REPÚBLICA DE PANAMÁ
UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE PASANTIA REALIZADA EN LA EMPRESA TELERED S.A.

PASANTÍA DE EXTENSIÓN PROFESIONAL OCUPACIONAL PARA OPTAR AL GRADO DE LICENCIATURA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD

Tutor: Prof. José Luis Munive De León

Autor: Gilberto Abraham Rodríguez Arrocha

Ciudad de Panamá, julio 2024

REPÚBLICA DE PANAMÁ
UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE PASANTIA REALIZADA EN LA EMPRESA TELERED S.A.

PASANTÍA DE EXTENSIÓN PROFESIONAL OCUPACIONAL PARA OPTAR AL GRADO DE LICENCIATURA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD

Autor: Gilberto Abraham Rodríguez Arrocha

Ciudad de Panamá, julio 2024

Carta de Aprobación del Tutor

Ciudad de Panamá, 02 de julio de 2024

Profesor. Nagib Yassir

Coordinador Comité de Titulación de Estudios de Licenciatura.

Presente.

En mi carácter de Tutor del Trabajo de Grado presentado por el Bachiller Gilberto Abraham Rodríguez Arrocha, documento de identidad (cédula o pasaporte) N.º 8-825-1169, para optar al grado de, Licenciatura en Ingeniería en Redes de Comunicaciones con énfasis en Seguridad considero que el trabajo: reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado examinador que se designe.

Atentamente,

_____

Ingeniero José Luis Munive De León
8-804-492

Línea de Investigación: Redes y Seguridad

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE ACTIVIDADES DE TUTORÍA OPCIÓN DE TITULACIÓN DE TRABAJO DE GRADO DE LICENCIATURA

Estudiante: Gilberto Abraham Rodríguez Arrocha

Ced. 8-825-1169

Tutor: Ingeniero José Luis Munive De León

Ced. 8-804-492

Correo electrónico del participante: gilberto.rodriguez@unicyt.net

Celular No. 60663440.

Título tentativo del trabajo de pasantía de extensión ocupacional profesional (PEOP).Informe de pasantía en la empresa Telered S.A.

Licenciatura en Ingeniería en Redes de Comunicaciones con énfasis en Seguridad

Línea de Investigación: Telecomunicaciones

Sesión	Fecha	HORA REUNIÓN	ASPECTO TRATADO	OBSERVACIÓN
1	04/08/2023	10:00 am	Revisión de inicial y asignaciones semanales	ok
2	04/08/2023	10:00 am	Diseño e implementación del servidor, la topología de cámaras y asignación de puerto.	ok

3	09/08/2023	09:00 am	Adecuaciones al servidor en tema de hardenizado.	ok
4	16/08/2023	09:00 am	Instalación y configuraciones los nuevos equipos en Panamá Pacifico, PID e IDC´s	ok
5	25/09/2023	05:00 pm	Revisiones, adecuaciones y documentación final.	ok
6	29/09/2023	02:00 pm	Entrega del Proyecto	ok
	01/07/2024	02:00 pm	Revisión con el tutor asignado	ok

Declaramos que las especificaciones anteriores representan el proceso de dirección del trabajo de grado arriba mencionado.

Firma Tutor

Firma Estudiante

AGRADECIMIENTO

En primer lugar, quisiera darle gracias a Dios por darme la energía, salud, comprensión, paciencia y capacidades necesarias para obtener esta victoria y seguir luchando para cumplir con todos mis objetivos.

Quiero agradecer a mi familia por apoyarme en todo momento, tanto en las buenas como en las malas, que gracias su gran apoyo y sin sus consejos no podía cantar **¡victoria!,** puesto que, el momento de decir **¡He logrado esta meta!** a llegado.

También, deseo agradecer a la empresa **TELERED,S.A.,** lugar donde laboro actualmente, por permitirme esta gran oportunidad, un lugar donde poder desarrollar todo mi conocimiento adquirido en mis estudios universitarios a través de la pasantía laboral dentro de esta empresa.

Por último, pero no menos importante, le agradezco a la Universidad Internacional de Ciencia y Tecnología, a su cuerpo administrativo, por la magnífica gestión y también a cada uno de mis profesores, mi tutor y a mis compañeros por inculcar en mí, todos sus conocimientos técnicos, teóricos y su experiencia de vida profesional durante todo el recorrido de esta carrera.

INDICE GENERAL

ÍNDICE DE IMÁGENES

REPÚBLICA DE PANAMÁ

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE PASANTÍA REALIZADA EN LA EMPRESA TELERED S.A.

Tutor: Prof. José Luis Munive De León

Autor: Gilberto Abraham Rodríguez Arrocha

Año: 2024

RESUMEN

Por medio del siguiente informe, Procederé a explicar los conceptos teóricos más básicos e importantes que debe conocer una persona para poder llevar a cabo las funciones que realiza el analista de seguridad dentro de una organización. Es necesario que la gestión del analista no perjudique la dinámica organizacional existente, sino que, por el contrario, la beneficie. En cuanto veamos el desarrollo práctico que conlleva esta gestión, entenderemos que hablamos de responsabilidades como las siguientes: La administración de los accesos físicos y digitales a la infraestructura de la organización, la evaluación de las posibles vulnerabilidades del sistema en relación a los riesgos de seguridad, responder a incidentes de seguridad, proponen e implementan estrategias de mejoras para la mitigación de riesgos a través de controles de seguridad apropiados para salvaguardar la información y la infraestructura de la organizacional. Finalizamos con los detalles que se manejan bajo una gestión de este tipo, junto con las conclusiones y líneas futuras de trabajo en esta área.

Palabras Clave: Seguridad, implementación, vulnerabilidad, información, riesgo.

REPUBLIC OF PANAMA

INTERNATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTER SCIENCE AND TECHNOLOGY

INTERNSHIP REPORT CARRIED OUT AT THE TELERED S.A. COMPANY

Tutor: Prof. José Luis Munive De León

Author: Gilberto Abraham Rodríguez Arrocha

Año: 2024

ABSTRACT

Through the following report, I will proceed to explain the most basic and important theoretical concepts that a person must know in order to carry out the functions performed by the security analyst within an organization. It is necessary that the analyst's management does not harm the existing organizational dynamics, but, on the contrary, benefits it. As soon as we see the practical development that this management entails, we will understand that we are talking about responsibilities such as the following: The administration of physical and digital access to the organization's infrastructure, the evaluation of possible system vulnerabilities in relation to security risks , respond to security incidents, propose and implement improvement strategies for risk mitigation through appropriate security controls to safeguard the information and infrastructure of the organization. We conclude with the details that are handled under a management of this type, along with the conclusions and future lines of work in this area.

