIL DE CARGO LIDER DE INGENIERIA

OBJETIVO DEL CARGO

Es el líder del equipo de ingeniería de seguridad de la organización Datasec SAS. Se encarga de planificar y ejecutar proyectos de seguridad más complejos y de supervisar el trabajo de los Ingenieros de Seguridad. Si se requiere una persona para dicho cargo, se buscaría entre los ingenieros de Seguridad N2 que hayan demostrado un destacado desempeño en sus responsabilidades anteriores.

PERFIL

El perfil técnico profesional para el cargo de Líder de Ingeniería en Datasec SAS, actualmente consta de las siguientes características:

- Formación académica en ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica, seguridad informática o carreras afines.

- Especialización en seguridad informática o gerencia de proyectos.

- Experiencia de al menos 3 años en gestión, planificación y desarrollo de proyectos en el área de seguridad o comunicaciones

- Conocimiento profundo en herramientas de seguridad de la información como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, entre otros.

- Conocimientos en metodologías de análisis gestión y respuesta de incidentes.

- Habilidades en dirección y liderazgo de equipos de centro de operaciones de ciberseguridad, CSOC.

- Experiencia en gestión, configuración, administración y monitoreo de dispositivos de seguridad.

- Certificaciones en NSE 8

HABILIDADES

El líder de ingeniería de seguridad debe ser un profesional con amplia experiencia en seguridad de la información y en la gestión de equipos de trabajo. Es fundamental que tenga un conocimiento avanzado de las tecnologías de seguridad,

así como de las herramientas de monitoreo y análisis de amenazas. Además, debe estar familiarizado con las técnicas de ataque y defensa, y ser capaz de identificar las vulnerabilidades y amenazas más comunes en las redes y sistemas informáticos.

Es esencial que tenga habilidades técnicas en la implementación y configuración de soluciones de seguridad, incluyendo firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS). También es importante que tenga experiencia en análisis forense en Host, Incident Handler, Análisis de malware, Threat Intelligence, Detección avanzada de intrusiones, Ethical Hacking avanzado, y conocimientos en los dominios de CISSP. Además, debe estar certificado en NSE 8, tener capacidad para responder de manera inmediata a las consultas sobre incidentes de seguridad y ser el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder presentarlos a los clientes.

COMPETENCIAS

- Comunicación efectiva: El líder de ingeniería debe tener habilidades de comunicación efectiva para poder transmitir claramente los objetivos y resultados de la gestión tanto a su equipo de trabajo como a los clientes finales. Es necesario que cuente con capacidad de adaptación de mensajes a diferentes audiencias y canales de comunicación.

- Resolución de problemas: El líder de ingeniería debe ser capaz de enfrentar situaciones estratégicas y desarrollar soluciones efectivas para satisfacer las necesidades de las organizaciones demandantes de servicios de seguridad cibernética. Es esencial que cuente con habilidades analíticas avanzadas y pueda aplicar técnicas de solución de problemas para enfrentar situaciones complejas.

- Liderazgo y gestión de equipos: El líder de ingeniería debe tener habilidades de liderazgo y gestión de equipos para liderar y supervisar procesos y técnicas en su equipo de trabajo. Es necesario que tenga la capacidad de motivar y guiar al equipo hacia la consecución de objetivos y metas, fomentando la colaboración y el trabajo en equipo.

- Toma de decisiones: El líder de ingeniería es responsable de tomar decisiones importantes en relación con las metas y objetivos del centro de operaciones de seguridad cibernética y velar por el cumplimiento de los acuerdos de nivel de servicio comprometidos con los clientes. Para tomar decisiones efectivas, debe contar con habilidades de análisis y resolución de problemas.

- Empatía: Debe estar en la capacidad de comprender las perspectivas y necesidades de su equipo y de los usuarios de la tecnología de la organización además de ponerse en el lugar de los demás y comprender sus emociones y preocupaciones para tomar decisiones justas y equilibradas.

- Ética profesional: El líder de ingeniería debe garantizar la integridad y confidencialidad de la información y los sistemas de la organización que lidera. Es esencial que cuente con un fuerte sentido de ética profesional y comprenda la importancia de la privacidad y la seguridad de los datos, así como la responsabilidad que tiene en el manejo de la información. Además, debe cumplir con los estándares éticos y legales en su trabajo y tomar decisiones justas y equilibradas en situaciones complejas.

DIAGNOSTICO DEL PERFIL

El perfil para Líder de Ingeniería en Datasec desempeña un papel esencial como director del equipo de ingeniería de seguridad, encargado de la planificación y ejecución de proyectos de seguridad avanzados. Con una sólida formación académica en áreas clave como ingeniería de sistemas o seguridad informática, respaldada por una especialización en seguridad informática o gerencia de proyectos, este líder demuestra una experiencia considerable de al menos 3 años en la gestión, planificación y desarrollo de proyectos en seguridad y comunicaciones.

El perfil destaca habilidades técnicas avanzadas, incluyendo un conocimiento profundo en herramientas de seguridad como firewalls, IDS/IPS, análisis de vulnerabilidades y SIEM. La certificación NSE 8 respalda su experiencia y competencia en la implementación y configuración de soluciones de seguridad, y su capacidad para liderar equipos de ingenieros de seguridad. Además, posee habilidades probadas en análisis forense, Threat Intelligence, Ethical Hacking avanzado y conocimientos en los dominios de CISSP.

Este perfil de líder de ingeniería no solo sobresale en habilidades técnicas, sino que también exhibe competencias clave, como una comunicación efectiva para transmitir claramente los objetivos a su equipo y clientes, resolución de problemas estratégicos, liderazgo efectivo y toma de decisiones informadas. Su empatía y ética profesional reflejan su capacidad para comprender las necesidades de su equipo y los usuarios, así como para tomar decisiones justas y equilibradas en situaciones complejas. En resumen, el Líder de Ingeniería en Datasec se presenta como un profesional integral con las habilidades y experiencia necesarias para dirigir con éxito proyectos de seguridad avanzados y liderar un equipo altamente capacitado.

6.2.8 PERFIL DE CARGO LIDER SOC

OBJETIVO DEL CARGO

El Líder SOC en Datasec SAS despliega un rol estratégico fundamental en la gestión integral de la seguridad cibernética. Su principal objetivo es liderar y coordinar todas las actividades del Centro de Operaciones de Seguridad (SOC), asegurando la detección, respuesta y mitigación eficaz de las amenazas de seguridad para las organizaciones clientes. Además, debe desplegar una visión integral de la ciberseguridad, asegurando la alineación de las operaciones del SOC con los objetivos de seguridad y las necesidades del negocio, supervisando el desempeño del equipo, facilitando de esta manera el cumplimiento de los estándares de calidad y promoviendo la mejora continua de los procesos y prácticas de seguridad.

PERFIL

El perfil técnico profesional para el cargo de Líder SOC en Datasec SAS, actualmente consta de las siguientes características:

- Formación académica en ingeniería de sistemas, ingeniería en telecomunicaciones, ingeniería electrónica, seguridad informática o carreras afines.

- Especialización en seguridad informática o gerencia de proyectos.

- Experiencia de al menos 4 años en el campo de la seguridad cibernética, con un enfoque específico en la operación y gestión de Centros de Operaciones de Seguridad (SOC) así como en gestión, planificación y desarrollo de proyectos en el área de seguridad. Se espera que haya ocupado roles progresivos de responsabilidad y liderazgo en proyectos de seguridad cibernética.

- Conocimientos profundos en sistemas operativos, redes, bases de datos, protocolos de seguridad, y herramientas de seguridad de la información como firewalls, IDS/IPS, SIEM, análisis de vulnerabilidades, entre otros. También se valorará la experiencia en técnicas avanzadas de detección y respuesta a amenazas, así como en análisis forense digital.

- Habilidades sólidas de liderazgo y gestión de equipos. Debe ser capaz de motivar, guiar y desarrollar al equipo del SOC, fomentando un ambiente de trabajo colaborativo y de alto rendimiento.

- Debe ser capaz de transmitir claramente los objetivos, procedimientos y resultados del SOC a diferentes audiencias, incluyendo el equipo interno, los líderes de la organización y los clientes.

- Mentalidad orientada a resultados, con la capacidad de establecer y cumplir objetivos y metas de seguridad cibernética. Debe ser capaz de gestionar eficazmente los recursos y tomar medidas para garantizar la eficiencia operativa y la efectividad en la respuesta a incidentes.

- Experiencia en gestión, configuración, administración e implementación de dispositivos de seguridad.

- Certificaciones en NSE 5, EJPT e ISO/IEC:27001

HABILIDADES

El Líder SOC debe destacarse por sus habilidades excepcionales de liderazgo y gestión de equipos. Debe ser capaz de inspirar confianza, motivar al equipo y promover un ambiente de trabajo colaborativo y productivo. Además, debe tener habilidades para la toma de decisiones estratégicas, la resolución de problemas y la gestión de conflictos, garantizando que el equipo del SOC esté preparado para enfrentar los desafíos de seguridad de manera efectiva y eficiente.

Asimismo, se requiere que el Líder SOC de Datasec SAS, posea habilidades avanzadas de comunicación tanto verbal como escrita. Debe ser capaz de transmitir claramente los objetivos, procedimientos y resultados del SOC a diferentes audiencias, incluyendo el equipo interno, los líderes de la organización y los clientes. Además, debe tener habilidades para la negociación y la persuasión, así como para la presentación de informes técnicos y análisis de seguridad de manera comprensible para audiencias no técnicas.

COMPETENCIAS

- Comunicación efectiva: El líder de ingeniería debe tener habilidades de comunicación efectiva para poder transmitir claramente los objetivos y resultados de la gestión tanto a su equipo de trabajo como a los clientes finales. Es necesario que cuente con capacidad de adaptación de mensajes a diferentes audiencias y canales de comunicación.

- Resolución de problemas: El líder SOC debe ser capaz de enfrentar situaciones estratégicas y desarrollar soluciones efectivas para satisfacer las necesidades de las organizaciones demandantes de servicios de monitoreos, análisis, contención y respuestas ante incidentes de seguridad cibernética.

Es esencial que cuente con habilidades analíticas avanzadas y pueda aplicar técnicas de solución de problemas para enfrentar situaciones complejas.

- Liderazgo y gestión de equipos: El líder SOC debe tener habilidades de liderazgo y gestión de equipos para liderar y supervisar procesos y técnicas en su equipo de trabajo. Es necesario que tenga la capacidad de motivar y guiar al equipo hacia la consecución de objetivos y metas, fomentando la colaboración y el trabajo en equipo y la resolución de conflictos.

- Toma de decisiones: El líder SOC es responsable de tomar decisiones importantes en relación con las metas y objetivos del centro de operaciones de seguridad cibernética y velar por el cumplimiento de los acuerdos de nivel de servicio comprometidos con los clientes. Para tomar decisiones efectivas, debe contar con habilidades de análisis y resolución de problemas.

- Empatía: Debe estar en la capacidad de comprender las perspectivas y necesidades de su equipo, de los usuarios de la tecnología de la organización y de los clientes, además de ponerse en el lugar de los demás , conectar con ellos y comprender sus emociones y preocupaciones para tomar decisiones justas y equilibradas.

- Ética profesional: El líder de ingeniería debe garantizar la integridad y confidencialidad de la información y los sistemas de la organización que lidera. Es esencial que cuente con un fuerte sentido de ética profesional y comprenda la importancia de la privacidad y la seguridad de los datos, así como la responsabilidad que tiene en el manejo de la información. Además, debe cumplir con los estándares éticos y legales en su trabajo y tomar decisiones justas y equilibradas en situaciones complejas.

DIAGNOSTICO DEL PERFIL

El líder SOC en Datasec SAS es un profesional altamente capacitado con experiencia en ciberseguridad y liderazgo de equipos. Con habilidades técnicas avanzadas en seguridad de la información, comunicación efectiva y resolución de problemas, este líder dirige la operación del Centro de Operaciones de Seguridad, garantizando la protección de los activos de la organización y la satisfacción de los clientes. Su ética profesional, empatía y capacidad de liderazgo son fundamentales para mantener al equipo comprometido y enfocado en los objetivos de seguridad.

6.3 LO QUE ESPERA LA EMPRESA

Datasec es una compañía reconocida como líder en el mercado colombiano en lo que respecta a ciberseguridad. Su compromiso con la excelencia en el servicio y su visión de negocio la impulsan constantemente a buscar perfiles de profesionales especializados en esta área. En particular, la empresa está interesada en incorporar profesionales para su centro de operaciones de Ciberseguridad que estén capacitados y cuenten con habilidades técnicas y competencias analíticas y altamente desarrolladas para fortalecer su equipo y ofrecer a sus clientes una protección eficaz contra las amenazas cibernéticas.

Los diagnósticos previos de habilidades y competencias, conformados a partir de los perfiles destinados a las diversas posiciones dentro del Centro de Operaciones de Seguridad (SOC), han sido elaborados mediante la colaboración entre el Líder del equipo SOC, la líder del equipo de Calidad y la alta gerencia de Datasec. Estos diagnósticos han sido fundamentales para el desarrollo y perfeccionamiento del modelo de gestión de servicios en ciberseguridad que la empresa ofrece a sus clientes, tanto del sector privado como público en Colombia. En su constante búsqueda por ser un referente en la protección de activos e intereses de las organizaciones, Datasec se erige como pionera en este ámbito.

Como líder innovador, Datasec se esfuerza continuamente por mantenerse a la vanguardia de las últimas tendencias y tecnologías en seguridad informática. Este compromiso no solo busca resguardar los activos e intereses de sus clientes, sino también contribuir activamente al fortalecimiento de la ciberseguridad en el país. La empresa reconoce la importancia crucial de contar con un equipo altamente capacitado, poseedor de habilidades y competencias específicas en el ámbito de la ciberseguridad, para alcanzar con éxito estos objetivos fundamentales.

El análisis de perfiles para las distintas posiciones en el Centro de Operaciones de Seguridad (SOC) de Datasec, que comprende la identificación de habilidades y conocimientos esenciales, sienta las bases de manera sólida para la creación de un plan de capacitación en los fundamentos de ciberseguridad. Este enfoque permitirá desarrollar un programa de formación dirigido tanto al personal existente en Datasec como a posibles candidatos para el rol de Analista SOC N1, guiándolos hacia una integración exitosa en el ámbito laboral de la ciberseguridad. Al alinear de manera precisa las necesidades de la empresa respecto al perfil deseado para las posiciones en el SOC con el programa de formación, se facilita una preparación más efectiva y específica. Este enfoque estratégico no solo responde de manera más efectiva al desafío de satisfacer la creciente demanda de profesionales en el Centro de Operaciones de Seguridad de DataSec SAS, sino que también desempeña un papel esencial en el fortalecimiento continuo del SOC.

7. MODELO DE COMPETENCIAS: HABILIDADES Y CONOCIMIENTOS NECESARIOS EN CIBERSEGURIDAD.

Para Datasec SAS, resulta crucial identificar las habilidades técnicas y competencias críticas necesarias para los roles vinculados a su Centro de Operaciones de Seguridad (SOC), siempre enfocándose en alinearlas con las expectativas y necesidades actuales de las organizaciones. Utilizar como referencia modelos de competencias elaborados por expertos en la materia se convierte en un recurso indispensable para obtener información clave y construir un mapa detallado y confiable de las competencias requeridas en el ámbito de la ciberseguridad. Este conocimiento será fundamental para determinar las habilidades y conocimientos esenciales que se integrarán en el plan de capacitación en ciberseguridad, orientado a la formación del personal en el Centro de Operaciones de Seguridad SOC de la empresa DataSec SAS.

7.1 MODELO DE COMPETENCIAS EN CIBERSEGURIDAD: LO QUE OPINAN LOS EXPERTOS

La Oficina de Administración de Personal (OPM) de los Estados Unidos, el Consejo de Directores de Información (CIO) y el Subcomité de Desarrollo de la Fuerza Laboral del Consejo de Directores de Capital Humano trabajaron en un modelo[30] de competencia en ciberseguridad. Se realizó mediante un estudio a nivel gubernamental para identificar las competencias críticas para el trabajo en ciberseguridad, para ello, los empleados y supervisores de todo el gobierno completaron encuestas para obtener un cuadro completo del trabajo en ciberseguridad.

Gracias a dicho modelo de competencia en ciberseguridad, se puede tener una planificación de la fuerza laboral optima, formación y desarrollo adecuados en el campo, mejorar la gestión del rendimiento y el reclutamiento selección en el campo de la ciberseguridad. Utilizar este modelo de competencias como base proporciona un punto de partida sólido para la creación de una ruta de aprendizaje y formación en los fundamentos de la ciberseguridad. A continuación, se detallan algunas de las competencias técnicas en ciberseguridad que se esperan de un profesional, basándonos en este modelo.

Gestión de la Seguridad de las Comunicaciones. Conocimiento de los principios, políticas y procedimientos involucrados en garantizar la seguridad de los servicios y datos de comunicaciones, y en mantener el entorno de comunicaciones en el que reside.

[30] Berry, J. (2011). Competency Model for Cybersecurity. U.S. Office of Personnel Management (OPM). Disponible en https://www.chcoc.gov/content/competency-model-cybersecurity.

Cumplimiento. Conocimiento de los procedimientos para evaluar y monitorear programas o proyectos para el cumplimiento de las leyes, regulaciones y orientación federales.

Informática Forense. Conocimiento de herramientas y técnicas utilizadas en la recuperación de datos y la preservación de evidencia electrónica.

Lenguajes de Informática. Conocimiento de los lenguajes de informática y sus aplicaciones para permitir que un sistema realice funciones específicas.

Defensa de la Red Informática. Conocimiento de medidas defensivas para detectar, responder y proteger información, sistemas de información y redes de amenazas.

Computadoras y Electrónica. Conocimiento de las placas de circuito eléctrico, procesadores, chips, hardware y software de computadora, incluidas las aplicaciones y la programación.

Gestión de la Configuración. Conocimiento de los principios y métodos para planificar o administrar la implementación, actualización o integración de componentes de sistemas de información.

Análisis Costo-Beneficio. Conocimiento de los principios y métodos del análisis costo-beneficio, incluido el valor del tiempo del dinero, los conceptos de valor presente y la cuantificación de beneficios tangibles e intangibles.

Investigación Criminal. Conocimiento de las pautas, regulaciones y procedimientos asociados con la investigación criminal, incluida la detección y manipulación de pruebas y la realización de inferencias y conclusiones fácticas apropiadas.

Gestión de Datos. Conocimiento de los principios, procedimientos y herramientas de gestión de datos, como técnicas de modelado, copia de seguridad de datos, recuperación de datos, diccionarios de datos, almacenamiento de datos, minería de datos, disposición de datos y procesos de estandarización de datos.

Administración de Bases de Datos. Conocimiento de los principios, métodos y herramientas para automatizar, desarrollar, implementar o administrar sistemas de bases de datos.

Cifrado. Conocimiento de los procedimientos, herramientas y aplicaciones utilizados para mantener seguros los datos o la información, incluyendo la infraestructura de clave pública, el cifrado punto a punto y las tarjetas inteligentes.

Gestión de Incidentes. Conocimiento de las tácticas, tecnologías, principios y procesos para proteger, analizar, priorizar y manejar incidentes.

Aseguramiento de la Información. Conocimiento de los métodos y procedimientos para proteger los sistemas y datos de información asegurando su disponibilidad, autenticación, confidencialidad e integridad.

Certificación de Seguridad de Sistemas de Información. Conocimiento de los principios, métodos y herramientas para evaluar las características de seguridad de los sistemas de información en relación con un conjunto de requisitos de seguridad. Incluye el desarrollo de planes de certificación y acreditación de seguridad.

Seguridad de Sistemas de Información/Redes. Conocimiento de métodos, herramientas y procedimientos, incluyendo el desarrollo de planes de seguridad de información, para prevenir vulnerabilidades en sistemas de información y proveer o restaurar seguridad en los sistemas de información y servicios de redes.

En resumen, el modelo de competencias en ciberseguridad presenta una amplia gama de habilidades técnicas necesarias para tener éxito en este campo en constante evolución. Desde la gestión de la seguridad de la información hasta la implementación y administración de sistemas, pasando por la protección de datos y la prevención de amenazas, cada una de estas competencias es esencial para garantizar la seguridad de los sistemas de información y la protección de los datos confidenciales de individuos y organizaciones. Es importante que los profesionales en ciberseguridad desarrollen una amplia gama de habilidades técnicas, a fin de estar preparados para enfrentar cualquier desafío de seguridad que se presente en el futuro.

Es importante para la empresa Datasec SAS considerar cuidadosamente los aspectos mencionados anteriormente al crear un programa de capacitación en ciberseguridad. Contribuir a una formación efectiva implica tener en cuenta la experiencia y los conocimientos previos de los estudiantes, ajustar el contenido de la capacitación a su nivel de comprensión y proporcionar herramientas y recursos que les permitan aplicar lo aprendido en situaciones del mundo real. Es esencial resaltar la importancia de la ética y la responsabilidad en el ámbito de la ciberseguridad, al tiempo que se enfatiza la necesidad imperativa de mantenerse actualizado y seguir aprendiendo en concordancia con el avance tecnológico y la evolución de los riesgos.

Teniendo en cuenta estos aspectos cruciales, Datasec tiene la oportunidad de optimizar su preparación para diseñar un programa de capacitación eficaz. Este programa estará enfocado en la preparación de posibles candidatos para el puesto de Analista SOC N1 en su Centro de Operaciones de Seguridad y, por supuesto, en contribuir a la capacitación interna de su personal activo.

7.2 ADAPTACIÓN DEL MODELO DE COMPETENCIAS EN CIBERSEGURIDAD PARA EL SOC DE DATASEC

Con base en lo anteriormente expuesto, podemos establecer las habilidades, y conocimientos técnicos base necesarios y adecuados, para desempeñarse en un centro de operaciones de Ciberseguridad, y definir así un modelo de competencias optimo y adaptado a las necesidades y prioridades del SOC de la empresa DATASEC.

Conocimientos sólidos en seguridad informática: Los profesionales en ciberseguridad deben contar con una base sólida en seguridad informática, que les permita comprender los principales riesgos y amenazas a la seguridad de los sistemas y datos, así como las mejores prácticas para mitigarlos.

Experiencia en el manejo de herramientas y tecnologías de seguridad: Los profesionales en ciberseguridad deben tener experiencia en el manejo de herramientas y tecnologías de seguridad, como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, entre otros.

Conocimientos en redes y sistemas: Es importante que los profesionales en ciberseguridad tengan conocimientos en redes y sistemas, ya que esto les permitirá entender el funcionamiento de los sistemas y redes, así como identificar posibles vulnerabilidades.

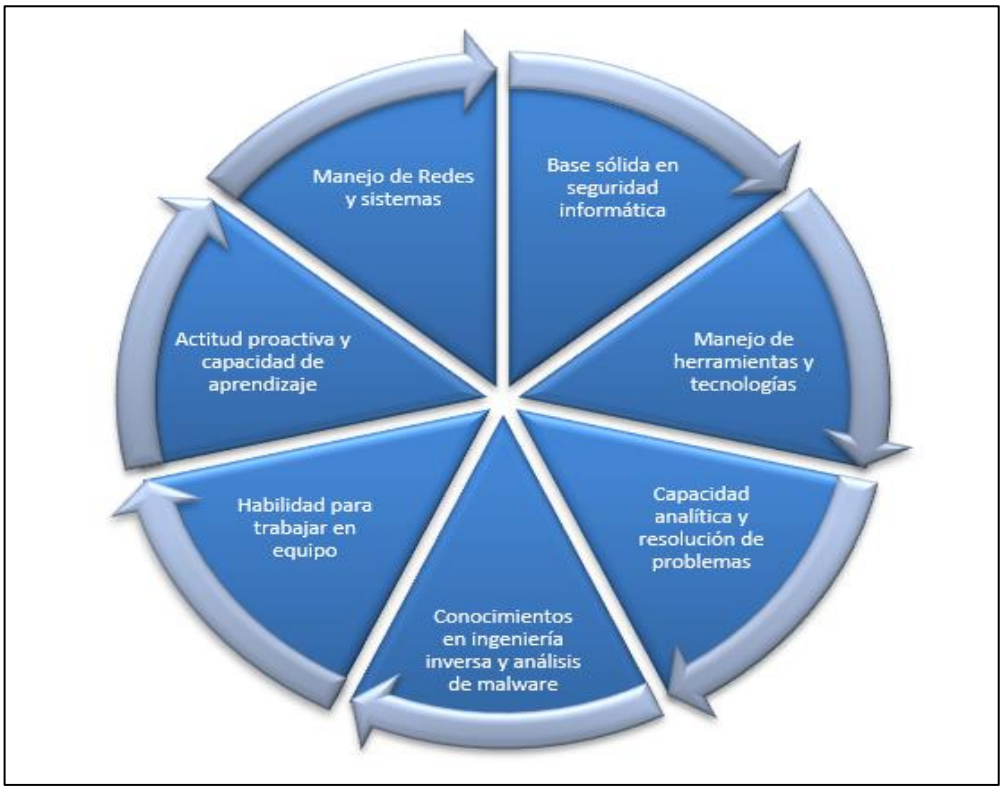
Capacidad analítica y resolución de problemas: Los profesionales en ciberseguridad deben tener una fuerte capacidad analítica y de resolución de problemas, para poder identificar y responder rápidamente a los incidentes de seguridad.

Conocimientos en ingeniería inversa y análisis de incidentes: Los profesionales en ciberseguridad deben tener conocimientos en ingeniería inversa y análisis de malware, para poder identificar y analizar posibles amenazas de seguridad.

Habilidad para trabajar en equipo: La ciberseguridad es un campo en el que el trabajo en equipo es esencial, por lo que los profesionales en ciberseguridad deben tener habilidades para trabajar en equipo y colaborar con otros profesionales de seguridad.

Actitud proactiva y capacidad de aprendizaje: Los profesionales en ciberseguridad deben tener una actitud proactiva en la identificación y resolución de problemas de seguridad, así como una capacidad constante de aprendizaje y actualización en las últimas tendencias y tecnologías en seguridad informática.

Figura 4 Adaptabilidad Modelo de Competencias SOC



Fuente: Datasec SAS.

Es claro que para poder desempeñarse con éxito en el centro de operaciones de ciberseguridad de Datasec SAS, es necesario contar con un conjunto de habilidades, conocimientos y competencias específicas. Estas incluyen sólidos conocimientos en seguridad informática, experiencia en el manejo de herramientas y tecnologías de seguridad, conocimientos en redes y sistemas, capacidad analítica y resolución de problemas, capacidad de análisis de incidentes, habilidades para trabajar en equipo, y actitud proactiva y capacidad de aprendizaje constante.

Al basarse en este modelo de competencias adaptado a las necesidades y prioridades del Centro de operaciones de Seguridad SOC de DATASEC, se logra una contribución significativa al programa de formación, asegurando que este aborde de manera integral las necesidades fundamentales. Además, este enfoque facilitará una evaluación objetiva y detallada de los potenciales candidatos, simplificando la selección de personal idóneo para integrar el equipo de ciberseguridad, especialmente desempeñando roles como Analistas SOC N1. Es de suma importancia que el programa de capacitación en fundamentos de ciberseguridad establezca las bases esenciales para preparar a los individuos que formarán parte del plan de capacitación, permitiéndoles ejecutar actividades de manera efectiva dentro de un centro de operaciones de ciberseguridad.

7.3 ESCALA DE EVALUACIÓN MODELO DE COMPETENCIAS DATASEC

Una vez establecidos las competencias y habilidades más esenciales para los cargos profesionales en el centro de operaciones de Datasec, se elige una metodología que permita evaluar de manera detallada, imparcial y objetiva cada candidato.

Para ello, se establece un sistema[31] que permita definir las competencias requeridas para cada rol y se utiliza una escala de evaluación del 1 al 5 que comprende el nivel de conocimientos, habilidades, complejidad y comprensión esperada para trabajar en el área del Centro de operaciones de Seguridad en los diferentes niveles, esta evaluación marcará el inicio de la identificación del perfil del candidato, contribuyendo a tener en cuenta los aspectos esenciales en ciberseguridad que deben incluirse en el plan de formación de Datasec SAS.

Tabla 1 Escala de evaluación modelo de competencias.

COMPETENCIAS TECNICAS	DESCRIPCIÓN	N1	N2	N3
Conocimiento de sistemas operativos, bases de datos, redes de comunicaciones y protocolos de seguridad.	Conocimiento en sistemas operativos, bases de datos, redes de comunicaciones y protocolos de seguridad para garantizar la correcta implementación de soluciones de seguridad.	5	5	5
Manejo de herramientas de seguridad de la información.	Capacidad para utilizar herramientas de seguridad de la información como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, SANDBOX, SOAR, DECEPTORS, NDR para proteger los sistemas y datos de la empresa.	3	4	5
Análisis de malware y técnicas de ingeniería inversa	Capacidad para realizar análisis de malware y aplicar técnicas de ingeniería inversa para comprender cómo funcionan los programas maliciosos y encontrar soluciones efectivas para combatirlos.	2	3	4

[31] Oitcinterfor Niveles de Competencias (2022) Disponible en https://www.oitcinterfor.org/sites/default/files/file_publicacion/Niveles-de-Competencia-para-Examinados.pdf

Conocimientos profundos en lenguajes de programación y scripting.	Conocimiento avanzado en lenguajes de programación y scripting, que permiten desarrollar soluciones de seguridad personalizadas y automatizar tareas.	2	3	4
Experiencia en análisis forense en Host, Incident Handler, Análisis de malware, Threat Intelligence, Detección avanzada de intrusiones, Ethical Hacking avanzado.	Experiencia en el análisis forense en Host, Incident Handler, Análisis de malware, Threat Intelligence, Detección avanzada de intrusiones, Ethical Hacking avanzado, que permite detectar y solucionar problemas de seguridad de manera efectiva.	1	2	3
Dominios de conocimiento de CISSP.	Conocimiento avanzado en los dominios de conocimiento de CISSP, lo que demuestra una comprensión completa de los principios y prácticas de seguridad de la información.	4	4	5

Fuente: Datasec SAS (2023). Titulo. Escala de evaluación modelo de competencias

7.4 EVALUACION DE CRITERIOS

Cada perfil es evaluado y se le asigna un puntaje, identificando el grado en que se encuentra el candidato. Una vez comprendido el perfil y nivel del técnico, se realiza una evaluación de competencias, incluyendo preguntas de conocimiento tales como:

1. ¿Cuál ha sido la experiencia previa en resolución y análisis de eventos de seguridad en entornos de seguridad operacional (SOC)?

2. ¿Qué conocimientos tiene en sistemas operativos? ¿Cuál es el nivel de experiencia en Windows, Linux y AIX?

3. ¿Qué herramientas de seguridad de la información ha utilizado antes?

4. ¿Cuál es el nivel de experiencia en Firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, SANDBOX y SOAR?

5. ¿Qué metodologías de análisis de incidentes de seguridad, gestión de incidentes y respuesta a incidentes conoce?

6. ¿Qué protocolos de red, puertos y servicios estándar conoce? ¿Podría explicar brevemente en qué consisten?

7. ¿Tiene experiencia en realizar análisis de incidentes y técnicas de ingeniería inversa? ¿Podría describir algún caso en el que haya tenido que hacerlo?

8. ¿Cuál es su nivel de conocimiento en lenguajes de programación y scripting?

9. ¿Qué herramientas conoce para hacer forense digital?

10. ¿Cuenta con estrategias para mantenerse actualizado en cuanto a las últimas amenazas y vulnerabilidades en ciberseguridad?

11. ¿Tiene experiencia en realizar pruebas de penetración o pentesting? ¿Podría explicar brevemente en qué consiste?

12. ¿Qué procedimientos sigue para asegurarse de que un sistema está bien protegido contra ataques externos?

13. ¿Ha tenido experiencia en la implementación de políticas y sistemas de seguridad?

14. ¿Qué experiencia tiene en la gestión de incidentes de seguridad?

15. ¿Qué experiencia tiene en la elaboración de informes técnicos relacionados con incidentes de seguridad?

16. ¿Cuál es el nivel de conocimiento en criptografía? ¿Podría explicar brevemente en qué consiste?

17. ¿Tiene experiencia en la implementación de medidas de seguridad en la nube? ¿Podría describir alguna?

18. ¿Cómo suele manejar situaciones de alta presión en el trabajo? ¿Podría describir algún caso en el que haya tenido que hacerlo?

Las preguntas anteriores desempeñan un papel crucial al permitirnos comprender el perfil del candidato. Estas son consideradas como elementos esenciales que deben ser incorporados en el programa de formación. De esta manera, el programa se enfoca en abordar conocimientos fundamentales que respondan a dichas preguntas.