Keywords: Security, vulnerability, information, risk, implementation.

INTRODUCCIÓN

El presente informe se realiza con el propósito de mostrar las actividades realizadas en la empresa Telered, S.A. como parte de la pasantía.

Durante la pasantía se realizarán funciones de analista de seguridad Jr. Como también estaré involucrado en la realización del Proyecto de Renovación de sistemas de videovigilancia, para el robustecimiento y mejoramiento del desempeño de dicho sistema.

Telered S.A. es una empresa que presta servicios como autopista transaccional de los diferentes bancos de la república, ubicada en ciudad de Panamá, Howard, Edificio 3835, Panamá Pacífico, Boulevard Business Park, piso 6.

La pasantía consiste en la implementación de un sistema de videovigilancia desde cero para disponer de una infraestructura de nueva generación con altos niveles de disponibilidad y calidad en tema de videovigilancia, que le permitirá reducir las incidencias en la grabación de video y el descarte de las cámaras dañadas o apagadas, incrementando la seguridad de las diferentes ubicaciones que administra la empresa.

CAPÍTULO 1.

Marco referencial de la empresa

1.1 Definición de la universidad y carrera que se estudia

1.1.1 UNICyT (Universidad Internacional de Ciencias y Tecnología)

Nuestro modelo pedagógico trabaja alineado con el aprendizaje colaborativo, donde los estudiantes son el centro del proceso de enseñanza y aprendizaje. Los programas académicos de pregrado, grado y postgrado que ofrece la Universidad Internacional de Ciencia y Tecnología (UNICyT) articulan todo un sistema de recursos orientados a facilitar su aprendizaje, basado en el principio de aprender a aprender. De esta forma, el escenario de aprendizaje se estructura poniendo a su disposición, por un lado, todos los recursos necesarios para optimizar su aprendizaje y, por otro, herramientas tecnológicas que permitan la interacción y participación con el resto de agentes de la comunidad educativa que intervienen en el proceso educativo. Además, ponemos en marcha estrategias pedagógicas que guían y orientan su aprendizaje para facilitar el camino a la consecución de los objetivos establecidos en las acciones formativas.

1.1.2 Licenciatura en Ingeniería en Redes de Comunicaciones con énfasis en Seguridad

Formar excelentes profesionales en el campo de las telecomunicaciones con capacidades para crear, planificar, diseñar, dirigir y ejecutar proyectos de redes e implementar procedimientos y políticas de seguridad tanto en entidades públicas como privadas con altos estándares de calidad, utilizando las herramientas acordes a los avances tecnológicos con alto sentido ético y profesionalismo.

Ilustración 1: Logo de la carrera.

1.2 Antecedentes de la empresa

Ilustración 2: Logo de la empresa

TELERED, S.A, es la empresa líder en el desarrollo de medios de pagos electrónicos en Panamá, contribuyendo al desarrollo económico del país a través de sus plataformas tecnológicas ACH Directo, Mis Pagos Hoy, hub de pagos que conecta las bancas en línea con las empresas facturadoras, y su filial PID (Procesamiento de Imágenes y Documentos).

Cuentan con una infraestructura soportada por tecnología que posee la capacidad y velocidad necesaria para implementar nuevas aplicaciones, y conectan a entidades nacionales e internacionales, ya sean privadas o públicas, por medio de una

infraestructura de comunicaciones que trasmite de forma segura y confiable la información con las Instituciones Financieras afiliadas.

"Somos una empresa 100% panameña, con el compromiso de todos y cada uno de los colaboradores de la organización, quienes con esmero, entusiasmo y dedicación han acogido como propio este reto de transformar el mercado, encarando con responsabilidad los desafíos de un entorno cada vez más exigente, a la altura de una compañía como Telered".

Alexander Acosta

Vicepresidente Ejecutivo y Gerente General

1.3 Cobertura

Con casi 30 años en el mercado, el SISTEMA Clave cuenta con más de 2 millones de tarjetas emitidas, más de 2 mil cajeros automáticos, una gran cantidad de puntos de venta y plataformas digitales de comercios aliados que permiten realizar transacciones e-commerce con e-Clave, a lo largo de todo el país. Todos estos beneficios se brindan a través de los distintos servicios orientados a personas, empresas e instituciones financieras.

1.4 Trayectoria de la Empresa

Con más de **30 años de experiencia**, lideramos la evolución de los servicios financieros electrónicos mediante plataformas automatizadas que nos han convertido en la autopista transaccional de Panamá, brindando a sus tarjetahabientes importantes beneficios y servicios que facilitan la vida de sus usuarios, tales como, retiro de efectivo en cajeros, recarga y pagos de servicios públicos y privados, envío de giros a nivel nacional, compras en más 26 mil comercios a lo largo de la República de Panamá, entre otros. Cuenta con más de 2,200 cajeros automáticos y 36 Instituciones Financieras afiliadas a la Red Clave.

Ilustración 4: Trayectoria de la empresa.

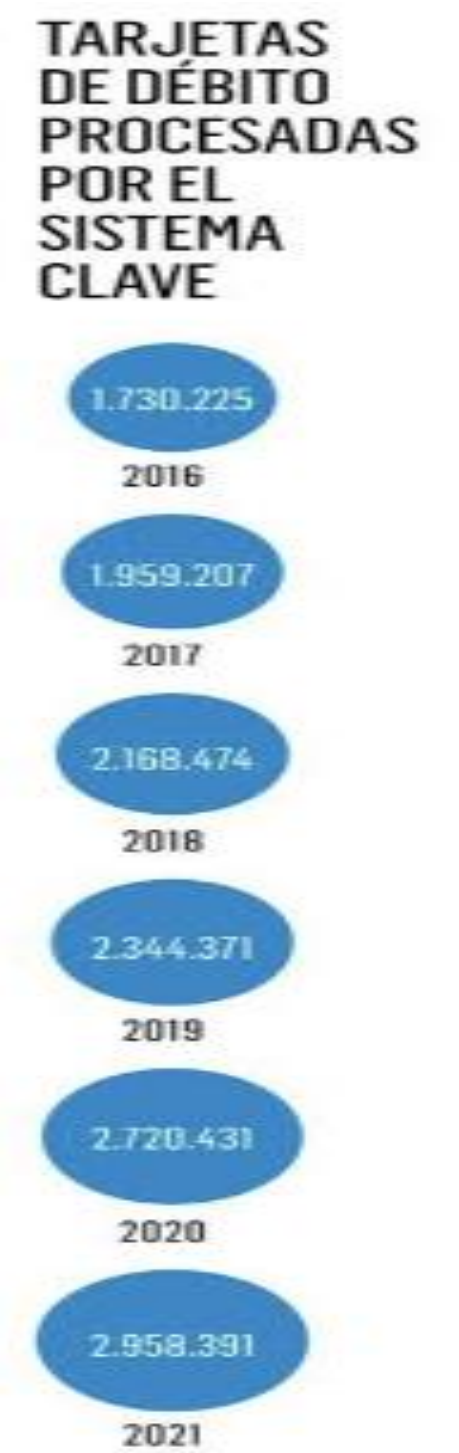


Ilustración 3: Crecimiento del sistema clave en Panamá

1.5 Misión de la Empresa

Ser la mejor solución de procesamiento electrónico de transacciones e información.