7.5 PRUEBA TÉCNICA DE COMPETENCIA

Para corroborar la información obtenida por el candidato, se realiza una prueba técnica con un escenario realista. El objetivo es evaluar la respuesta ante incidentes de seguridad, capacidades de decisión y analítica, prestación de servicio, actitudes, aptitudes, manejo de herramientas, tecnologías y experiencia basado en un enfoque de gestión por competencias.[32]

La realización de cada prueba técnica se aplica a cargos del Centro de operaciones se Seguridad SOC de Datasec en vista de que es una excelente manera de evaluar las habilidades y competencias necesarias para desempeñarse eficazmente en cada posición. Al probar a los profesionales con escenarios realistas, se pueden identificar mejor sus fortalezas y debilidades en términos de respuesta a incidentes, capacidad analítica, toma de decisiones, trabajo en equipo, manejo de herramientas y tecnologías de seguridad, y experiencia en el campo.

Esto permitirá a la empresa Datasec seleccionar, contratar y garantizar constantemente que su personal cuente con los mejores profesionales en ciberseguridad para cada puesto, asegurando que el SOC sea constituido por un equipo altamente capacitado y competente para enfrentar cualquier amenaza de seguridad que se presente. Además, al utilizar una metodología basada en la gestión por competencias, se garantiza una evaluación imparcial y objetiva, lo que aumenta la eficacia del proceso de selección de ser necesario.

Considerar esta metodología de gestión por competencias proporciona una visión clara de las expectativas para los profesionales en el centro de operaciones de Seguridad de Datasec. Como se mencionó anteriormente, la posición inicial en el SOC de la empresa es la de Analista N1, y se espera que estos colaboradores, a medida que adquieran experiencia, puedan postularse para cargos de mayor responsabilidad dentro de la compañía. Por lo tanto, es esencial que los candidatos al cargo de Analista SOC N1 posean bases sólidas en ciberseguridad y los fundamentos necesarios para adaptarse eficazmente al modelo de competencias de la organización Datasec.

En DATASEC SAS, actualmente, se implementan pruebas técnicas específicas para cada puesto en su centro de operaciones de ciberseguridad. A continuación, se detallan las características de estas evaluaciones, aspecto esencial a considerar al planificar el desarrollo del programa de formación base en ciberseguridad.

[32] NOE C HERNANDEZ La gestión por competencias y ejercicio de coaching empresarial, dos estrategias internas para la organización, Disponible en http://www.scielo.org.co/pdf/pege/n33/n33a07.pdf

7.5.1 Prueba técnica de competencias analista SOC N1

Objetivo: Evaluar las habilidades y conocimientos básicos del candidato en resolución y análisis de eventos de seguridad.

Requerimientos:

- Computadora con acceso a internet.
- Herramientas de seguridad de la información, como firewalls, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, FIREWALL.

Duración estimada: 2 horas.

Parte 1:

- Configurar un sistema operativo Windows Server 2016 y configurar algunos de los siguientes servicios: Active Directory, DNS, DHCP. Documentar los pasos realizados en la configuración.
- Configurar un servidor web Apache en un sistema operativo Linux. Documentar los pasos realizados en la configuración.

Parte 2:

- Crear un usuario en el Active Directory de Windows y configurar una política de contraseñas. Documentar los pasos realizados en la configuración.
- Configurar un sistema IDS/IPS en una red virtual utilizando el ambiente Fortigate. Documentar los pasos realizados en la configuración.
- Realizar un análisis de vulnerabilidades en los sistemas operativos Windows y Linux utilizando la herramienta FortiSIEM. Documentar los pasos.

7.5.2 Prueba técnica de competencias analista SOC N2

Objetivo: Evaluar las habilidades y conocimientos del candidato en resolución y análisis de eventos de seguridad, utilizando herramientas y tecnologías propias para seguridad.

Requerimientos:

- Computadora con acceso a internet.

- Herramientas de seguridad de la información, como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, SANDBOX y SOAR.

Duración estimada: 2-3 horas.

Parte 1:

- Configurar un sistema operativo Windows Server 2016 y configurar los siguientes servicios: Active Directory, DNS, DHCP y File Sharing. Documentar los pasos realizados en la configuración.

- Configurar un servidor web Apache en un sistema operativo Linux. Documentar los pasos realizados en la configuración.

- Integrar los servidores anteriormente configurados a la herramienta FortiSIEM y realizar un análisis de vulnerabilidades con herramienta Nmap. Documentar los pasos.

Parte 2:

- Simular un ataque de SQL Injection en un sitio web que se encuentra alojado en el servidor Apache. Documentar los pasos seguidos para realizar la simulación.

- Documentar una metodología de análisis de incidentes de seguridad con la herramienta FortiSIEM.

- Describir los pasos a seguir para responder a un incidente de seguridad en un entorno SOC.

- Simular un ataque de phishing y documentar los pasos que seguidos para realizar la simulación.

7.5.3 Prueba técnica de competencias analista SOC N3

Objetivo: Evaluar las habilidades y conocimientos avanzados del candidato en resolución y análisis de eventos de seguridad.

Requerimientos:

- Computadora con acceso a internet.

- Herramientas de seguridad de la información, como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, SANDBOX y SOAR.

Duración estimada: 2-3 horas

Parte 1:

- Configurar un sistema operativo Windows Server 2016 y configurar los siguientes servicios: Active Directory, DNS, DHCP y File Sharing. Documentar los pasos realizados en la configuración.

- Configurar un servidor web Apache en un sistema operativo Linux. Documentar los pasos realizados en la configuración.

- Realizar un análisis de vulnerabilidades en los sistemas operativos Windows y Linux utilizando la herramienta Nessus y realizar la integración a la herramienta FortiSIEM de los servidores. Documentar los pasos.

Parte 2:

- Simular un ataque de SQL Injection en un sitio web que se encuentra alojado en el servidor Apache que configuraste en el paso. Crear un playbook en FortiSOAR para automatizar la acción de respuesta.

- Documentar una metodología de análisis de incidentes de seguridad que pueda utilizar para resolver un ataque de ransomware en una organización.

- Simular un ataque de phishing y documenta los pasos seguidos para realizar la simulación.

Parte 3:

- Realizar un análisis de malware utilizando la herramienta tipo IOC y documentar los pasos seguidos para realizar el análisis.

- Crear un script en Python que pueda automatizar la búsqueda de un archivo específico en un sistema operativo Linux y documenta los pasos.

7.5.4 Prueba técnica de competencias ingeniero de seguridad N1

Objetivo: Evaluar las habilidades y puesta en marcha de soluciones de seguridad de primer nivel para ingeniero de seguridad.

Requerimientos:

- Computadora con acceso a internet.
- Herramientas de seguridad de la información, como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, FIREWALL, SANDBOX, FORTISIEM y SOAR.

Duración estimada: 2-3 horas

Parte 1:

- Realizar un escaneo de vulnerabilidades en una red de prueba utilizando una herramienta de la elección del candidato.
- Identificar las principales vulnerabilidades encontradas y determinar el nivel de riesgo para cada una.
- Proponer medidas de mitigación para cada vulnerabilidad encontrada.

Parte 2:

- Configurar un firewall para permitir el tráfico web y de correo electrónico en una red corporativa.
- Configurar el firewall para bloquear todo el tráfico entrante y saliente desde una dirección IP específica.
- Configurar el firewall para permitir el acceso remoto a una red mediante VPN.

Parte 3:

- Simular una alerta de intrusión en una red empresarial. Describir procedimiento para responder a esta alerta y detallar el procedimiento completo.
- Analizar un archivo sospechoso enviado por correo electrónico y determine si es un archivo malicioso.

Parte 4:

- Configurar una regla de firewall en FortiGate Security que permita el acceso web a un servidor en una red.

- Utilizar FortiSIEM, para generar un informe de amenazas recientes y detallar las medidas de mitigación recomendadas.

- Con FortiSIEM, configurar una regla que le notifique cuando se detecte tráfico malicioso en la red.

Parte 5:

- Realizar un análisis de vulnerabilidades en un sistema operativo Linux, previamente configurado utilizando la herramienta de preferencia. Documentar los pasos que seguiste para realizar el análisis.

- Realizar una búsqueda de exploits para el sistema operativo AIX y documentar el proceso que seguiste para realizar la búsqueda.

- Utiliza la herramienta Wireshark para capturar el tráfico de red entre dos sistemas en una red virtual. Documenta los pasos que seguiste para realizar la captura de tráfico.

7.5.5 Prueba técnica de competencias ingeniero de seguridad N2

Objetivo: Evaluar las habilidades y puesta en marcha de soluciones de seguridad de primer nivel para ingeniero de seguridad.

Requerimientos:

- Computadora con acceso a internet.

- Herramientas de seguridad de la información, como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, SANDBOX, FORTISIEM y SOAR.

Duración estimada: 2-3 horas

Parte 1:

- Configurar una regla de firewall en FortiGate Security que permita el acceso web a un servidor en la red.
- Utilizando FortiSIEM, generar un informe de amenazas recientes y detallar las medidas de mitigación recomendadas.

- Con FortiSIEM, configurar una alerta que le notifique cuando se detecte tráfico malicioso en la red y Sincronizarlos para que FortiSOAR tome la respuesta directa en el Firewall.

Parte 2:

- Realizar un análisis de vulnerabilidades en un sistema operativo Linux, previamente configurado utilizando la herramienta de preferencia. Documentar los pasos que seguiste para realizar el análisis.

- Realizar una búsqueda de exploits para el sistema operativo de muestra y documentar el proceso seguido para realizar la búsqueda.

- Utilizar la herramienta Wireshark para capturar el tráfico de red entre dos sistemas en una red virtual. Documentar los pasos que seguidos para realizar la captura de tráfico.

Parte 3:

- Analizar un archivo malicioso y determinar su funcionalidad y posible origen.

- Describir el proceso para recuperar datos importantes de una imagen forense utilizando la herramienta Autopsy.

- Realiza un análisis de malware utilizando herramientas IOC y documentar los pasos seguidos en el análisis.

- Utilizar la herramienta de preferencia para realizar una imagen forense de un disco duro en una computadora en la que se simula infección con malware y documentar los pasos para realizar la imagen forense.

7.5.6 Prueba técnica de competencias Líder de Ingeniería.

Objetivo: Evaluar las habilidades y conocimientos del líder de Ingeniería, en planificación, ejecución y supervisión de proyectos de seguridad avanzados, así como en la gestión de equipos de ingeniería de seguridad.

Requerimientos:

- Computadora con acceso a internet.

- Herramientas de seguridad de la información, como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, SIEM, SANDBOX, FORTISIEM, NDR y SOAR.

Duración estimada: 3-4 horas

Parte 1:

- Configurar un firewall para permitir el tráfico web y de correo electrónico en una red corporativa.

- Configurar el firewall para bloquear todo el tráfico entrante y saliente desde una dirección IP específica.

- Configurar el firewall para permitir el acceso remoto a una red mediante VPN.

- Realizar un escaneo de vulnerabilidades en una red de prueba y proponer medidas de mitigación para cada vulnerabilidad encontrada.

Parte 2:

- Desarrollar un plan de proyecto detallado para la implementación de un nuevo sistema de detección de intrusiones en una red empresarial.

- Crear las tareas y responsabilidades a los miembros del equipo de ingeniería de seguridad para el proyecto mencionado en el punto anterior.

- Sustentar que métodos utilizaría para la Supervisión del progreso del proyecto que permitan asegurar el cumplimiento de plazos establecidos.

- Simular una reunión de equipo para discutir los desafíos del proyecto y colaborar en la identificación de soluciones.

Parte 3:

- Simular una alerta de intrusión en una red empresarial. Describir el procedimiento para implementar controles en infraestructura que permitan responder a esta alerta y detallar el procedimiento completo.

- Analizar un archivo sospechoso enviado por correo electrónico y determinar si es un archivo malicioso, extraer indicadores de compromiso e importarlos a un Firewall y Sandbox.

- Realizar un informe analítico de hallazgo de malware utilizando herramientas de IOC documentando los pasos seguidos en el análisis.

- Utilizar la herramienta de preferencia para realizar una imagen forense de un disco duro en una computadora infectada con malware y documentar el vector de ataque utilizado en el evento destacando lecciones aprendidas a tener en cuenta en modelos de implementación de infraestructuras seguras.

7.5.7 Prueba técnica de competencias Líder SOC.

Objetivo: Evaluar las habilidades y conocimientos del líder SOC, liderazgo, gestión de equipos y resolución de incidentes de seguridad en un entorno de Centro de Operaciones de Seguridad (SOC).

Requerimientos:

- Computadora con acceso a internet.
- Herramientas de seguridad de la información, como firewalls, IDS/IPS, sistemas de detección de intrusiones, análisis de vulnerabilidades, gestión de riesgo, monitoreo de marca, SIEM, SANDBOX, FORTISIEM, NDR y SOAR.

Duración estimada: 5-6 horas

Parte 1:

- Desarrollar un plan de gestión de riesgos para identificar, evaluar y mitigar las amenazas potenciales a la seguridad de la información en un entorno SOC.
- Realizar un análisis de vulnerabilidades en la infraestructura de red simulada de Datasec SAS, utilizando herramientas especializadas y documentar las vulnerabilidades identificadas junto con las recomendaciones de mitigación.
- Implementar un sistema de monitoreo de marca básico, para detectar y responder a actividades de fraude, suplantación de identidad o uso indebido de la marca en línea.
- Configurar en el simulador SIEM de Datasec SAS, una plataforma de inteligencia de amenazas para recopilar, analizar y compartir información sobre las últimas amenazas cibernéticas relevantes.
- Simular un escenario de incidente de seguridad y sustentar como utilizaría la inteligencia de amenazas para mejorar la detección temprana y la respuesta efectiva al incidente.

Parte 2:

- Desarrollar un plan de proyecto detallado para mejorar la respuesta a incidentes de seguridad en un SOC, alineado a los estándares de la norma ISO/IEC 27001:2022.

- Crear tareas y responsabilidades a asignar a los miembros del equipo SOC para el proyecto mencionado en el punto anterior.

- Sustentar que métodos utilizaría para la supervisión del progreso del proyecto que facilite el cumplimiento en plazos establecidos.

- Simular una reunión ante la alta gerencia para exponer los resultados del proyecto y presentar recomendaciones para mejorar la seguridad de la organización.

Parte 3:

- Utilizando el simulador SIEM, generar un informe detallado de amenazas recientes y detallar las medidas de mitigación recomendadas

- Configurar y ejecutar un archivo sospechoso en un entorno controlado de sandbox para analizar su comportamiento y determinar si es malicioso. Documentar los indicadores de compromiso identificados y las recomendaciones para la respuesta.

- Implementar un par de señuelos de red utilizando la herramienta simulada Deceptor con el fin de detectar y engañar a posibles atacantes.

- Utilizar el gestor de vulnerabilidades de DATASEC SAS, para realizar un escaneo exhaustivo de la infraestructura de red laboratorio, en busca de vulnerabilidades conocidas. Priorizar las vulnerabilidades identificadas según su gravedad y proponer medidas de mitigación.

- Configurar y desplegar un caso de uso en el sistema NDR para monitorear tráfico de red en busca de comportamientos anómalos y actividades sospechosas.

Parte 4:

- Desarrollar un plan de capacidad para el SOC, considerando escenarios de demanda actual y futura de servicios de seguridad cibernética. Identificar los recursos necesarios, como personal, herramientas y tecnologías, para garantizar la efectividad operativa del SOC.

- Realizar un análisis de costos asociados a los servicios ofrecidos en un escenario SOC, incluyendo recursos humanos, licencias de software, infraestructura tecnológica y otros gastos operativos. Identificar áreas de optimización y eficiencia para mejorar la rentabilidad y calidad del servicio.

7.6 RESULTADOS

En Datasec, una vez obtenidos los resultados de las pruebas técnicas, se elaboran planes de desarrollo para que los colaboradores adquieran o mejoren las competencias necesarias para su rol. Estos planes son específicos, medibles, alcanzables, relevantes y con un plazo definido para su cumplimiento. El líder del proyecto proporciona retroalimentación y apoyo continuo a los colaboradores para que puedan alcanzar sus objetivos de desarrollo de competencias. Asimismo, se establecen programas de capacitación y formación continua para asegurar que los colaboradores sigan adquiriendo y mejorando sus habilidades y conocimientos en un campo de la ciberseguridad. Estos programas de formación y capacitación son respaldados por las empresas líderes en ciberseguridad a nivel mundial, con las que Datasec mantiene relaciones comerciales, tales como Fortinet, Cisco y Tenable.

Con base en lo expuesto, se puede afirmar que basarse en un modelo de competencias en ciberseguridad resulta esencial para aquellas organizaciones que aspiran a tener dentro de sus filas, personal que se desempeñe eficientemente en roles vinculados a un Centro de Operaciones de Seguridad SOC. La conjunción de conocimientos sólidos en seguridad informática, experiencia en el manejo de herramientas y tecnologías de seguridad, competencia en redes y sistemas, habilidades analíticas y resolutivas, dominio en ingeniería inversa y análisis de incidentes, capacidad para colaborar en equipo, actitud proactiva y capacidad de aprendizaje, les permitirá enfrentar los desafíos actuales en materia de seguridad y salvaguardar los sistemas y datos de las organizaciones. Dada la naturaleza siempre cambiante del campo de la ciberseguridad, resulta imperativo que los profesionales se mantengan actualizados y prosigan con un aprendizaje continuo para hacer frente a las amenazas y riesgos emergentes.

En consideración de lo expuesto, es esencial destacar la importancia de basarse en un modelo de competencias cuidadosamente adaptado a las necesidades específicas del Centro de Operaciones de Seguridad (SOC) de Datasec SAS. Este enfoque aporta significativamente al proceso de identificación y selección de profesionales más idóneos para cubrir los cargos y desempeñar las funciones requeridas, mejorando así la eficacia y eficiencia de la gestión de la seguridad informática en la organización. Además, un modelo de competencias desempeña un papel clave en la facilitación del proceso de capacitación y desarrollo de los profesionales en ciberseguridad, contribuyendo a alinearlos con los objetivos estratégicos de la empresa y garantizando la continuidad y calidad de los servicios de seguridad ofrecidos. No cabe duda, entonces, de que basarse en un modelo de competencias adaptado a las necesidades específicas del SOC de Datasec proporciona una base óptima para el diseño de un plan de capacitación en fundamentos de ciberseguridad. Esto, a su vez, permite la formación de potenciales candidatos para ingresar al campo laboral en el rol de Analistas SOC N1 en el centro de operaciones de ciberseguridad de la empresa.

8. PROGRAMA DE CAPACITACIÓN EN FUNDAMENTOS DE CIBERSEGURIDAD PARA ANALISTAS SOC.

En DATASEC SAS ha tomado la iniciativa de desarrollar un programa de formación en fundamentos de ciberseguridad que no solo busca abordar la escasez de talento en este campo, sino que también establece un camino para identificar y cultivar futuros especialistas en seguridad cibernética. Este programa no solo se propone llenar la brecha de habilidades existente, sino también impulsar la formación continua y el desarrollo del personal en el centro de operaciones de seguridad de la empresa.

Este tercer objetivo en nuestro proyecto se centra en el desarrollo de un programa diseñado para potenciales candidatos interesados en adentrarse en el ámbito de la ciberseguridad. Este plan de capacitación se respalda en material didáctico actualizado y libre, de organizaciones pioneras a nivel mundial en el campo de la ciberseguridad, laboratorios de práctica y evaluaciones de conocimientos, con el propósito de proporcionar a quienes participen en el programa las habilidades fundamentales y el conocimiento necesario para ingresar al campo de la ciberseguridad con bases sólidas. De esta manera, contribuirá a abordar la problemática actual de la empresa DATASEC SAS relacionada con la escasez de profesionales capacitados para asumir roles en su centro de operaciones de ciberseguridad, especialmente en su cargo de entrada, Analista SOC N1. Además, establece una herramienta que permite que el personal activo se mantenga actualizado en este ámbito en constante evolución.

Como se desprende del diagnóstico del perfil de los cargos ocupados por el personal del Centro de Operaciones de Seguridad en Datasec SAS y del modelo de competencias que se ha adoptado, ajustado a las necesidades específicas de la empresa, el programa de formación en fundamentos de ciberseguridad debe abordar una diversidad de temas y habilidades. Esto con el objetivo de capacitar a los participantes y dotarlos de las aptitudes necesarias para enfrentar los desafíos en constante evolución en el ámbito de la seguridad informática. A continuación, se detallan las temáticas clave seleccionadas en colaboración con la Gerencia, el área de Calidad y el Líder SOC, las cuales serán incluidas en el programa de formación.

- Fundamentos de Ciberseguridad.
- Técnicas de seguridad.
- Herramientas y tecnologías.
- Seguridad de Red.
- Seguridad de Sistemas Operativos.
- Seguridad de Aplicaciones Web.
- Seguridad en la Nube.
- Gestión de Incidentes y Respuesta a Incidentes.
- Cumplimiento y Normativas.

Es importante brindar a los participantes una formación integral y robusta que los sumerja de manera efectiva en el ámbito de la ciberseguridad, estableciendo las bases fundamentales para abordar los desafíos dinámicos de la seguridad informática. En la constante búsqueda de la excelencia, resulta esencial reconocer la importancia de acceder a material educativo de la más alta calidad proveniente de fabricantes líderes en la industria de la ciberseguridad. En este sentido, se propone el diseño del programa educativo con la inclusión de cursos libres, gratuitos y abiertos al público de destacadas organizaciones líderes en ciberseguridad como Cisco, Fortinet e ISC2, reconocidas a nivel mundial por su amplia experiencia y compromiso inquebrantable con la protección en ciberseguridad. Estas organizaciones líderes no solo proporcionarán valiosos recursos didácticos, sino que también ofrecen cursos y certificaciones de prestigio, enriqueciendo de manera significativa la formación interna.

La inclusión de estas certificaciones en el plan de capacitación en ciberseguridad de Datasec representa una oportunidad excepcional para los participantes, brindándoles la posibilidad de adquirir competencias especializadas en el apasionante campo de la ciberseguridad. Los cursos ofrecidos por Cisco, Fortinet e ISC2 son reconocidos por su enfoque riguroso y su énfasis en la aplicación práctica de conceptos y técnicas en entornos reales. Al completar exitosamente estos cursos y obtener certificaciones de entrada ampliamente respetadas a nivel global, los participantes estarán considerablemente mejor preparados para enfrentar tanto los desafíos actuales como los futuros en el campo de la ciberseguridad.

Esta metodología no solo generará beneficios evidentes para los participantes, sino que también fortalecerá la posición de DATASEC SAS en el mercado al proporcionar un flujo constante de potenciales candidatos capacitados, listos para contribuir al éxito del Centro de Operaciones de Seguridad SOC. Además, facilitará que los colaboradores actuales en el SOC de la empresa se mantengan actualizados con las últimas tecnologías y prácticas de ciberseguridad, brindando a DataSec SAS una posición óptima para abordar las actividades propias de su negocio en cuanto a la protección de sus clientes en el creciente entorno de amenazas cibernéticas.

8.1 NOMBRE DEL PROGRAMA DE CAPACITACIÓN

El plan de capacitación en ciberseguridad para la formación de personal en el centro de operaciones de seguridad SOC de la empresa Datasec SAS, llevará por nombre: “Programa de Formación en fundamentos de ciberseguridad para Analistas SOC”.

8.2 INTRODUCCIÓN AL PROGRAMA DE CAPACITACIÓN

El Programa de Formación en Fundamentos de Ciberseguridad para Analistas SOC permite a los participantes desarrollar las habilidades y conocimientos esenciales para desempeñarse de manera eficiente en el rol de Analista en centros de

operaciones de seguridad. Diseñado para aquellas personas que buscan adquirir o fortalecer competencias clave en el monitoreo, gestión, respuesta y generación de informes de incidentes de ciberseguridad, este programa proporciona una sólida base para enfrentar los desafíos de la seguridad informática

A lo largo del programa, los participantes aprenderán a identificar y analizar eventos de seguridad, aplicando procedimientos para mitigar y resolver dichos eventos. Obtendrán conocimientos fundamentales sobre las diversas amenazas y vulnerabilidades presentes en el entorno de seguridad de la información. Además, se familiarizarán con las herramientas y tecnologías utilizadas en los Centros de Operaciones de Seguridad, así como con los estándares y marcos de trabajo más relevantes en el ámbito de la ciberseguridad.

El programa abarca el eficiente uso de sistemas de detección y respuesta de incidentes, así como el mantenimiento de un monitoreo constante para detectar posibles brechas de seguridad. Al completar el programa de manera satisfactoria, los participantes estarán preparados para asumir roles de responsabilidad en Centros de Operaciones de Seguridad. Además, para aquellos que ya forman parte activa de un SOC, el programa ofrece una valiosa oportunidad para mejorar habilidades existentes y profundizar conocimientos especializados. Su sólida formación en análisis de incidentes y gestión de amenazas los capacitará para tomar decisiones informadas y rápidas en situaciones críticas, lo que contribuirá de manera significativa a la protección y defensa de la infraestructura y los activos digitales de las organizaciones.

Se anticipa que los participantes que destaquen y muestren un rendimiento excepcional durante el programa no solo adquirirán las habilidades necesarias para desempeñarse como Analistas SOC, sino que también, aquellos que ya están activos en el campo de la ciberseguridad, se destacarán como potenciales líderes en dicha área.

En Datasec SAS, reconocemos y valoramos el esfuerzo, la dedicación y el compromiso de nuestros participantes más destacados. Por lo tanto, se brindará especial atención y consideración a aquellos individuos que demuestren un rendimiento excepcional, brindándoles la oportunidad de crecimiento profesional y el potencial para asumir el rol de Analista SOC N1 dentro de nuestro equipo de ciberseguridad. Este programa no solo es una plataforma para adquirir conocimientos; es una oportunidad para destacarse, crecer y forjar una carrera exitosa en el emocionante y dinámico campo de la ciberseguridad.

8.3 OBJETIVO DEL PROGRAMA DE CAPACITACIÓN

Brindar una capacitación integral que permita a los participantes desarrollar habilidades y conocimientos fundamentales para desempeñarse de manera eficiente como analistas en el ámbito de la ciberseguridad. Este programa

proporcionará a los participantes la oportunidad de adquirir competencias clave en el monitoreo, gestión, respuesta y generación de informes de incidentes de ciberseguridad, además de familiarizarlos con herramientas, tecnologías y estándares relevantes en el campo. De este modo, se busca prepararlos de manera óptima para desempeñarse exitosamente como Analistas SOC N1.

8.4 REQUISITOS MÍNIMOS DEL PROGRAMA CAPACITACIÓN

Los requisitos mínimos para que un participante pueda inscribirse en el Programa de Formación en Fundamentos de Ciberseguridad para Analistas SOC de Datasec son los siguientes:

- Educación: Ser tecnólogo o ingeniero titulado o estar actualmente en formación en carreras relacionadas con electrónica, informática, telecomunicaciones, sistemas o disciplinas afines. En caso de estar cursando estudios, estos deben ser en modalidad virtual o de lo contario, estar próximos a la graduación (3 meses).
- Conocimientos Básicos: Contar con conocimientos básicos en informática y sistemas, incluyendo una comprensión elemental de redes, sistemas operativos y virtualización.

- Inglés Nivel Medio: Tener un nivel medio de inglés esencial para facilitar la comprensión y estudio de material técnico y audiovisual en dicho idioma.

- Acceso a Internet y Equipo de Cómputo: Disponer de conexión a internet estable y de un equipo de cómputo para participar en las sesiones virtuales y llevar a cabo las actividades del programa de formación.

- Habilidades Técnicas: Demostrar habilidades técnicas básicas, como el manejo de herramientas informáticas, capacidad para resolver problemas y disposición para el autoaprendizaje.

- Interés en Ciberseguridad: Mostrar interés y motivación para adentrarse en el campo de la ciberseguridad, respaldado por una comprensión básica de los desafíos y la importancia de la seguridad informática.

- Habilidades de Comunicación: Poseer habilidades de comunicación efectivas, ya que los roles en ciberseguridad implican colaboración y comunicación clara con otros miembros del equipo y partes interesadas.

- Disponibilidad de Tiempo: Estar dispuesto a comprometerse con el programa de formación, que puede incluir sesiones presenciales o virtuales, así como tiempo dedicado a prácticas y estudios independientes.

- Ubicación: Residir en Bogotá, ciudad donde se encuentra ubicado el centro de operaciones de seguridad de Datasec SAS.

- Acuerdos de Confidencialidad: Aceptar los acuerdos de confidencialidad dispuestos por Datasec SAS para enrolarse en el programa de formación.

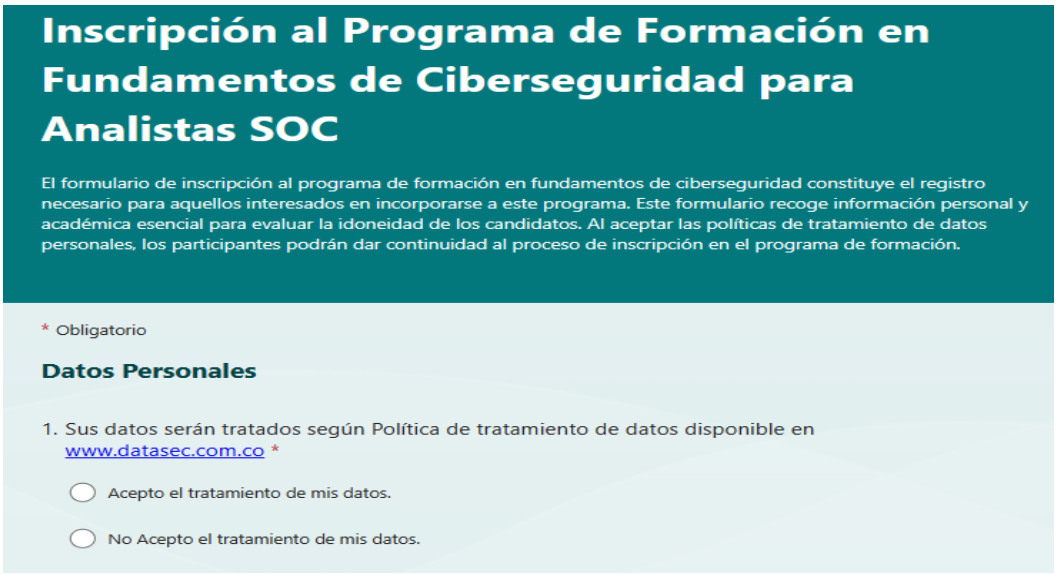
- Cumplimiento de Requisitos Adicionales: Cumplir con cualquier requisito adicional establecido por Datasec, como entrevistas de selección, evaluaciones técnicas u otros criterios específicos.

Estos requisitos aseguran que los participantes cuenten con la base educativa, habilidades técnicas y disposición necesarias para aprovechar al máximo el programa de formación y contribuir al éxito del Centro de Operaciones de Seguridad SOC de Datasec.

8.5 INSCRIPCIÓN AL PROGRAMA DE CAPACITACIÓN

El formulario de inscripción al programa de formación en fundamentos de ciberseguridad de Datasec, constituye el registro necesario para aquellos interesados en incorporarse a este programa. Este formulario recoge información personal y académica esencial para evaluar la idoneidad de los candidatos. Al aceptar las políticas de tratamiento de datos personales, los participantes podrán dar continuidad al proceso de inscripción en el programa de formación.

Figura 5 Formulario de Inscripción al Programa de Formación Ciberseguridad.



Fuente: Datasec SAS.

8.6 AGENDA GENERAL DEL PROGRAMA DE CAPACITACIÓN

Figura 6 Agenda General Programa de Formación Ciberseguridad.

PLATAFORMA	CURSO	TIEMPO
DATASEC	CUSTIONARIO DE CONOCIMIENTOS PREVIOS	1h 00m
DATASEC	CONFERENCIA DE BIENVENIDA Y CONTEXTUALIZACIÓN	0h 45m
DATASEC	INDUCCIÓN Y GENERALIDADES	1h 00m
FORTINET	FCF - INTRODUCTION TO THE THREAT LANDSCAPE	2h 48m
FORTINET	FCF - GETTING STARTED IN CYBERSECURITY	1h 42m
FORTINET	FCF -ECHNICAL INTRODUCTION TO CYBERSECURITY 1.0 SELF-PACED	5h 43m
CISCO	INTRODUCCIÓN A LA CIBERSEGURIDAD	6h 30m
ISC2	CAPACITACIÓN EN LÍNEA OFICIAL DE ISC2 EN CIBERSEGURIDAD CC	5h 45m
DATASEC	APROBACIÓN PROGRAMA DE FORMACIÓN	0h 00m
DATASEC	CONFERENCIA FINALIZACIÓN PLAN DE ESTUDIOS	0h 45m
DATASEC	RETRALIMENTACIÓN Y MEJORA CONTINUA	0h 00m

Fuente: Datasec SAS.