1.6 Vision de la Empresa

Convertir el manejo de efectivo en pagos electrónicos.

1.7 Perfil de la Empresa

Son una empresa de capital panameño, con 30 años de experiencia en el mercado y que provee soluciones a Instituciones Financieras, que facilitan el intercambio de transacciones y pagos de forma electrónica.

La junta de accionistas de TELERED está conformada por Bancos cuya solidez y experiencia aportan a la empresa un gran respaldo y confiabilidad en los servicios que brinda.

1.7.1 Política de Calidad

En Telered, S.A. estamos comprometidos en brindar productos y servicios de alta calidad al sector financiero y comercial, en miras de superar las expectativas y necesidades de nuestros clientes y accionistas. Por ello, buscamos servir, fortalecer y desarrollar el ecosistema de pagos, con el procesamiento de transacciones en Panamá, a través de tecnología innovadora, agilidad y mejora continua de nuestros procesos, en cumplimiento con los requisitos y regulaciones, y aplicando las prácticas y normas de la industria.

1.8 Beneficios de la Empresa

En Telered no solo se preocupan por el bienestar económico del equipo, también es importante que el colaborador pueda gozar de buena salud y unión familiar, para lo cual han desarrollado un paquete de beneficios que aportan valor a la vida de cada uno de sus colaboradores:

- ✓ Actividades recreativas y deportivas
- ✓ Adelanto de salario
- ✓ Aguinaldo
- ✓ Anualidad de la tarjeta Clave
- ✓ Apoyo para gastos funerarios
- ✓ Bonificación por desempeño
- ✓ Consulta médica mensual
- ✓ Vale de alimentación

- ✓ Días de asueto remunerado
- ✓ Póliza de vida y gastos médicos
- ✓ Programa de wellness
- ✓ Reconocimiento por años de servicio
- ✓ Sábados libres
- ✓ Sala de lactancia

1.9 Productos de la Empresa

Ilustración 5: Productos de la empresa

La marca **SISTEMA Clave** ofrece múltiples servicios de transacciones electrónicas realizadas a través de distintos canales, como cajeros automáticos, puntos de venta y comercio electrónico local, disponibles a través de las Instituciones Financieras con licencia general.

ACH Directo es un sistema de transferencia electrónica de fondos que brinda exactitud, seguridad, comodidad y rapidez a todos sus usuarios y beneficiarios, directos e indirectos, enlazando electrónicamente a las instituciones financieras, a las empresas y a las personas naturales para agilizar su pagos y cobros.

Mis Pagos Hoy es un servicio que conecta, en una misma plataforma tecnológica, a las Instituciones Financieras con empresas de servicios. Los clientes pueden gestionar sus pagos a través de la página web de su banco y disponer del saldo de forma inmediata, en cualquier momento y desde cualquier lugar.

PID, Este servicio ofrece la posibilidad de tercerizar el procesamiento de documentos, para los bancos miembros del sistema bancario panameño, logrando mayor agilidad y

eficiencia en los tiempos de gestión. Es un servicio seguro y confiable que permite procesar los cheques enviados y recibidos con la finalidad de ser procesados por PID y enviados al cobro a través de la Cámara de Compensación del Banco Nacional de Panamá.

1.10 Descripción del Departamento

El departamento de seguridad se encarga de salvaguardar la toda infraestructura tanto física como lógica de la empresa y de los clientes con los cuales esta interactúa.

El objetivo principal de un Departamento de Seguridad es proteger a la organización contra amenazas internas y externas. Sus responsabilidades pueden variar según el tipo de empresa y sector, entre ellas están las siguientes:

- **Gestión de riesgos:** Identificar, evaluar y reducir los riesgos de seguridad en todos los niveles de la organización, desde la infraestructura tecnológica hasta los procedimientos operativos y la formación de empleados.
- **Protección de activos:** Garantizar la seguridad física de las instalaciones, equipos y recursos críticos de la organización. Esto puede implicar la implementación de sistemas de vigilancia, controles de acceso y políticas de seguridad.
- **Seguridad de la información:** Salvaguardar los datos sensibles y confidenciales de la organización contra amenazas como el acceso no autorizado, el robo, el malware y los ataques cibernéticos. Esto implica el desarrollo e implementación de políticas de seguridad de la información, la realización de auditorías y la formación de los empleados sobre las mejores prácticas de seguridad.
- **Respuesta a incidentes:** Preparación para manejar eficientemente cualquier incidente de seguridad que pueda ocurrir. Esto incluye la detección temprana, la planificación e investigación posterior al incidente.

Tabla 1 - Los Roles y las responsabilidades están divididas de la siguiente manera:

Responsable	Funciones
Gerente de Seguridad	• Liderar el equipo de trabajo. • Toma de decisiones de Alta Gerencia. • Asignar responsabilidades a los supervisores. • Identifica posibles riesgos.
Supervisor de Seguridad	• Administrar la seguridad de la Infraestructura Tecnológica. • Atender y remediar los hallazgos de auditoría. • Gestión de usuario a las herramientas y/o aplicaciones que brinda la Organización. • Participar en el análisis, diseño y pruebas de aspectos de seguridad en las diferentes iniciativas y proyectos. • Ejecutar e Identificar vulnerabilidades en la Infraestructura Tecnológica. • Proponer políticas, procedimientos y metodologías apropiadas para la gestión de la Seguridad. • Vigilar los lineamientos necesarios sobre los servicios de seguridad ofrecidos. • Apoyar en las estrategias enfocadas a la seguridad. • Divulgar y concientizar a los colaboradores en el cumplimiento de las políticas de seguridad. • Preparar a los grupos de trabajos ante posibles incidentes de seguridad y activar el Plan de Respuesta de Incidentes. • Proponer mejoras y participar en el desarrollo e implementación de nuevos proyectos. • Mantener la confidencialidad de la información manejada en el área. Atender y evidenciar solicitudes a las diferentes auditorias (Internas y Externas). • Planificar, coordinar y gestionar las actividades del área con su