8.7 CUESTIONARIO DE CONOCIMIENTOS PREVIOS

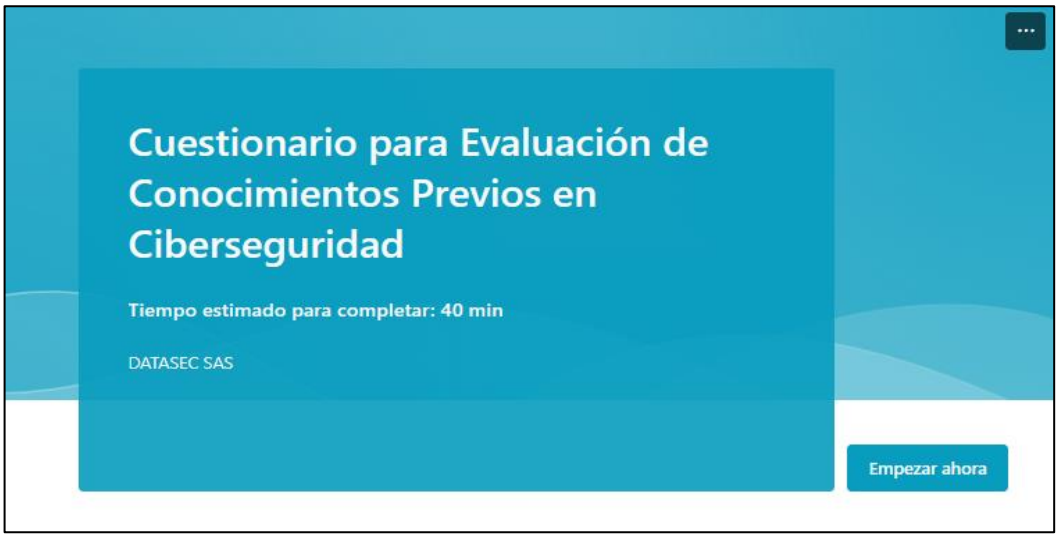
Para dar inicio al programa de capacitación, se llevará a cabo un cuestionario integral denominado Evaluación de Conocimientos Previos en Ciberseguridad. Este instrumento está diseñado para evaluar el conocimiento actual del participante en el ámbito de la ciberseguridad, redes y sistemas operativos. Las respuestas proporcionadas serán cruciales para personalizar la experiencia en el Programa de Formación en Fundamentos de Ciberseguridad para Analistas SOC de Datasec, permitiéndonos dar énfasis en el contenido de manera eficiente según las necesidades identificadas en cada participante. El objetivo principal es comprender el nivel de conocimiento inicial del participante para medir con mayor precisión su progreso al finalizar el programa.

El cuestionario consta de 20 preguntas de opción múltiple, con una sola respuesta correcta, cada una evaluada con un peso de 1 punto. Tiempo estimado 40 minutos. Los niveles de conocimiento se clasifican de la siguiente manera:

ALTO: 18 a 20 puntos.
MEDIO: 13 a 17 puntos.
BAJO: 7 a 12 puntos.
MINIMO: 0 a 6 puntos.

El participante recibirá el enlace de acceso al cuestionario en el correo electrónico proporcionado durante el proceso de inscripción. Al abrir dicho enlace, tendrá la posibilidad de acceder al cuestionario.

Figura 7 Cuestionario para evaluación de conocimientos previos .



Fuente: Datasec SAS.

Las siguientes preguntas son ejemplos del banco de preguntas a aplicar en los cuestionarios.

- ¿Qué es un ataque de phishing?

a) Intento de acceso no autorizado a un sistema
b) Suplantación de identidad mediante correos electrónicos fraudulentos
c) Virus que afecta a las computadoras
d) Acceso indebido a través de una red inalámbrica

- ¿Qué es un protocolo HTTPS?

a) Protocolo para transferencia de archivos
b) Protocolo de seguridad para la transferencia de datos en la web
c) Protocolo de comunicación de red
d) Protocolo de transmisión de video

- ¿Cuál es el propósito principal de un SOC?

a) Desarrollo de software operativo centralizado
b) Monitoreo y gestión de seguridad
c) Mantenimiento de consolas operativas de seguridad
d) Administración de bases de datos tipo SOC

- ¿Qué es un ataque de fuerza bruta?

a) Ataque que aprovecha una debilidad en el software
b) Intento de adivinar una contraseña probando todas las combinaciones posibles
c) Ataque dirigido a la red de una organización
d) Ataque que utiliza software malicioso para el robo de datos

- ¿Cuál es la función principal de un Sistema de Detección de Intrusos (IDS)?

a) Bloquear el tráfico no deseado
b) Detectar actividades sospechosas en una red
c) Filtrar correos electrónicos no deseados
d) Optimizar el rendimiento de la red

- ¿Qué significa VPN?

a) Virtual Private Network
b) Virus Protection Network
c) Very Private Network
d) Virtual Personal Network

- ¿Qué es un certificado SSL?

a) Niveles de Software de seguridad
b) Estándar de encriptación para conexiones seguras en internet
c) Código malicioso encriptado
d) Protocolo de red capa 3

- ¿Qué es la autenticación de dos factores?

a) Uso de dos contraseñas diferentes
b) Verificación de identidad mediante dos métodos distintos
c) Acceso en doble vía sin necesidad de contraseña
d) Uso de huellas dactilares para la autenticación

- ¿Qué significa el término "Zero-Day"?

a) Ataque que ocurre cero días a la semana
b) Vulnerabilidad recién descubierta y aún no parcheada
c) Ataque que ocurre en muy pocos segundos
d) Amenaza inexistente

- ¿Qué es un botnet?

a) Software antivirus
b) Red de dispositivos infectados controlados remotamente por un atacante
c) Herramienta de análisis de vulnerabilidades en red automatizadas
d) Dispositivo Firewall en nube

- ¿Qué es la encriptación de extremo a extremo?

a) Protección de extremo a extremo contra malware
b) Método de encriptación que asegura privacidad de información en transmisión
c) Seguridad solo en el extremo del servidor
d) Sistema de seguridad centralizado

- ¿Qué es un ataque DDoS?

a) Ataque que niega el acceso a servicios legítimos al saturar un sistema con tráfico falso
b) Acceso no autorizado a sistemas DoS
c) Bloqueo de cuentas de usuario
d) Ataque de fuerza bruta

- ¿Cuál es el propósito de un análisis de vulnerabilidades?

a) Monitorizar la red en busca de amenazas
b) Identificar y evaluar posibles brechas de seguridad en un sistema
c) Optimizar el rendimiento de la red
d) Desarrollar software seguro

- ¿Qué sistema operativo es conocido por su núcleo de código abierto y se utiliza comúnmente en servidores?

a) Windows
b) macOS
c) Linux
d) Android

- ¿Cuál de las siguientes opciones describe mejor la función del sistema de archivos en un sistema operativo?

a) Administrar la memoria RAM
b) Organizar y almacenar datos en dispositivos de almacenamiento
c) Administrar la velocidad de la CPU
d) Controlar el acceso a la red

- ¿Cuál de las siguientes direcciones IP es una dirección IP privada?

a) 192.168.1.1
b) 203.120.15.5
c) 172.31.45.2
d) 64.233.162.101

- ¿Cuál es el propósito del comando "ping" en la línea de comandos?

a) Enviar mensajes de pulsos electrónicos ttl
b) Probar la conectividad de red
c) Comprimir archivos
d) Gestionar la impresión de documentos

- ¿Cuál de los siguientes protocolos se utiliza comúnmente para acceder de forma remota a sistemas Unix/Linux?

a) SSH
b) FTP
c) HTTP
d) SNMP

- ¿Qué número de puerto se asocia comúnmente con el protocolo Telnet?

a) 21
b) 22
c) 23
d) 25

- ¿Cuál de las siguientes afirmaciones describe mejor el concepto de "ingeniería social" en ciberseguridad?

a) Proteger la infraestructura física de una organización
b) Utilizar la psicología para engañar a las personas y obtener información confidencial
c) Desarrollar software en sociedad para prevenir ataques cibernéticos
d) Auditar la seguridad de una red informática

8.8 CONFERENCIA DE BIENVENIDA Y CONTEXTUALIZACIÓN

Una vez completado el Cuestionario de Evaluación de Conocimientos Previos, los participantes serán convocados a la primera sesión del programa, que tiene como propósito ofrecer una cálida bienvenida y proporcionar una visión integral del camino que emprenderán. En esta sesión inicial de 45 minutos, se brindará una breve

introducción de la empresa Datasec SAS, permitiendo a los participantes conocer mejor la organización que respalda este programa de formación. El Líder del Centro de Operaciones de Ciberseguridad compartirá los objetivos del programa, explicará la metodología que se seguirá y presentará de manera general las funciones y responsabilidades del Centro de Operaciones de Ciberseguridad de Datasec, brindando a los participantes una comprensión clara de la relevancia y el impacto de su formación.

8.9 PLAN DE ESTUDIO PROGRAMA DE FORMACIÓN

En esta sección, los participantes tendrán la oportunidad de explorar el Plan de Estudios, una guía detallada que les proporcionará una hoja de ruta integral para su aprendizaje y desarrollo en los fundamentos esenciales de la ciberseguridad. A lo largo de los diversos módulos del Plan de Capacitación, se abordarán desde los conceptos más básicos hasta los escenarios prácticos y desafíos del mundo real que los participantes podrían enfrentar en el campo de la ciberseguridad.

Este enfoque integral no solo garantiza una comprensión sólida de los principios teóricos, sino que también proporciona habilidades prácticas aplicables. A continuación, se presenta en detalle el Plan de Estudios del Programa de Formación en Ciberseguridad de Datasec SAS, destacando la estructura cuidadosamente diseñada que fusiona teoría y práctica para un aprendizaje efectivo y holístico.

8.9.1 FORTINET CURSOS CIBERSEGURIDAD

Durante las fases iniciales del programa de formación en ciberseguridad, nos dedicaremos a construir una base conceptual sólida. Utilizando como guía los cursos de ciberseguridad de Fortinet, exploraremos los conceptos fundamentales de la ciberseguridad, comprendiendo su importancia y los principios rectores de la protección de la información. Para abordar la temática de fundamentos en ciberseguridad, se ha seleccionado la certificación: "**Certified Fundamentals (FCF**)"[33] de Fortinet.

Esta certificación atestigua la maestría del estudiante en los conocimientos técnicos y las habilidades esenciales requeridas para puestos de nivel inicial en el ámbito de la ciberseguridad. El plan de estudios incluye cursos que abarcan el panorama actual de amenazas y los conceptos fundamentales de la ciberseguridad.

La certificación FCF se recomienda tanto para profesionales que están dando sus primeros pasos en ciberseguridad como para aquellos que desean forjar una carrera en este campo. Además, resulta valiosa para profesionales que necesitan adquirir una comprensión sólida de los conceptos de ciberseguridad más comunes. La

[33] FORTINET. [Sitio web] Fortinet Latin-America [Consultado: 5 de enero de 2024] Disponible en: https://training.fortinet.com/local/staticpage/view.php?page=fcf_cybersecurity

primera acción que llevará a cabo el participante será seguir instrucciones claras para iniciar sesión en la academia de Fortinet y enrolarse en los cursos contemplados en este plan de capacitación. Posterior a ello, el participante podrá iniciar con los cursos propuestos.

FORTINET CURSO 1: INTRODUCTION TO THE THREAT LANDSCAPE[34]

Durante este curso, los participantes se sumergirán en el panorama actual de las amenazas cibernéticas. Este abordaje incluirá las amenazas que representan riesgos para las redes informáticas, el conjunto de actores maliciosos detrás de estas amenazas y los principios fundamentales de la ciberseguridad. Siguiendo estos principios, se contribuirá a garantizar la seguridad de los activos de las organizaciones.

Diseñado como un punto de entrada, el curso introduction to the threat landscape está especialmente creado para aquellos que están dando sus primeros pasos en el campo de la ciberseguridad. A continuación, se presenta la estructura del curso.

Agenda del curso.

- Introducción a la Ciberseguridad
- El Panorama de Amenazas
- Ingeniería Social
- Malware

Objetivos del curso

- Describir la ciberseguridad y los principios de la seguridad de la información.
- Identificar los tipos de actores malintencionados, sus métodos y las contramedidas utilizadas contra ellos.
- Enumerar diferentes técnicas de ingeniería social.
- Describir los tipos de malware y sus métodos de distribución.

[34] FORTINET. [Sitio web] Fortinet Latin-America [Consultado: 5 de enero de 2024] Disponible en: https://training.fortinet.com/local/staticpage/view.php?page=library_introduction-to-the-threat-landscape

Figura 8 Imagen Cronograma Fortinet Curso 1

PLATAFORMA	CURSO	MODULO	LECCION	T' min
FORTINET	NS1: INTRODUCTION TO THE THREAT LANDSCAPE	Modulo 1: Introduction to Cybersecurity	Lección 01: Introduction to Cybersecurity Overview.	2
			Lección 02: What is Cybersecurity?.	10
			Lección 03: Principles of Information Security.	8
		Módulo 2: The Threat Landscape	Lección 01: The Threat Landscape Overview.	3
			Lección 02: Threat Actors.	15
			Lección 03: Cybersecurity Threats.	15
			Lección 04: Threat Intelligence.	15
			Lección 05: Attack Frameworks.	10
		Módulo 3: Social Engineering	Lección 01: Social Engineering Overview.	3
			Lección 02: Social Engineering Techniques, Part A.	13
			Lección 03: Social Engineering Techniques, Part B.	15
			Lección 04: Insider Threat.	18
			Lección 05: Fraud, Scams, and Influence Campaigns.	8
		Módulo 4: Malware	Lección 01: Malware Overview.	3
			Lección 02: Malware Types.	15
			Lección 03: Malware Attack Vectors and Methods.	15

Fuente: Datasec SAS.

Modulo 1: Introduction to Cybersecurity

Introducción a la Ciberseguridad: En este módulo, se aprenderán conceptos básicos de ciberseguridad, por qué es importante la ciberseguridad y los principios rectores de la protección de la información. Este módulo cuenta con 3 lecciones y un quiz que se detalla a continuación:

- Lección 01: Introduction to Cybersecurity Overview.
- Lección 02: What is Cybersecurity?
- Lección 03: Principles of Information Security.
- Quiz

Modulo 2: The Threat Landscape

Panorama Actual de Amenazas: En este módulo, exploraremos el panorama de amenazas tanto físicas como digitales, así como los vectores de ataque comúnmente presentes en estos entornos. Abordaremos la diversidad de actores maliciosos, sus motivaciones y métodos de ataque. Además, se analizará el funcionamiento de los servicios de inteligencia de amenazas, centrándonos en cómo identifican, resuelven y previenen problemas relacionados con ciberataques. Este módulo cuenta con 5 lecciones y un quiz.

- Lección 01: The Threat Landscape Overview
- Lección 02: Threat Actors

- Lección 03: Cybersecurity Threats
- Lección 04: Threat Intelligence
- Lección 05: Attack Frameworks
- Quiz

Modulo 3: Social Engineering

Ingeniería Social: En este módulo, el participante aprenderá sobre los diferentes métodos de ingeniería social, como phishing, fraude, estafas y campañas de influencia que los malos actores utilizan para obtener lo que quieren. También aprenderá cómo y por qué funciona la ingeniería social. Este módulo cuenta con 5 lecciones y un quiz que se detalla a continuación.

- Lección 01: Social Engineering Overview.
- Lección 02: Social Engineering Techniques, Part A.
- Lección 03: Social Engineering Techniques, Part B.
- Lección 04: Insider Threat.
- Lección 05: Fraud, Scams, and Influence Campaigns.
- Quiz

Modulo 4: Malware

Malware: En este módulo, el participante aprenderá sobre los diferentes tipos de malware, como virus, gusanos y ransomware. Después de familiarizarse con las características del malware y su uso previsto, estará mejor preparado para los ciberataques. Este módulo cuenta con 3 lecciones y un quiz que se detalla a continuación:

- Lección 01: Malware OverviewLinked Course.
- Lección 02: Malware TypesLinked Course.
- Lección 03: Malware Attack Vectors and MethodsLinked Course.

Una vez completado este curso en la academia de Fortinet, el participante obtendrá la insignia del examen Introduction to the Threat Landscape. Este examen forma parte de la certificación Fortinet Certified Fundamentals – Cybersecurity de Fortinet. Deberá enviar el certificado vía correo a la cuenta del SOC de Datasec y se le proveerá un enlace a un cuestionario que confirmará sus nuevos conocimientos obtenidos.

FORTINET CURSO 2: GETTING STARTED IN CYBERSECURITY [35]

Durante este curso, los participantes aprenderán sobre los fundamentos de la ciberseguridad. Este curso está diseñado como un punto de entrada para cualquier persona interesada en aprender sobre ciberseguridad e introduce conceptos básicos y tecnologías en ciberseguridad.

A partir de estos conceptos, se podrá explorar temas más detallados en ciberseguridad.

Agenda del curso.

- Firewall
- NAC
- Sandbox
- WAF
- SEG
- Content Filters
- Secure Wi-Fi
- Endpoint Hardening Techniques
- Endpoint Monitoring
- SOAR
- SIEM
- Secure SD-WAN
- ZTNA
- Cloud Service Models
- SASE

Objetivos del curso

- Identificar conceptos de seguridad de redes y explicar cómo protegen las redes y los datos.