	equipo de trabajo. • Darle seguimiento al cumplimiento de las actividades asignadas a su equipo de trabajo. • Gestionar las actividades administrativas correspondientes a su equipo de trabajo (control de objetivos, planificación de vacaciones/permisos, horas extras, oncall, entre otros.) • Gestionar los planes de desarrollo individual de su equipo de trabajo.
Supervisor en Prevención de Fraudes	• Atender y remediar los hallazgos de auditoría. • Participar en el análisis, diseño y pruebas de aspectos para la prevención de fraude en las diferentes iniciativas y proyectos. • Proponer políticas, procedimientos y metodologías apropiadas para la gestión en la prevención de fraude. • Vigilar los lineamientos necesarios sobre los servicios para la prevención de fraude ofrecidos. • Apoyar en las estrategias enfocadas a la prevención de fraude. • Preparar a los grupos de trabajos ante posibles incidentes de para la prevención de fraude y activar el Plan de Respuesta de Incidentes. • Proponer mejoras y participar en el desarrollo e implementación de nuevos proyectos. • Mantener la confidencialidad de la información manejada en el área. • Atender y evidenciar solicitudes a las diferentes auditorias (Internas y Externas). • Planificar, coordinar y gestionar las actividades del área con su equipo de trabajo. • Darle seguimiento al cumplimiento de las actividades asignadas a su equipo de trabajo. • Gestionar las actividades administrativas correspondientes a su

	equipo de trabajo (control de objetivos, planificación de vacaciones/permisos, horas extras, oncall, entre otros.) • Gestionar los planes de desarrollo individual de su equipo de trabajo.
Arquitecto de Seguridad	• Encargado de ubicar y mitigar todas las vulnerabilidades en el perímetro de empresa.
Analista de Cumplimiento	• Encargado de validar que el diseño, desarrollo e implementación de los proyectos en el área de seguridad cumplan con las normativas regulatorias. • Auditor de Sistemas o de IT, o de Cumplimiento IT, Conocimientos en ISO 27001 u otra ISO de Seguridad de la Información, SOX, PCI DSS, o estándares globales relacionados, Conocimientos amplios en tecnología.
Analista de Ciberseguridad	• Levantar los informes de monitores con alertas y hallazgos. • Realizar seguimientos de los hallazgos y proponer remediaciones ante cualquier mal funcionamiento de las herramientas. • Apoyar en las tareas asignadas para la atención y cumplimiento con las auditorías de los sistemas en PCI PIN, PCI SS y KPMG. • Realizar monitoreo de vulnerabilidad. • Realizar prueba anual correspondiente al plan de respuesta de Incidentes de seguridad. • Mantener diariamente actualizadas las herramientas que aseguren la protección de la información. • Verificar diariamente el correcto funcionamiento de las herramientas. • Brindar soporte y Threat Hunting a los logs. Monitorear los accesos a la información mediante las distintas herramientas SIEM y CYNET.
Analista especialista	• Administración y desarrollo de las principales herramientas para la prevención del fraude.

en Monitoreo de fraude.	• Realizar monitoreos diariamente a los movimientos transaccional de las tarjetas claves. • Enviar notificaciones a las entidades financieras de las transacciones sospechosas y en listas negras. • Dar respuesta de los oficios a la fiscalía de las diferentes investigaciones de transacciones sospechosas. • Preparar reportes estadísticos para el envío de informes a las instituciones financieras afiliadas al servicio de prevención de fraude. Dar atención y respuesta a las solicitudes emitidas por la mesa de servicios de la empresa, relacionadas con los reclamos por transacciones no reconocidas. • Atender las consultas diarias por parte de las instituciones financieras.
Analista de seguridad	• Asistir a la Gerencia de Seguridad en la elaboración de políticas de seguridad basadas en las mejores prácticas de la industria. • Velar, en conjunto con otras áreas de la empresa, por el cumplimiento de políticas, procedimientos y controles internos relacionados con el aseguramiento de los recursos informáticos e instalaciones de la empresa. • Desarrollo y mantenimiento de procedimientos internos relacionados a las Administración de la Seguridad. • Recibir y atender consultas y/o solicitudes de usuarios internos y externos en materia de seguridad. • Atender las solicitudes de los clientes con relación a la generación de llaves, certificados y acceso a todos los sitios de la red. • Mantener una documentación organizada y debidamente controlada de la administración de la seguridad, de manera que se tengan disponibles las evidencias. • Monitorear y detectar las desviaciones de las políticas de seguridad y de los controles implementados.

	• Asistir en la administración de herramientas de Seguridad que apoyan la Infraestructura de la empresa, tales como, antivirus, antispam, filtrado de navegación de Internet, directorio activo, encriptado de discos, administración de dispositivos removibles, firewall, entre otros. • Mantener la confidencialidad y estricta discreción de la información manejada en el Departamento de Seguridad. • Asistir al Gerente de Seguridad en la relación con proveedores de la empresa relacionados a su gestión. • Presentar al Gerente de Seguridad los indicadores propios de su gestión. • Participar en el desarrollo de nuevos proyectos.
Analista de Fraude	• Realizar monitoreos diariamente a los movimientos transaccional de las tarjetas claves. • Enviar notificaciones a las entidades financieras de las transacciones sospechosas y en listas negras. • Dar respuesta de los oficios a la fiscalía de las diferentes investigaciones de transacciones sospechosas. • Preparar reportes estadísticos para el envío de informes a las instituciones financieras afiliadas al servicio de prevención de fraude. Dar atención y respuesta a las solicitudes emitidas por la mesa de servicios de la empresa, relacionadas con los reclamos por transacciones no reconocidas. • Atender las consultas diarias por parte de las instituciones financieras. • Preparar y enviar al área de Producto Clave reporte diario del comportamiento de las transacciones de los comercios E-Commerce. • Preparar y enviar un informe diario a la Vicepresidencia y gerencia, por turno de la actividad en general del área.

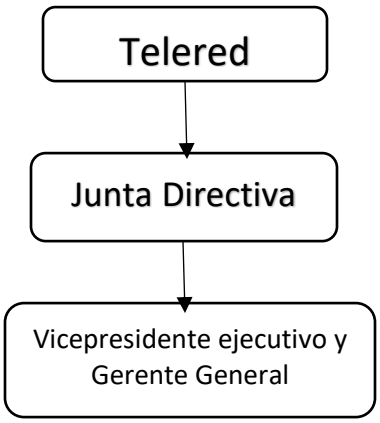
Analista de seguridad jr.	• Atender diariamente las solicitudes de las entidades financieras para la seguridad de cajeros automáticos. • Gestionar las solicitudes de la gestión de accesos a usuarios internos (físicos y lógicos) y externos (entidades financieras y proveedores). • Mantener actualizado la documentación de normativas y procedimientos aplicables a la seguridad de Telered. Evidenciar y sustentar el cumplimiento de los controles requeridos para las auditorías de PCI. • Orientar, asesorar y guiar en las mesas ágiles con relación a temas propios de Seguridad Informática y otros relacionados con su rol. • Ejecutar y documentar los procesos de monitoreo de las diferentes herramientas de Seguridad. • Dar el seguimiento a los hallazgos identificados en los monitoreos realizado hasta el cierre de los mismos. Monitorear el correcto funcionamiento del sistema de videovigilancia y del sistema de acceso físico. • Mantener la comunicación y el manejo con los proveedores de las herramientas que utilizan. • Generar reportes o informes de gestión a solicitud de acuerdo a las necesidades del área Realizar las funciones asignadas de acuerdo a su rol. • Personal encargado de brindar soporte a los clientes Instalaciones y entrega de servicios

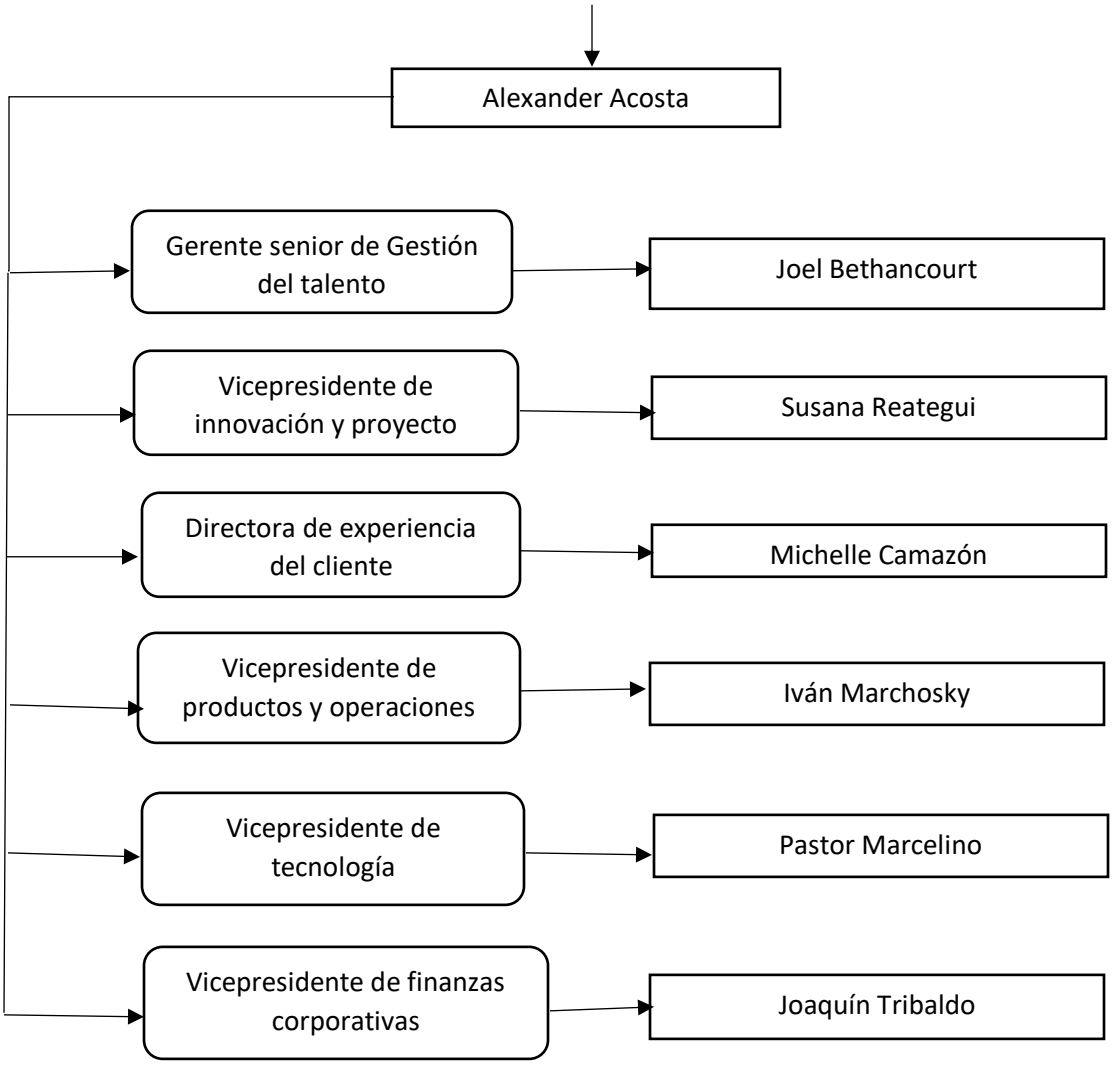
1.11 Mis funciones dentro de la empresa en el periodo de Pasantía.

Durante mi paso por el área de seguridad se me asigno el rol de **Analista de seguridad jr.** Por lo cual, mis funciones fueron las siguientes:

- Atender las solicitudes de las entidades financieras y proveedores a través de los distintos canales de comunicación para realizar cambios en la configuración de los cajeros automáticos.
- Atender las solicitudes de las entidades financieras y proveedores para la creación, modificación y eliminación de accesos a sus colaboradores autorizados en las herramientas de la empresa.
- Gestionar las solicitudes de accesos a usuarios internos (Colaboradores, proveedores y pasantes) según sus roles asignados.
- Proyecto de renovación e implementación completo de un nuevo sistema de monitoreo de cámara para la videovigilancia en las oficinas principales y filiales.
- Ejecutar el monitoreo y documentar los procesos críticos de las diferentes herramientas de Seguridad dentro de la empresa.
- Dar el seguimiento a los hallazgos identificados en los monitoreos realizado hasta el cierre de los mismos.
- Monitorear el correcto funcionamiento del sistema de videovigilancia y del sistema de acceso físico.
- Mantener la comunicación y el manejo con los proveedores de las herramientas que utilizan.
- Generar reportes o informes de gestión a solicitud de acuerdo a las necesidades del área.
- Realizar las funciones asignadas de acuerdo a su rol.

1.12 Estructura Organizacional de la Empresa




Alexander Acosta
Gerente senior de Gestión del talento
Joel Bethancourt
Vicepresidente de innovación y proyecto
Susana Reategui
Directora de experiencia del cliente
Michelle Camazón
Vicepresidente de productos y operaciones
Iván Marchosky
Vicepresidente de tecnología
Pastor Marcelino
Vicepresidente de finanzas corporativas
Joaquín Tribaldo

CAPÍTULO II.