- Describir cómo la tecnología de seguridad de redes se ha desarrollado para contrarrestar las amenazas cibernéticas en constante evolución.

[35] FORTINET. [Sitio web] Fortinet Latin-America [Consultado: 5 de enero de 2024] Disponible en: https://training.fortinet.com/local/staticpage/view.php?page=library_getting-started-in-cybersecurity

Figura 9 Imagen Cronograma Fortinet Curso 2

PLATAFORMA	CURSO	LECCION	TIEMPO (min)
FORTINET	NS2: FCF - GETTING STARTED IN CYBERSECURITY	Lección 01: Firewalls	8
		Lección 02: NAC	8
		Lección 03: Sandbox	6
		Lección 04: WAF	6
		Lección 05: SEG	5
		Lección 06: Content Filters	5
		Lección 07: Secure Wi-Fi	5
		Lección 08: Endpoint Hardening Techniques	13
		Lección 09: Endpoint Monitoring	7
		Lección 10: SOAR	6
		Lección 11: SIEM	6
		Lección 12: Secure SD-WAN	7
		Lección 13: TNA	8
		Lección 14: Cloud Service Models	7
		Lección 15: SASE	5

Fuente: Datasec SAS.

Una vez completado este curso en la academia de Fortinet, el participante obtendrá la insignia del examen getting started in cybersecurity. Este examen forma parte de la certificación Fortinet Certified Fundamentals – Cybersecurity de Fortinet. Deberá enviar el certificado vía correo a la cuenta del SOC de Datasec y se le proveerá un enlace a un cuestionario que confirmará sus nuevos conocimientos obtenidos.

FORTINET CURSO 3: TECHNICAL INTRODUCTION TO CYBERSECURITY [36]

Durante este curso, los participantes aprenderán sobre los fundamentos de la ciberseguridad. Este curso está diseñado como un punto de entrada para cualquier persona nueva en el campo de la ciberseguridad y que esté interesada en seguir una carrera en tecnologías de la información, gestión tecnológica o ciberseguridad. El curso introduce a los conceptos y tecnologías de la ciberseguridad, sobre los cuales podrás avanzar para explorar temas más avanzados relacionados con estas trayectorias profesionales.

Agenda del curso.

- Cryptography and PKI
- Secure Network

[36] https://training.fortinet.com/local/staticpage/view.php?page=library_technical-introduction-to-cybersecurity

- Authentication and Access Control
- Secure Remote Access
- Endpoint Security
- Secure Data and Applications
- Cloud Security and Virtualization

Objetivos del curso

- Describe la terminología y los conceptos utilizados en ciberseguridad.
- Explica cómo asegurar una red mediante criptografía y una seguridad efectiva en los puntos finales.
- Enumera formas de asegurar cualquier tipo de punto final utilizando técnicas de autenticación y endurecimiento del host.
- Explica cómo los modelos de red segura y tecnologías como SD-WAN y SASE pueden mejorar la ciberseguridad.
- Describe las diferencias involucradas en asegurar redes y puntos finales de computación física en las instalaciones, virtual y en la nube.

Figura 10 Imagen Cronograma Fortinet Curso 3

PLATAFORMA	CURSO	MODULO	TIEMPO (min)
FORTINET	NS3: TECHNICAL INTRODUCTION TO CYBERSECURITY	Módulo 1: Cryptography and the public key infrastructure	61
		Módulo 2: Secure Network	70
		Módulo 3: Authentication and Access Control	66
		Módulo 4: Secure Remote Access	30
		Módulo 5: Endpoint Security	2
		Módulo 6: Secure Data and Applications	75
		Módulo 7: Cloud Security and Virtualization	39

Fuente: Datasec SAS.

Modulo 1: Cryptography and the public key infrastructure.

Criptografía y la infraestructura de clave pública: En este módulo, el participante aprenderá sobre una variedad de mecanismos criptográficos y cómo funcionan para resolver problemas. También aprenderá sobre el propósito y los componentes de la infraestructura de clave pública (PKI). Este módulo cuenta con 5 lecciones y un quiz que se detalla a continuación:

- Lección 01: Cryptography and the Public Key Infrastructure Overview
- Lección 02: Ciphers
- Lección 03: Keys and Cryptographic Algorithms
- Lección 04: Hashing and Digital Signatures
- Lección 05: Public Key Infrastructure

Modulo 2: Secure Network

Red Segura: En este módulo, el participante aprenderá sobre los componentes importantes de una red segura, como los firewalls, y cómo puede usarlos para prevenir amenazas comunes a la red. También aprenderá sobre diferentes modelos de red, como perímetro seguro y confianza cero, y sobre diversas implementaciones de red, como red de área amplia definida por software segura (SD-WAN) y borde de servicio de acceso seguro (SASE). Este módulo cuenta con 12 lecciones y un quiz que se detalla a continuación:

- Lección 01: Secure Network Overview.
- Lección 02: Secure Perimeter.
- Lección 03: Zero Trust Principles.
- Lección 04: Centralized Security Network Management.
- Lección 05: Secure SD-WAN.
- Lección 06: SASE.
- Lección 07: Network Segmentation.
- Lección 08: Firewalls.
- Lección 09: Secure Switching and Ports.
- Lección 10: Security Protocols.
- Lección 11: Sandbox.
- Lección 12: Common Network Threats and Prevention.
- Quiz

Modulo 3: Authentication and Access Control

Autenticación y Control de Acceso: En este módulo, el participante aprenderá sobre los procesos y tecnologías de autenticación, autorización y control de acceso que ayudan a controlar el acceso de los usuarios a su red y a los recursos de su red. Este módulo cuenta con 8 lecciones, el contenido del módulo se detallará a continuación.

- Lección 01: Authentication and Access Control Overview.
- Lección 02: Authentication Methods.
- Lección 03: Single Sign-On.
- Lección 04: Authentication Framework, Protocols, and Tools.
- Lección 05: Access Control and Methods.
- Lección 06: Access Control Best Practices.
- Lección 07: Network Access Control.
- Quiz

Modulo 4: Secure Remote Access

Acceso Remoto Seguro: En este módulo, el participante conocerá los métodos y tecnologías de seguridad que permiten a entidades externas conectarse de forma segura a las redes, como IPSec VPN, SSL VPN y el acceso a redes de confianza cero (ZTNA). Este módulo cuenta con 5 lecciones, el contenido del módulo se detallará a continuación.

- Lección 01: Secure Remote Access Overview.
- Lección 02: SSL VPN.
- Lección 03: IPsec VPN.
- Lección 04: Zero Trust Network Access (ZTNA).

Modulo 5: Endpoint Security

Seguridad en los Puntos Finales.: En este módulo, el participante aprenderá acerca de los dispositivos finales, cómo protegerlos y cómo la prevalencia de "traiga su propio dispositivo" (BYOD) y el Internet de las cosas (IoT) complica la seguridad de la red. También aprenderá sobre la tecnología de supervisión de endpoints, como la plataforma de protección de endpoints (EPP) y la detección y respuesta de endpoints (EDR). Este módulo cuenta con 5 lecciones, el contenido del módulo se detallará a continuación.

- Lección 01: Endpoint Security Overview.
- Lección 02: Internet of Things.
- Lección 03: Endpoint Hardening Techniques.
- Lección 04: Endpoint Monitoring.

Modulo 6: Secure Data and Applications

En este módulo, el participante aprenderá sobre la importancia de la privacidad y la protección de datos, y las tecnologías y técnicas que puede utilizar para proteger los datos, como los filtros de contenido, los firewalls de aplicaciones web (WAF), las pasarelas de correo electrónico seguras (SEG) y el refuerzo de aplicaciones. Este módulo cuenta con 7 lecciones, el contenido del módulo se detallará a continuación.

- Lección 01: Secure Data and Applications Overview.
- Lección 02: Data Protection.
- Lección 03: Data Privacy.
- Lección 04: Secure Email Gateway.
- Lección 05: WAF.
- Lección 06: Content Filters.
- Lección 07: Application Hardening Techniques.
- Quiz

Modulo 7: Cloud Security and Virtualization

Seguridad en la Nube y Virtualización: En este módulo, el participante aprenderá sobre las amenazas comunes asociadas con el uso de aplicaciones, máquinas virtuales (VM) y datos en la nube, y cómo mitigar esas amenazas utilizando tecnología de seguridad. También aprenderá acerca de los servicios de seguridad que se alojan en la nube, como Firewalls y puertas de enlace de correo electrónico, y cómo las API pueden ayudar a conectar de forma segura los servicios en la nube con otros componentes de red y aplicaciones de terceros. Este módulo cuenta con 6 lecciones, el contenido del módulo se detallará a continuación.

- Lección 01: Cloud Security and Virtualization Overview.
- Lección 02: Cloud Service Models.
- Lección 03: Virtual Machine Risks.
- Lección 04: Common Cloud Threats.
- Lección 05: Cloud Hosted Security Services.
- Lección 06: Securing the Cloud
- Quiz.

Una vez completado este curso en la academia de Fortinet, el participante obtendrá la insignia del examen technical introduction to cybersecurity. Este examen forma parte de la certificación Fortinet Certified Fundamentals – Cybersecurity de Fortinet. Deberá enviar el certificado vía correo a la cuenta del SOC de Datasec y se le proveerá un enlace a un cuestionario que confirmará sus nuevos conocimientos obtenidos.

8.9.2 CISCO CURSO CIBERSEGURIDAD

Cisco y su plataforma Networking Academy representan una herramienta invaluable para aquellos que buscan destacarse en el campo de la ciberseguridad, y esto se debe a diversos motivos. En primer lugar, brindan cursos especializados y continuamente actualizados que establecen una sólida base en los principios fundamentales de la ciberseguridad. Además, la plataforma no solo se limita a la teoría; proporciona acceso a recursos prácticos y experiencias de laboratorio, permitiendo a los estudiantes aplicar sus conocimientos en entornos simulados de manera efectiva, fortaleciendo así su comprensión práctica. La certificación en ciberseguridad otorgada por Cisco goza de reconocimiento a nivel mundial, añadiendo un valor significativo al currículum de los profesionales que la obtienen, lo que potencia sus oportunidades laborales. Dentro de este programa de capacitación integral, se espera que los participantes cursen y superen con éxito el módulo de Introducción a la Ciberseguridad de Cisco, el cual constituye un pilar fundamental para el desarrollo de habilidades cruciales en el ámbito de la seguridad informática.

CURSO INTRODUCCIÓN A LA CIBERSEGURIDAD[37]

Este curso se orienta hacia el establecimiento de una base sólida en los principios fundamentales de la ciberseguridad, brindando a los participantes las destrezas esenciales para identificar y abordar amenazas de seguridad en entornos de red. Este curso de constituye una puerta de entrada al fascinante ámbito de la ciberseguridad, donde los participantes adquirirán conocimientos sobre los conceptos fundamentales que resguardan su vida digital personal. Además, se explorarán en detalle los desafíos más significativos en materia de seguridad que actualmente enfrentan empresas, gobiernos e instituciones educativas, dotando así a los participantes con una comprensión integral de los panoramas de seguridad actuales.

Agenda del curso.

- Introducción a la Ciberseguridad.
- Ataques, conceptos y técnicas.
- Protegiendo sus datos y su privacidad y la Organización.

Objetivo del curso.

El curso de Introducción a la Ciberseguridad de Cisco tiene como objetivo brindar a los participantes una comprensión sólida de los conceptos esenciales de ciberseguridad, abordando temas clave como ataques cibernéticos, protección de datos y seguridad organizacional. Los participantes desarrollarán habilidades prácticas para abordar los desafíos de seguridad actuales.

Figura 11 Imagen Cronograma Curso Cisco Modulo 1.

MODULO	LECCION	T' min
Módulo 1: Introducción a la Ciberseguridad	1.1 El mundo de la Ciberseguridad	60
	1.2 Datos de la Organización	
	1.3 ¿Qué fue tomado?	
	1.4 Ciberatacantes	
	1.5. Guerra Cibernetica	
	1.6 Cuestionario	

Fuente: Datasec SAS.

[37] Cisco (2024) Networking Academy Introduction to Cybersecurity [Consultado: 5 de enero de 2024] Disponible en https://www.netacad.com/courses/cybersecurity/introduction-cybersecurity

Figura 12 Imagen Cronograma Curso Cisco Modulo restantes.

Módulo 2: Ataques, conceptos y técnicas	2.1 Análizando un Ciberataque	90
	2.2 Métodos de Infiltración	
	2.3 Aprovechamiento de las vulnerabilidades de seguridad	
	2.4 El panorama de la ciberseguridad	
	2.5 Cuestionario	
Módulo 3: Protegiendo sus datos y su privacidad	3.1 Proteja sus dispositivos y su red	90
	3.2 Mantenimiento de datos	
	3.3 ¿A quién le pertenecen sus datos?	
	3.4 Protección de la privacidad en línea	
	3.5 Descubre su propio comportamiento riesgoso en línea	
	3.6 Cuestionario	
Módulo 4: Protegiendo a la Organización	4.1 Dispositivos de Ciberseguridad y Tecnología	90
	4.2 Enfoque de comportamiento de la ciberseguridad	
	4.3 Enfoque de cisco para la ciberseguridad	
	4.4 Cuestionario	
Módulo 5: ¿Su futuro estará relacionado con la ciberseguridad?	5.1 Cuestiones Legales y Técnicas	60
	5.2 Educación y Carreras	
	5.3 Cuestionario	

Fuente: Datasec SAS.

Modulo 1: Introducción a la Ciberseguridad

Este módulo ofrece una perspectiva integral del entorno cibernético, guiando al participante a través de los fundamentos esenciales de la ciberseguridad. Se destacará la importancia de comprender las amenazas actuales y futuras, abarcando desde la salvaguarda de datos organizativos hasta la identificación de ciberatacantes. Este módulo sienta las bases esenciales para desarrollar una comprensión sólida de los desafíos en el mundo digital actual. Además, se adentrará en el concepto de guerra cibernética y se analizará su impacto en la seguridad a escala global. Este módulo cuenta con 5 lecciones y un cuestionario.

- Lección 01: El mundo de la Ciberseguridad.
- Lección 02: Datos de la Organización.
- Lección 03: ¿Que fue tomado?
- Lección 04: Ciberatacantes
- Lección 5: Guerra Cibernética
- Cuestionario.

Modulo 2: Ataques, conceptos y técnicas

Este Modulo proporciona un análisis profundo de los ciberataques y métodos de infiltración que constituyen amenazas críticas en el ámbito digital. A lo largo de cuatro lecciones, el participante explorará la complejidad de analizar un ciberataque, los diversos métodos utilizados para infiltrarse en sistemas, y cómo se aprovechan las vulnerabilidades de seguridad. Concluiremos este módulo examinando el panorama general de la ciberseguridad. Este módulo cuenta con 4 lecciones y un cuestionario.

- Lección 01: Analizando un Ciberataque
- Lección 02: Métodos de infiltración
- Lección 03: Aprovechamiento de las vulnerabilidades de seguridad
- Lección 04: El panorama de la ciberseguridad
- Cuestionario.

Modulo 3: Protegiendo sus datos y privacidad

Este módulo se centra en salvaguardar la información personal y la privacidad en el entorno digital. El participante comenzará explorando estrategias para proteger dispositivos y redes, seguido por el mantenimiento adecuado de datos y reflexiones sobre la propiedad de la información personal. Además, se abordarán prácticas para la protección de la privacidad en línea y se analizará el propio comportamiento en línea para identificar posibles riesgos. Consta de 5 lecciones y un cuestionario.

- Lección 01: Proteja sus dispositivos y red
- Lección 02: Mantenimiento de datos
- Lección 03: ¿A quién le pertenece sus datos?
- Lección 04: Protección de privacidad en línea
- Lección 05: Descubra su propio comportamiento riesgoso en línea
- Cuestionario.

Modulo 4: Protegiendo a la Organización

Este módulo se adentra en estrategias y tecnologías clave para fortalecer la seguridad organizacional en el ámbito digital. El participante comenzará explorando dispositivos de ciberseguridad y tecnología esenciales, seguido por un análisis del enfoque de comportamiento en ciberseguridad. Concluirá con una inmersión en el enfoque distintivo de Cisco para abordar los desafíos cibernéticos. Este módulo, consta de 3 lecciones y un cuestionario.

- Lección 01: Dispositivos de ciberseguridad y tecnología
- Lección 02: Enfoque de comportamiento de la ciberseguridad
- Lección 03: Enfoque de Cisco para la ciberseguridad

- Cuestionario.