Análisis de la experiencia durante la Pasantía Laboral

2.1 Objetivos de la Pasantía

- Cumplir con el requisito solicitado por la universidad Internacional de Ciencia y Tecnología en el área de Telecomunicaciones de realizar una pasantía laboral en una empresa aplicando los conocimientos adquiridos en clases y a lo largo de la carrera.
- Aplicar los conocimientos teórico-prácticos adquiridos a través de los estudios para enfrentar al Campo Laboral.
- Incrementar la experiencia laboral del estudiante en el ámbito profesional dentro de esta área de aprendizaje.

2.2 Planteamiento del Problema

El modelo de negocio en la empresa **Telered S.A.** es la entrega de nuevos productos a las instituciones financieras acordes los servicios financieros electrónicos mediante plataformas automatizadas, lo cual, ha convertido a esta empresa en la autopista transaccional de Panamá.

Para lograr esta meta es necesario contar con una infraestructura soportada sobre los 3 pilares de la seguridad (Integridad, disponibilidad y confidencialidad) que posea la capacidad y velocidad necesaria para implementar nuevas aplicaciones, y conectar a entidades nacionales e internacionales con sus clientes, ya sean privadas o públicas, por medio de una infraestructura de comunicaciones que trasmite de forma segura y confiable la información con las Instituciones Financieras afiliadas.

El problema con el cual nos hemos encontrado es que la empresa actualmente se maneja con un sistema de videovigilancia basado en la combinación de DVR y NVR con cámaras que actualmente están obsoletas.

Debido mantener esta problemática donde la empresa se ve expuesta. Por distintas anomalías como por ejemplo: En algunas áreas se visualizan puntos ciegos muy notorios, a causa, que algunas cámaras han dejado de funcionar. También se está presentando mucha intermitencia con la comunicación entre las cámaras que se encuentran funcionando y el servidor, que han provocado la perdida en la continuidad de los días de grabación.

La empresa al verse afectada por esta situación, la cual, es crítica para cumplir con las normas y estándares exigidos una empresa dentro del rubro. Ha optado por la implementación de la propuesta para la renovación del sistema de videovigilancia, la cual, consiste en implementar un nuevo sistema de videovigilancia con base en un servidor NVR y cámaras con las especificaciones solicitadas para el proyecto.

2.3 Objetivo General

Implementar el proyecto reemplazo de cámaras para la videovigilancia de las oficinas principales, recintos remotos y filiales según requerimientos de la empresa, realizar entrega a satisfacción y cumplir con las funciones destinadas al rol de asignado dentro de la empresa.

2.3.1 Objetivos Específicos

- Implementar el sistema de videovigilancia diseñado dentro de las diferentes oficinas y filiales de empresa bajo los parámetros tecnológicos y de calidad solicitados.
- Documentar la infraestructura del sistema a manera que permita el continuo funcionamiento de mismo una vez concluida la pasantía.
- Cumplir todas las solicitudes asignadas bajo el rol designado con la mayor eficiencia y responsabilidad posible dentro de los tiempos asignados.

2.4 Marco Teórico

Toda empresa debe tener un departamento encargado de la seguridad informática, el mismo debe tener un liderazgo claro, una normativa bien específica, bajo la cual se deben regir todos los procedimientos.

Lo más importante es tener presente cuales son las normativas que se deben respetar, pero también contar con el personal adecuado para resguardar los intereses de nuestra empresa, y recordar que mientras más sensible sea el área donde nos desempeñemos y la información que manejemos, mayor será la inversión que debe darse en este tópico.

2.4.1¿De qué trata los objetivos de la seguridad informática?

Dada la importancia de este tema, incluso existe la Normativa ISO 27002 , que trata de las buenas prácticas en esta área. Cabe destacar que esta norma es internacional y con ella se determina la forma adecuada del protocolo de prácticas. Para garantizar una buena implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en empresas. En la Normativa siguiente se destacan los objetivos de la seguridad informática:

- **Accesibilidad:**

A pesar de que la persona o departamento encargado de cumplir con los objetivos de la seguridad informática, no debe compartir dicha información . A su vez, debe dejar los accesos correspondientes para que el personal de la empresa pueda revisar o consultar la información cuando sea necesario. Para ello, se debe definir quiénes son las personas autorizadas para acceder a dicha información .

- **Integridad:**

En este caso como profesional en el área de seguridad es necesario asegurar que bajo ningún concepto se pueden modificar datos. Es decir, que la información que

se tramita en el sistema, no puede ser modificada por este profesional. Si bien éste tiene acceso a ellos, no son de su competencia y tampoco es su tarea manipularlo.

- **Confidencialidad:**

Cada día, los hackers utilizan métodos que son una amenaza para la información de las empresas. Es menester que estas tengan un sistema lo suficientemente seguro para soportar los ataques. Por lo tanto, una persona que se encarga de crear, implementar o mantener la infraestructura de seguridad informática debe tener conciencia de que es confidencial. Es decir, que ningún tercero tendrá acceso a dichos datos ni los permisos necesarios.

- **Sin rechazo:**

Cuando hablamos del no rechazo se refiere a la comunicación que existe entre dos partes . Por lo tanto, se trata de una responsabilidad por la que el emisor y receptor no deben rechazar el envío y recepción de información. Ya que de esto depende la garantía de que el sistema funcione correctamente y que la empresa o el encargado de esta área esté al tanto de todo lo que sucede.

2.4.2. Relación entre el departamento de seguridad informática y el resto de la empresa

Normalmente la conformación de las estructuras organizacionales está sujetas a discusión, pese a todos los tratados que se han escrito al respecto. Hay ciertas áreas o unidades de negocios que naturalmente se comprende lo que deben abarcar, pero otras que no es tan obvia su ubicación dentro de un organigrama. Tal es el caso de seguridad informática, ¿o deberíamos decir seguridad de la información? Para el caso no sería lo mismo, veamos por qué.

Es bien sabido que al referirnos a seguridad informática, nos estamos focalizando especialmente en el aspecto tecnológico de la seguridad (desde firewalls y antivirus hasta IDS y DLP) en tanto que seguridad de la información abarca además

aspectos no técnicos (físicos y administrativos, por ejemplo). En el primer caso, pareciera natural pensar que debería depender de algún órgano técnico, como ser el área de sistemas o de tecnologías de la información. De esta manera, dependiendo del tamaño de la empresa, podrá existir una gerencia o una dirección de sistemas, de informática, o de tecnología, de la cual se desprenda el área de seguridad. Esta solución resulta bastante trivial, y es debido a que el verdadero problema se encuentra al intentar ubicar el segundo caso. Ahora pues, se tiene un área que abarca temas relacionados con la tecnología, pero también vinculados a los recursos humanos, al área de legales, y hasta a la vigilancia del edificio.

2.4.3. Analistas de seguridad informática de una empresa

Un analista de seguridad tiene como principal responsabilidad mantener segura la información confidencial de las empresas. Para ello, estos profesionales se dedican a analizar posibles vulnerabilidades y mejorar las medidas de seguridad informática de la empresa. También suele dar formación a otros empleados para que mejoren sus procesos de trabajo en lo que se refiere a las medidas de seguridad de la empresa.

Se trata de un profesional que trabaja a nivel interdepartamental para poder identificar y corregir todos los fallos en los sistemas informáticos de la empresa para la que trabaja. Además, como decimos, es el encargado de proponer soluciones e implementar medidas de seguridad que mejoren el trabajo con medios digitales e Internet en la compañía.

2.4.4. Herramientas del área de seguridad utilizadas por las empresas

A. Antivirus

Los antivirus son programas informáticos diseñados para buscar, identificar y actuar frente a agentes nocivos que puedan amenazar la integridad de un sistema. Estos softwares rastrean patrones o afectaciones en el código de los sistemas y suelen actuar

de forma inmediata para proteger los equipos y erradicar los agentes maliciosos. Cuando las amenazas son significativas, el programa avisa a las compañías que se encuentran ante un riesgo que amerita tomar acciones mayores.

Una de las ventajas de los antivirus es que sus desarrolladores las actualizan constantemente, por lo que están optimizadas para enfrentar los problemas más comunes y novedosos.

B. Antispyware

Los antispyware fueron creados para identificar rupturas y brechas en las paredes de seguridad de los sistemas. Esto con el fin de evitar que agentes de espionaje y robo de datos accedan a tus sistemas y redes.

Estos son muy similares a los antivirus, pero están optimizados para contrarrestar los efectos de un agente intrusivo que no necesariamente busque afectar la operatividad de un sistema, sino extraer información. Los antispyware funcionan como filtros que impiden la entrada de estas amenazas, pero también evalúan el estado de tus equipos para encontrar brechas, erradicar agentes espías y fortalecer tus plataformas.

C. Certificados SSL

Otra herramienta que puede fortalecer tu actividad online son los certificados SSL. Estos recursos dotan de mayor seguridad a los sitios web mediante capas de sockets seguros. Esto significa que, solo cuando se activa un certificado de este tipo, se permite el acceso a un servidor web. Seguro has visto el código «https» al inicio de una URL. Este fragmento indica que el sitio está protegido por un SSL. Esto te garantiza que estás visitando un sitio seguro con un protocolo adecuado para proteger tu información.

Los certificados SSL funcionan como protocolos de acceso que conectan los servidores con el navegador. De este modo, se afianza la seguridad del sistema para llevar a cabo transacciones, ingreso de información y la privacidad del visitante.

D. Almacenamientos de respaldo

Una forma de mantener segura tu información es emplear sistemas de almacenamiento de respaldo. Con esta estrategia, obtendrás historiales o versiones de tu trabajo para

volver en cualquier momento a puntos de control. Aunque pierdas o se dañe un sistema, tendrás la confianza de que no se extraviarán tus datos.

E. Servidores proxy

La función del proxy es mantener la privacidad de un sistema y el anonimato de los usuarios de una red, al momento de solicitar y enviar información. Estos actúan como intermediarios entre un repositorio de datos y un solicitante para tercerizar las solicitudes y filtrar interacciones sin poner en riesgo tu integridad.

Los proxys limitan el tipo de solicitudes que se hacen a tus sistemas, filtran automáticamente los contenidos que entran en tus bases de datos y registran todos los accesos y tráfico a tus redes, mientras garantizan el anonimato de los visitantes a tus sitios y de tus gestores empresariales.

A. Firewall

Los firewalls están emparentados con los antivirus y antispyware, pero funcionan como paredes que bloquean el acceso y salida de información para ser evaluada por medio de su código. Por eso, también son conocidos como cortafuegos. Con un firewall, garantizas que tus sistemas, aplicaciones y equipos se mantendrán seguros al conectarse a la red. Así, detectarás elementos amenazantes con anticipación a su entrada en tus plataformas. A su vez, son útiles para redes locales porque vigilan el tránsito de información entre equipos y personas.

B. Escáneres de vulnerabilidad

Es común confundir los escáneres de vulnerabilidad con los antivirus y antispyware. Esto se debe a que, comúnmente, estos programas incluyen escáneres para detectar amenazas. Sin embargo, son sistemas con funciones diferentes.

Los escáneres de vulnerabilidad evalúan el estado de un sistema, red o plataforma para detectar aquellas zonas más vulnerables y alertar sobre posibles brechas de seguridad. De igual manera, te informan si necesitas actualizar o mantener tus plataformas para tenerlas en las mejores condiciones. Esta herramienta te dará información sobre las

decisiones que debes tomar para proteger tus redes, pero no llevan a cabo acciones correctivas para fortalecer tus plataformas.

C. Encriptadores

Un encriptador está optimizado para codificar archivos, documentos o datos y transmitirlos con la certeza de que no serán legibles en caso de que se extravíen o sean objeto de un robo de información.

Para encriptar un objeto, será necesario contar con un programa que convierta los archivos en un código que, después, se retraducirá por el mismo programa para tu destinatario. Los archivos encriptados también pueden acompañarse de sellos que refuercen la certificación y validación de los usuarios o portadores de datos. Con este recurso, te aseguras de que la información se mantendrá privada y que, solo aquellos con autorización, pueden verla.

D. Generadores de contraseñas

Si utilizas una misma contraseña para todas tus cuentas y dispositivos, te tenemos una mala noticia: el 40 % de las infracciones digitales ocurren por robo de contraseñas. Esto compromete una gran cantidad de plataformas si empleas el mismo código de verificación de identidad. Pero ¿cómo se puede memorizar decenas o cientos de contraseñas para cada uno de tus programas, cuentas y equipos?

Para ayudar a las personas en esta tarea, algunas compañías como han desarrollado generadores de contraseñas que crean y resguardan códigos de seguridad para ser utilizados solo desde ciertos equipos y para cuentas específicas. Estas contraseñas suelen ser complejas y se componen por números, letras y símbolos que dificultan su replicación.

E. VPN

Funciona como una red privada virtual que solo conecta equipos o usuarios específicos e impide que alguien más pueda entrar de manera online a ellas.

Los VPN aprovechan las redes de internet para conectar equipos de punto a punto, pero sin hacerse de acceso público. Con ellas, solo quienes tienen autorización, acceden al sistema y utilizan los datos y canales de comunicación.