Modulo 5: Su futuro está relacionado con la ciberseguridad

Este módulo ofrece una perspectiva esencial sobre las dimensiones legales, éticas y profesionales en el campo de la ciberseguridad. La Lección 1 aborda cuestiones cruciales relacionadas con la legalidad y ética en el ámbito digital, proporcionando una comprensión integral de las responsabilidades. La Lección 2 se enfoca en la educación y las perspectivas de carrera en el vasto y dinámico campo de la ciberseguridad. Este módulo, clave para planificar el futuro profesional en este sector, cuenta con 2 lecciones y un cuestionario.

- Lección 01: Cuestiones legales y éticas
- Lección 02: Educación y carreras
- Cuestionario.

Al finalizar con éxito este curso en la Academia de Cisco, los participantes recibirán el certificado correspondiente al curso "Introducción a Ciberseguridad". Se requiere el envío del certificado a la dirección de correo del SOC de Datasec. Una vez recibido, se proporcionará un enlace al participante para acceder a un cuestionario que validará los nuevos conocimientos adquiridos durante el curso de Cisco.

8.9.3 ISC2 CURSO CIBERSEGURIDAD

ISC2 es una organización global sin fines de lucro dedicada a educar y certificar profesionales en ciberseguridad a lo largo de sus carreras Y es conocida por ser líder en el desarrollo de certificaciones de ciberseguridad de primer nivel y programas educativos de clase mundial. Con una membresía en constante crecimiento que supera los 500,000 miembros, candidatos y asociados en todo el mundo, desempeñando un papel fundamental en la promoción y el avance del conocimiento y las mejores prácticas en el campo de la ciberseguridad.

CURSO CON CERTIFICACIÓN OFICIAL ISC2 EN CIBERSEGURIDAD (CC)[38]

La certificación "Certified in Cybersecurity (CC)" constituye un programa integral meticulosamente diseñado para dotar a los participantes de conocimientos esenciales en la terminología de la industria y los fundamentos necesarios para desempeñarse de manera competente en roles de seguridad cibernética, especialmente en niveles iniciales o junior. Este programa abarca diversos módulos, desde principios de seguridad hasta conceptos avanzados de respuesta a incidentes y operaciones de seguridad, brindando así una formación exhaustiva. El curso no solo ofrece una sólida base en las mejores prácticas, políticas y

[38] ISC2 CC (2024) Ciberseguridad formación en línea a su propio ritmo Cybersecurity [Consultado: 5 de enero de 2024] Disponible en https://www.isc2.org/training/online-self-paced/spanish

procedimientos críticos en el ámbito de la ciberseguridad, sino que también fomenta un enfoque proactivo hacia el aprendizaje continuo y el crecimiento profesional.

Los participantes no solo adquirirán conocimientos fundamentales, sino que también demostrarán su disposición y capacidad para evolucionar profesionalmente. Este enfoque no solo valida su comprensión teórica, sino que también destaca su preparación para asumir responsabilidades más avanzadas en el campo de la seguridad cibernética. Al completar con éxito este programa, los participantes no solo obtienen una certificación reconocida, sino que también se posicionan como profesionales altamente capacitados y comprometidos con la excelencia en un campo en constante evolución. Este curso no solo es una inversión en conocimientos, sino también en el desarrollo de habilidades y competencias esenciales que impulsan el éxito a largo plazo en el ámbito de la ciberseguridad.

Agenda del curso.

- Introducción al curso
- Principios de seguridad
- Conceptos de respuesta a incidentes, continuidad del negocio y recuperación
- Conceptos de control de acceso
- Seguridad de la red
- Operaciones de seguridad
- Conclusión del curso
- Glosario

Objetivo del curso.

El curso Certified in Cybersecurity (CC) tiene como objetivo proporcionar a los participantes una comprensión integral de los principios fundamentales de ciberseguridad, abordando conceptos clave en seguridad de la información, gestión de riesgos, controles de seguridad, y gobernanza. Los participantes aprenderán a aplicar principios éticos y prácticas del Código de Ética (ISC)², así como a analizar y responder eficientemente a incidentes de seguridad.

Asimismo, los participantes dirigirán su atención hacia la implementación efectiva de controles de acceso tanto físicos como lógicos. Profundizarán en los principios fundamentales de la seguridad en redes y explorarán las operaciones de seguridad, abarcando la gestión de datos, registro y monitoreo, cifrado, y la capacitación en conciencia de seguridad. A lo largo del curso, se fomentará una práctica activa, involucrando la aplicación constante de la terminología y la revisión de conceptos. Este enfoque activo fortalecerá de manera integral las habilidades y conocimientos necesarios para destacar en el dinámico campo de la ciberseguridad.

Figura 13 Imagen Cronograma Curso ISC2.

MODULO	LECCION	T' min
Introducción del curso	Módulo 1: Primeros Pasos	10
	Módulo 2: Introducción al Curso	
Capítulo 1: Principios de la Seguridad	Módulo 1: Comprender los conceptos de seguridad de la garantía de la información	60
	Módulo 2: Comprender el proceso de gestión de riesgos.	
	Módulo 3: Comprender los controles de seguridad.	
	Módulo 4: Comprender los elementos y procesos de gobernanza.	
	Módulo 5: Entender ISC2 Código de Ética.	
	Módulo 6: Capítulo 1 Resumen.	
Capítulo 2: Respuesta a incidentes, Continuidad del negocio y Recuperación ante desastres	Módulo 1: Comprender las respuestas a incidentes	60
	Módulo 2: Comprender la continuidad del negocio (BC).	
	Módulo 3: Comprender la recuperación ante desastres (DR).	
	Módulo 4: Capítulo 2 Resumen.	
Capítulo 3: Conceptos de Control de Acceso	Módulo 1: Comprender los conceptos de control de acceso.	60
	Módulo 2: Comprender los controles de acceso físico.	
	Módulo 3: Comprender los controles de acceso lógico.	
	Módulo 4: Resumen del Capítulo 3.	
Capítulo 4: Seguridad de la Red	Módulo 1: Comprender las redes informáticas.	60
	Módulo 2: Comprender las amenazas y ataques (cibernéticos) de red.	
	Módulo 3: Comprender la infraestructura de seguridad de la red.	
	Módulo 4: Resumen del Capítulo 4.	
Capítulo 5: Operaciones de Seguridad	Módulo 1: Comprender la seguridad de los datos.	60
	Módulo 2: Comprender el endurecimiento del sistema.	
	Módulo 3: Comprender las políticas de seguridad de mejores prácticas.	
	Módulo 4: Comprender la capacitación de concientización sobre seguridad.	
	Módulo 5: Resumen del Capítulo 5.	
Conclusión del Curso	Video: Comenzando en la Ciberseguridad.	35
	Registrarse y prepararse para el examen.	
	Evaluación posterior al curso.	
	Evaluación del curso.	

Fuente: Datasec SAS.

Introducción al curso

Esta sección proporciona una descripción general de las especificaciones del curso para la capacitación autodidáctica con certificación oficial ISC2 en seguridad cibernética (CC).

Capítulo 1: Principios de la seguridad

En el capítulo 1, "Principios de la Seguridad", de la Certificación Certified in Cybersecurity (CC) de ISC2, los participantes se sumergirán en los fundamentos esenciales de la ciberseguridad. Este capítulo ofrece una sólida base para discutir conceptos clave, reconocer principios fundamentales de la seguridad de la información y comprender la gestión de riesgos. Desde la clasificación de controles de seguridad hasta la distinción entre políticas y leyes, los participantes explorarán de manera integral los principios que sustentan el panorama de la ciberseguridad. Se fomentará la práctica activa de la terminología y la revisión de principios para consolidar un conocimiento sólido en esta disciplina crucial. Este capítulo consta de 6 módulos.

- Módulo 1: Comprender los conceptos de seguridad de la garantía de la información.
- Módulo 2: Comprender el proceso de gestión de riesgos.
- Módulo 3: Comprender los controles de seguridad.
- Módulo 4: Comprender los elementos y procesos de gobernanza.
- Módulo 5: Entender ISC2 Código de Ética.
- Módulo 6: Capítulo 1 Resumen

Capítulo 2: Respuesta a incidentes, Continuidad del negocio y Recuperación.

En el capítulo 2, "Respuesta a Incidentes, Continuidad del Negocio y Recuperación ante Desastres", de la Certificación Certified in Cybersecurity (CC) de ISC2, el participante se sumergirá en la esfera crítica de la disponibilidad dentro de la tríada CIA. Este capítulo destaca la importancia de mantener operativos los recursos humanos y del sistema mediante la implementación de planes integrales de Respuesta a Incidentes, Continuidad del Negocio (BC) y Recuperación de Desastres (DR). Aunque estos planes pueden superponerse en su alcance, son fundamentales para la supervivencia organizacional. Al finalizar este capítulo, los participantes estarán preparados para explicar las estrategias de respuesta y recuperación durante interrupciones no planificadas, recordar términos y componentes clave, resumir elementos de planes de continuidad del negocio y reconocer componentes esenciales de la recuperación ante desastres. Este capítulo consta de 4 módulos.

- Módulo 1: Comprender las respuestas a incidentes
- Módulo 2: Comprender la continuidad del negocio (BC).
- Módulo 3: Comprender la recuperación ante desastres (DR).
- Módulo 4: Capítulo 2 Resumen.

Capítulo 3: Conceptos de Control de Acceso

En el capítulo 3, "Conceptos de Control de Acceso", de la Certificación Certified in Cybersecurity (CC) de ISC2, el participante se sumergirá en un análisis detallado de los tipos de control de acceso esenciales para cualquier profesional de la seguridad de la información. Explorará tanto los controles físicos como los lógicos, comprendiendo cómo se entrelazan para fortalecer la seguridad integral de una organización. Este capítulo se adentra en la gestión de quién tiene acceso a qué, por qué ese acceso es necesario y cómo se administra de manera efectiva. Al concluir este capítulo, los participantes estarán equipados para seleccionar controles de acceso apropiados en escenarios específicos, relacionar conceptos y procesos con situaciones concretas, comparar diversos controles físicos y describir los controles de acceso lógico. Este capítulo consta de 6 módulos.

- Módulo 1: Comprender los conceptos de control de acceso.
- Módulo 2: Comprender los controles de acceso físico.
- Módulo 3: Comprender los controles de acceso lógico.
- Módulo 4: Resumen del Capítulo 3.

Capítulo 4: Seguridad de la Red

En el capítulo 4, "Seguridad de la Red", de la Certificación Certified in Cybersecurity (CC) de ISC2, el participante explorará las complejidades de las redes informáticas y su seguridad. En el mundo interconectado actual, donde Internet vincula casi todo, estas redes se convierten en un componente vital. Este capítulo destaca la dualidad de las redes, considerándolas no solo como un elemento positivo, sino también como una fuente de posibles vulnerabilidades que los delincuentes pueden explotar. Explorará también los componentes esenciales de las redes, las amenazas y ataques, y aprenderemos estrategias para protegerlas de potenciales atacantes. Al finalizar este capítulo, los participantes estarán capacitados para explicar conceptos de seguridad en redes, reconocer modelos y términos comunes, identificar protocolos y puertos seguros, comprender amenazas cibernéticas, analizar herramientas preventivas y familiarizarse con la terminología relacionada con el diseño de una red segura. Este capítulo consta de 4 módulos.

Capítulo 5: Operaciones de Seguridad

En el capítulo 5, "Operaciones de Seguridad", de la Certificación Certified in Cybersecurity (CC) de ISC2, el participante se adentrará en la esencia misma de las operaciones diarias que sustentan los controles de seguridad y las estrategias de mitigación de riesgos en una organización. Este capítulo destaca la importancia crítica de salvaguardar datos y sistemas continuamente, así como de fomentar prácticas seguras entre aquellos que interactúan con la información en su quehacer

cotidiano. Al concluir este capítulo, los participantes estarán capacitados para explicar conceptos clave en operaciones de seguridad, discutir mejores prácticas en la gestión de datos, identificar elementos cruciales de registro y monitoreo, resumir los distintos tipos de cifrado, describir conceptos de gestión de la configuración, explicar la aplicación de políticas de seguridad comunes y comprender la importancia de la concientización en seguridad. Este capítulo consta de 5 módulos.

Conclusión del Curso

Este curso ha preparado a los participantes para afrontar con éxito el desafío del examen de certificación, brindándoles una sólida base de conocimientos en ciberseguridad. Ahora, al aprobar el examen, los participantes se unirán a la distinguida comunidad de ISC2, llevando consigo las habilidades necesarias para destacar en el campo de la ciberseguridad. La sección de conclusión ofrece recursos adicionales, como un video introductorio a la ciberseguridad, orientación sobre el proceso de registro y preparación para el examen, así como evaluaciones posteriores al curso para reforzar el aprendizaje.

Al aprobar el examen final de este curso de la Academia de ISC2, los participantes recibirán el certificado correspondiente. Se requiere el envío del certificado a la dirección de correo del SOC de Datasec. Una vez recibido, se proporcionará un enlace al participante para acceder a un cuestionario que validará los nuevos conocimientos adquiridos durante el curso de ISC2.

8.10 APROBACIÓN PROGRAMA DE FORMACIÓN

La aprobación exitosa del programa de formación en fundamentos de ciberseguridad de Datasec implica cumplir integralmente con varios requisitos. El participante debe haber completado plenamente el plan de estudios, remitiendo los certificados de los cursos correspondientes a la cuenta de correo del SOC, así como haber superado con éxito los cuestionarios de confirmación de conocimientos. Además, es esencial haber participado activamente en todas las sesiones en vivo, interactuando con los profesionales de Datasec y demostrando un compromiso destacado. Una vez que se hayan cumplido estos requisitos fundamentales, el participante será elegible para recibir una invitación exclusiva a la conferencia de Finalización del plan de estudios del programa de formación, un evento significativo que celebra los logros y prepara el terreno para futuras oportunidades en el ámbito de la ciberseguridad.

8.11 CONFERENCIA DE FINALIZACIÓN PLAN DE ESTUDIOS

Una vez que los participantes hayan culminado satisfactoriamente el plan de estudios y superado los cuestionarios de validación de conocimientos, serán convocados a la emocionante sesión de clausura del programa de formación en fundamentos de ciberseguridad de Datasec. El principal objetivo de esta sesión es

brindar una sincera felicitación y reconocimiento a aquellos que han alcanzado con éxito la finalización del programa, además de llevar a cabo una breve revisión de los notables logros y conocimientos adquiridos durante la capacitación. Se resaltará el evidente crecimiento y desarrollo de habilidades que los participantes han experimentado a lo largo del programa. La sesión también servirá como fuente de inspiración, motivando a los analistas a continuar avanzando en sus carreras en ciberseguridad y aplicar de manera proactiva los conocimientos adquiridos en su quehacer diario. Asimismo, se fomentará el compromiso con el aprendizaje continuo y la participación en la vibrante comunidad de ciberseguridad.

En la conferencia de finalización del plan de estudios, el líder del Centro de Operaciones de Ciberseguridad compartirá información valiosa sobre la emocionante siguiente etapa: la posibilidad de integrarse al selecto grupo de candidatos para Analistas SOC N1 en Datasec. Durante la sesión, se detallará el proceso de solicitud, animando a los participantes a enviar sus solicitudes al correo del SOC para recibir el enlace al formulario correspondiente.

Esta sesión culminante, con una duración estimada de 45 minutos, no solo brindará cierre al plan de estudios, sino que también marcará el inicio de nuevas y prometedoras oportunidades profesionales en Datasec SAS. Más allá de ser un simple punto final, esta conferencia será un punto de partida para aquellos que buscan embarcarse en roles clave en el ámbito de la ciberseguridad. Se alentará a todos los participantes a aprovechar esta valiosa oportunidad y a explorar las emocionantes perspectivas que aguardan en el camino profesional que se avecina.

8.12 RETROALIMENTACIÓN Y MEJORA CONTINUA

En línea con el compromiso constante con la excelencia, Datasec facilitará un espacio dedicado a la retroalimentación, destinado a aquellos participantes que hayan completado el programa de formación en fundamentos de ciberseguridad. Aquí, se invita a los participantes a compartir sus valiosas percepciones a través de un formulario específico, proporcionando un canal abierto para expresar sus experiencias y observaciones detalladas.

Esta iniciativa está diseñada con el objetivo principal de recopilar comentarios exhaustivos que serán fundamentales para identificar áreas de mejora y posibles ajustes. Al contribuir con sus perspectivas, los participantes se convierten en agentes activos en la evolución continua del programa, influyendo en futuras iteraciones para garantizar que el contenido y la metodología sigan siendo pertinentes y efectivos. Se reconoce así que la retroalimentación desempeña un papel central en la búsqueda constante de ofrecer una formación de calidad y relevante en el siempre dinámico campo de la ciberseguridad.

9. CONCLUSIONES

El análisis de las funciones críticas en el Centro de Operaciones de Seguridad (SOC) de Datasec ha resaltado la importancia de identificar con precisión las habilidades y conocimientos esenciales necesarios para cada puesto, desde el Analista SOC N1 hasta el Líder del equipo SOC. Este diagnóstico de los perfiles ocupados por el personal en DataSec SAS no solo ha proporcionado una comprensión precisa de los requisitos de cada función, sino que también ha enfatizado la necesidad primordial de contar con una sólida base en ciberseguridad para alcanzar el éxito en estas responsabilidades. Esta orientación ha llevado a una alineación estratégica de la formación ofrecida en el plan de capacitación con las demandas específicas del SOC, facilitando así una preparación efectiva para abordar los desafíos presentes y futuros en el campo de la ciberseguridad.

Además, determinar las habilidades y conocimientos necesarios para desempeñarse en el área de la ciberseguridad mediante un modelo de competencias adaptado a las necesidades específicas de la organización posibilita una evaluación objetiva de los colaboradores, lo que facilita la identificación de áreas de mejora y la elaboración de planes de desarrollo personalizados. Este enfoque integral no solo fortalece las competencias existentes del equipo, sino que también sienta las bases para un plan de capacitación continuo, permitiendo una constante actualización de habilidades y conocimientos en el campo de la ciberseguridad. En consecuencia, el uso de un modelo de competencias no solo ha identificado y desarrollado las habilidades necesarias, sino que también proporciona una herramienta invaluable para el diseño de un plan de capacitación sólido en ciberseguridad.

La elaboración de un programa de formación en ciberseguridad respaldado por cursos de Cisco, Fortinet e ISC2 permite enfrentar la escasez de profesionales en su Centro de Operaciones de Ciberseguridad SOC. La integración de temas clave y certificaciones de prestigio no solo garantiza a los estudiantes una formación integral y sólida, sino que también posiciona a Datasec SAS como referente en el sector al contar con profesionales altamente capacitados y actualizados. Este enfoque proactivo no solo aborda la problemática actual de la empresa, sino que también establece un camino claro para identificar y cultivar futuros expertos en seguridad cibernética, asegurando así la resiliencia y competitividad continua en el cambiante panorama de la ciberseguridad.

En conclusión, el plan de capacitación en ciberseguridad para el Centro de Operaciones de Seguridad (SOC) de Datasec SAS marca un paso importante en la estrategia de la empresa para abordar los desafíos en constante evolución de la seguridad cibernética. Al identificar con precisión las habilidades y competencias necesarias, y al elaborar un programa integral que abarca desde la formación básica hasta la especialización avanzada, se establecen las bases para la preparación efectiva del personal en todos los niveles de experiencia. Al utilizar un modelo de

competencias adaptado a las necesidades específicas del SOC, se logra una evaluación objetiva del personal y se facilita el diseño de planes de desarrollo personalizados, lo que garantiza una mejora continua en las capacidades del equipo. La integración de cursos y certificaciones de prestigio respaldados por líderes de la industria en ciberseguridad no solo asegura una formación actualizada y de alta calidad, sino que también posiciona a Datasec SAS como un referente en el ámbito de la seguridad cibernética. Este enfoque proactivo no solo beneficia a la empresa, sino que también contribuye al fortalecimiento del ecosistema de seguridad cibernética en Colombia, preparando a individuos capacitados para superar las amenazas emergentes y proteger los activos digitales de manera efectiva.

En última instancia, el diseño de este plan de capacitación permite a Datasec SAS enfrentar la demanda de profesionales al proporcionar una formación integral y actualizada, y establecer un camino claro para el desarrollo y retención del talento en un campo altamente demandado y competitivo. Esto garantiza que el SOC esté equipado con un equipo capacitado y preparado para abordar eficazmente las amenazas cibernéticas emergentes, asegurando así la protección de los activos digitales de la empresa y su competitividad en el mercado.

10. RECOMENDACIONES

Realizar evaluaciones periódicas del desempeño del personal del SOC ayudará a identificar habilidades y áreas de mejora de manera continua, lo que permitirá ajustar el plan de capacitación según las necesidades específicas del equipo. Promover un ambiente propicio para que los miembros del equipo compartan comentarios y sugerencias sobre el plan de capacitación y sus necesidades individuales, contribuirá a que el diagnóstico del perfil sea más preciso y completo.

Establecer un comité de especialistas en ciberseguridad dentro y fuera de la empresa para revisar y validar la aplicabilidad y vigencia del modelo de competencias facilitará que se reflejen con precisión las habilidades y conocimientos requeridos en el campo. Esto brindará una guía más sólida para el desarrollo del plan de capacitación. Dado que el panorama de la ciberseguridad está en constante evolución, es importante revisar y actualizar el modelo de competencias periódicamente para garantizar que refleje los cambios en las amenazas y tecnologías emergentes, manteniendo así la relevancia del plan de capacitación.

Además del programa inicial, implementar programas de aprendizaje continuo y desarrollo profesional permitirá al personal del SOC mantenerse actualizado con las últimas tendencias y tecnologías en ciberseguridad, fortaleciendo así su capacidad para enfrentar las amenazas en constante cambio. La inclusión de ejercicios prácticos, salas de crisis y simulaciones de incidentes de seguridad en el programa de capacitación proporcionará a los participantes experiencias realistas que mejorarán su capacidad de respuesta y toma de decisiones ante situaciones reales en el SOC.

Datasec podría establecer un sistema estructurado para identificar y premiar a los colaboradores que demuestren un alto nivel de alineación con el modelo de competencias de la organización y un rendimiento excepcional en sus funciones. Estos planes de reconocimiento podrían incluir incentivos financieros, oportunidades de desarrollo profesional, ascensos, reconocimientos públicos y otros beneficios que motiven y fidelicen a los profesionales clave del SOC. La implementación de estas prácticas no solo fortalecerá el compromiso y la satisfacción de los colaboradores, sino que también contribuirá significativamente a prevenir la fuga de talento, asegurando la retención de profesionales altamente calificados en un campo tan demandado como la ciberseguridad.

Finalmente, con el objetivo de fortalecer la estrategia de captación de talento especializado en ciberseguridad, se sugiere que Datasec SAS establezca canales de comunicación con universidades de Bogotá que ofrezcan programas de formación virtual en disciplinas afines como Ingeniería de Sistemas, Ingeniería de Telecomunicaciones o Ingeniería Eléctrica. La empresa podría contactar a estas instituciones para presentar la propuesta de socializar el plan de capacitación en

ciberseguridad con estudiantes en curso de dichas carreras. Este enfoque no solo permitirá identificar y atraer a jóvenes talentos interesados en ciberseguridad, sino que también establecerá una vía efectiva para la vinculación de aquellos que demuestren un desempeño destacado en el programa. Los estudiantes que completen el programa de formación con los mejores resultados podrían ser considerados como candidatos preferentes para futuras oportunidades laborales, especialmente para roles clave como Analistas SOC N1. Esta estrategia no solo contribuirá a satisfacer las necesidades de talento especializado de Datasec, sino que también fortalecerá la colaboración entre la empresa y las instituciones educativas, creando un flujo constante de profesionales preparados y alineados con los estándares del Centro de Operaciones de Ciberseguridad.

BIBLIOGRAFÍA

ALMANZA, Andrés R. Resiliencia digital: La nueva frontera para las organizaciones del siglo XXI. Sistemas [en línea] 2021 junio, Núm. 159, 105-120. [Consultado: 9 de mayo 2023] Disponible en: https://doi.org/10.29236/sistemas.n159a4

CHAVEZ HERNANDEZ, Noé. La gestión por competencias y ejercicio de coaching empresarial, dos estrategias internas para la organización. Pensamiento & Gestión, núm. 33, 2012, p. 140-161

CIO MEXICO. [Sitio web]. México: CIO México, Cinco habilidades que un analista SOC debe poseer. [Consultado: 9 de mayo 2023] Disponible en: https://cio.com.mx/cinco-habilidades-que-un-analista-de-soc-debe-poseer/ .

CISCO NETWORKING ACADEMY. [Sitio web]. Cisco Networking Academy, Introducción a la ciberseguridad. [Consultado: 9 de mayo 2023] Disponible en: https://www.netacad.com/es/courses/cybersecurity/introduction-cybersecurity

CISCO NETWORKING ACADEMY. [Sitio web]. Introduction to Cybersecurity [Consultado: 5 de enero de 2024] Disponible en https://www.netacad.com/courses/cybersecurity/introduction-cybersecurity

DÍAZ ISMODES, David. Definición y control de competencias. Presentación realizada en la Conferencia de la Región SAM de la OACI [en línea] 2012 octubre, 5-11 [Consultado: 9 de mayo 2023] Disponible en: https://www.icao.int/SAM/Documents/2012/DSOSYMP12/Definici%C3%B3n%20y%20control%20de%20Competencias%20.pdf

EDICIONES DE LA UNIVERSIDAD DE CASTILLA-LA MANCHA. [Sitio web]. Castilla, NAVARRO, Esteban, LARRIVA-NOVO, X. A., & Villagrá, V. A. (2021). Diseño de un sistema de correlación basado en software libre para la detección de anomalías en el campo de la ciberseguridad. [Consulta: 29 de abril 2023] Disponible en https://doi.org/10.18239/jornadas_2021.34.13

ELASTICSEARCH B.V. [Sitio web] Bogotá: Elastic, ¿Qué es Elasticsearch? [Consultado: 8 de mayo 2023] Disponible en: https://www.elastic.co/es/what-is/elasticsearch

FORTINET. [Sitio web] Fortinet Latin-America [Consultado: 5 de enero de 2024] Disponible en: https://training.fortinet.com/local/staticpage/view.php?page=library_getting-started-in-cybersecurity

FORTINET. [Sitio web] Fortinet Latin-America [Consultado: 5 de mayo 2023] Disponible en: https://www.fortinet.com/lat

FORTINET. [Sitio web] Fortinet Latin-America [Consultado: 5 de enero de 2024] Disponible en: https://training.fortinet.com/local/staticpage/view.php?page=fcf_cybersecurity

FORTINET. [Sitio web] Fortinet Latin-America [Consultado: 5 de enero de 2024] Disponible en: https://training.fortinet.com/local/staticpage/view.php?page=library_introduction-to-the-threat-landscape

FORTINET. [Sitio web] Sunnyvale: Fortinet, ¿Qué es un SOC? [Consultado: 5 de mayo 2023] Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/what-is-soc

FORTINET. [Sitio web] Sunnyvale: Fortinet, Ataques de DoS y Ataque DDoS. Tipos de ataques cibernéticos. [Consultado: 2 de mayo 2023] Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks

FORTINET. [Sitio web] Sunnyvale: Fortinet, Cómo prevenir el ransomware. [Consultado: 5 de mayo 2023] Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/how-to-prevent-ransomware

FORTINET. [Sitio web] Sunnyvale: Fortinet, FortiGuard Labs informa que el malware destructor aumenta más del 50 por ciento. [Consultado: 5 de mayo 2023] Disponible en: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent

FORTINET. [Sitio web] Sunnyvale: Fortinet, Información de seguridad y administración de eventos (SIEM). [Consultado: 5 de mayo 2023] Disponible en: https://www.fortinet.com/lat/products/siem/fortisiem

FORTINET. [Sitio web] Sunnyvale: Fortinet, Malware. [Consultado: 5 de mayo 2023] Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/malware

FORTINET. [Sitio web] Sunnyvale: Fortinet, reportar y prevenir el phishing [Consultado: 5 de mayo 2023] Disponible en: https://www.fortinet.com/lat/blog/industry-trends/reconocer-reportar-y-prevenir-el-phishing#:~:text=%C2%BFQu%C3%A9%20es%20el%20phishing%3F,de%20texto%20o%20social%20media.

FORTINET. [Sitio web] Sunnyvale: Instituto de entrenamiento Fortinet Network Security Associate. NSE1 [Consultado: 5 de mayo 2023] Disponible en: https://training.fortinet.com/local/staticpage/view.php?page=nse_1

FORTINET. [Sitio web] Sunnyvale: Instituto de entrenamiento Fortinet Network Security Associate. NSE2 [Consultado: 5 de mayo 2023] Disponible en: https://training.fortinet.com/local/staticpage/view.php?page=nse_2

FORTINET. [Sitio web] Sunnyvale: Instituto de entrenamiento Fortinet Network Security Associate. Course description [Consultado: 5 de mayo 2023] Disponible en: https://training.fortinet.com/local/staticpage/view.php?page=library_fortigate-security

FUNDACIÓN DIANLNET [Sitio web] Madrid: ACOSTA, Pastor A. Capacitación profesional y formación especializada en ciberseguridad. Cuadernos de Estrategia, p. 291-350. [Consultado: 25 de abril 2023] Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6115627

HARVARD BUSINESS REVIEW. [Sitio web] Cambridge: D. David, 5 Models for the Post-Pandemic Workplace. [Consultado: 28 de abril 2023] Disponible en: https://hbr.org/2021/06/5-modelsfor-the-post-pandemic-workplace

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS [Sitio web]. New Jersey: PACHECO, F, Simulación de respuesta ante incidentes de ciberseguridad para aprendizaje en organizaciones y en el aula. [Consultado: 25 de abril 2023] Disponible en: https://ieeexplore.ieee.org/document/9939841/authors#authors

INSTITUTO NACIONAL DE CIBERSEGURIDAD ES CIBERSEGURIDAD [Sitio web]. España: INCIBE, Protege tu empresa - Glosario de términos de ciberseguridad, una guía de aproximación para el empresario. [Consultado: 28 de abril 2023] Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

ISC2 CC (2024) Ciberseguridad formación en línea a su propio ritmo Cybersecurity [Consultado: 5 de enero de 2024] Disponible en https://www.isc2.org/training/online-self-paced/spanish

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES [Sitio web]. Bogotá: MinTic, Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [Consultado: 28 de abril 2023] Disponible en:https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MIT TECHNOLOGY REVIEW [Sitio web] España: WINICK, E. La falta de expertos en ciberseguridad obliga a recurrir a estudiantes. [Consultado: 27 de abril 2023] Disponible en: https://www.technologyreview.es/s/10614/la-falta-de-expertos-en-ciberseguridad-obliga-recurrir-estudiantes.

NATIONAL INSTITUTE OF SATNDARDS AND TECHNOLOGY. PETERSEN [Sitio web] R, Maryland: ANDERSON, Zia. Workforce Development Toolkit It's all on NICCS 32nd Annual Conference. [Consultado: 21 de abril 2023] Disponible en: https://csrc.nist.gov/CSRC/media/Events/FISSEA-32nd-Annual-Conference/documents/Track_3/FISSEA%20Presentation_Anderson%20EA%20approved.pdf

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) [Sitio web]. Maryland**:** NICE, Cybersecurity Workforce Framework Revisions. NICE Framework Resource Center. [Consultado: 25 de abril 2023] Disponible en: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-framework-revisions

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) [Sitio web]. Maryland**:** NICE, Framework Resource Center [Consultado: 25 de abril 2023] Disponible en: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

PLAY MARKETING. [Sitio web]. CASALLAS, Daniela, Tendencias de seguridad cibernética "no técnicas" para 2023. [Consultado: 9 de mayo 2023]. Disponible en: https://playmarketing.net/tendencias-de-seguridad-cibernetica-no-tecnicas-para-2023/

PULZO [Sitio web]. Bogotá: LOZANO, D, Faltan profesionales de ciberseguridad en Colombia: hay casi 3 millones de vacantes. [Consultado: 28 de abril 2023] Disponible en:https://www.pulzo.com/tecnologia/ciberseguridad-colombia-hay-casi-3-millones-vacantes-PP2130987A

RSUBSECRETAÍA DE PLANIFICACIÓN Y POLÍTICA SECTORIAL E INTERSECTORIAL. Propuesta de niveles de competencia para el catálogo nacional de cualificaciones Ecuador. Quito: Dirección De Políticas Sectoriales E Intersectoriales, 2015, p. 5-9 Disponible en https://www.oitcinterfor.org/sites/default/files/file_publicacion/Niveles-de-Competencia-para-Examinados.pdf

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. [Sitio web]. Washington, DC: V. BERRY, Modelo de competencias para ciberseguridad. [Consulta: 29 de abril 2023] Disponible en: https://www.chcoc.gov/content/competency-model-cybersecurity

URCUQUI LÓPEZ, Christian Camilo; GARCÍA PEÑA, Melisa; OSORIO QUINTERO, José Luis y NAVARRO CADAVID, Andrés. Ciberseguridad. Un enfoque desde la ciencia de datos. Cali: Editorial Universidad Icesi, 2018, p. 23-73

ANEXOS

Anexo A Enlace Video socialización de propuesta Fernando Serrano.

https://youtu.be/bDW6c8qVNWI