2.4.5. ¿En qué consiste el monitoreo de cámaras de seguridad?

El servicio de monitoreo de cámaras con sus respectivas especificaciones, para evitar los hurtos en las empresas; además de vigilar a los empleados para que puedan cumplir sus funciones o no se sustraigan los productos, para la prevención del delito y para la disuasión; sean cual sean las verdaderas motivaciones de quienes usen estos novedosos dispositivos, deben conocer más sobre ello ante de su implementación o para postularse a un puesto laboral como operador de cámaras de seguridad.

2.5. Descripción del trabajo realizado

El trabajo por realizar durante el periodo de la pasantía será la que realiza dentro de la empresa un analista Jr. Con algunas limitaciones en temas de accesos y dentro de la pasantía también se implementó el proyecto de renovación del sistema de videovigilancia a nivel de todos los recintos existentes.

2.5.2. Gestión realizada como Analista Jr. de seguridad.

Se realizaron múltiples funciones administrativas a usuarios internos, externo, invitados y proveedores. Durante mi gestión como Analista Jr. de seguridad gestione el control de accesos a usuarios físicos y virtuales, como también realice la creación, modificación y eliminación de credenciales, entre otras más funciones del puesto asignado.

2.5.3. Proyecto de Renovación de sistemas de videovigilancia.

Este proyecto de implementación de renovación del sistema de videovigilancia está constituido por una serie de equipos de vigilancia (cámaras) que se conectan a un servidor NVR centralizado a través de una red UTP existente.

Este equipamiento debe cumplir con los requisitos de la empresa, entre ellos:

- Almacenamiento para más de 200 días de grabación.

- Interface amigable para el usuario de fácil acceso desde el cliente y desde el servidor.
- Políticas robustas de seguridad.
- Compatible con Windows, Linux o AIX.
- Detector de movimiento por infrarrojos.

En concreto se deben que tener en cuenta aspectos como:

- Tamaño y acondicionamiento del rack (espacio del servidor)
- Equipamiento para cada cámara (Equipos activos y pasivos)
- Control de acceso a las áreas y recintos.
- Personal de planta externa y contratistas.

El nuevo sistema de videovigilancia se integrará de 84 cámaras que llegaran al servidor ubicado en la empresa, a través de un switch de conmutación principal.

La implementación de este proyecto deberá abarcar los siguientes aspectos:

- ✓ Un servidor con una disponibilidad de servicio de 99.95% anual.
- ✓ Soporte para interfaces Gigabit Ethernet y 10 Gigabit Ethernet.
- ✓ Escalabilidad del sistema: puertos disponibles para futura expansión.

2.5.3.1. Montaje de las cámaras (Personal del proveedor)

El montaje de las cámaras se ejecutará utilizando los métodos más adecuados y seguros que garanticen el correcto funcionamiento de la red, a largo plazo, por parte del Proveedor (Ilustración 18).

El método de reemplazo será el siguiente:

Paso 1. Se valida la cámara actual en el servidor viejo si funciona o si pertenece al grupo de las dañadas. Esto se hace para validar la ubicación y el IP Asignado.

Paso 2. Se procede a retirar la cámara vieja de su ubicación e instalar la nueva (Ilustración 19).

Paso 3. Se cambia el puerto en el viejo servidor hacia el nuevo servidor y validamos que levante (Ilustración 16).

Paso 4. Se valida en el nuevo servidor si reconoce la cámara y se le asigna nombre e IP (Ilustración 17).

Paso 5. Ajustamos vista y que responda a los requerimientos exigidos por la empresa.

2.6. Actividades Realizadas durante el periodo de pasantía

2.6.2. Actividades como Analista Jr.

Las principales actividades realizadas como Analista Jr. de seguridad son las siguientes:

- Administración de las herramientas de acceso físicos y virtuales de la empresa.
- Administración de accesos a las herramientas de gestión de las diferentes áreas.
- Aplicación de políticas los Firewall de la empresa.
- Gestión con proveedores.
- Gestión de correos y prevención del ataque Phishing.
- Validación de los reportes de vulnerabilidades.
- Entre otras asignaciones.
- Gestión de reportes diarios asociados a temas de seguridad informados por los usuarios internos de la empresa.

2.6.3. Actividades del Proyecto de renovación del sistema de videovigilancia

2.6.3.1. Implementación del Hardware

Un sistema NVR (grabador de vídeo en red) con cámaras IP proporciona controles de video centralizados para ver, administrar y almacenar videos fácilmente, que se ha utilizado ampliamente en proyectos de vigilancia con cámaras. Por lo general, se usa en una red de videovigilancia IP para recibir imágenes en vivo o secuencias de video y

grabarlas digitalmente en un disco duro, unidad flash USB u otro dispositivo de almacenamiento masivo.

Los usuarios pueden ver, reproducir y descargar grabaciones cuando sea necesario. Por lo general, basado en entornos Windows o Linux, el NVR tiene una interfaz fácil de usar para el uso diario y está equipado con detección de movimiento inteligente y capacidad de control de cámara. El acceso remoto también está disponible con NVR, y otros beneficios incluyen la capacidad de manejar grandes cantidades de transmisiones de video, una instalación simple, etc.

Ilustración 6: Diagrama Base en oficinas principales

2.6.3.1.1. Milestone Husky IVO™ 1800R.

Para esta implementación nos conectaremos a un switch previamente configurado y activo en la red por el área de Comunicación de la empresa, por lo cual, iniciaremos con un sistema Milestone Husky IVO™ 1800R.

Ilustración 7: Milestone Husky IVO 1800R

Es un equipo de alto rendimiento, de arquitectura robusta, diseñado para soportar alto tráfico, de convergencia rápida ante cualquier evento en la red, utilizado mucho en centros de datos.

2.6.3.1.2. Interfaces de gestión

Management Client

XProtect VMS son programas de software de gestión de vídeo diseñados para instalaciones de todas las formas y tamaños. Si quiere proteger su almacenamiento frente actos de vandalismo o quiere manejar una instalación de alta seguridad en varios sitios. Las soluciones ofrecen gestión centralizada de todos los dispositivos, servidores y usuarios, y proporcionan un sistema de reglas extremadamente flexible impulsado por calendarios y eventos.

El sistema también incluye funcionalidad totalmente integrada de Matrix para la visualización distribuida de vídeo desde cualquier cámara en su sistema de vigilancia en cualquier ordenador que tenga XProtect Smart Client instalado XProtect VMS incorpora una página web de instalación administrativa. Que permite a los administradores descargar e instalar XProtect u otros componentes del sistema Management Client en cualquier otro ordenador de la red.

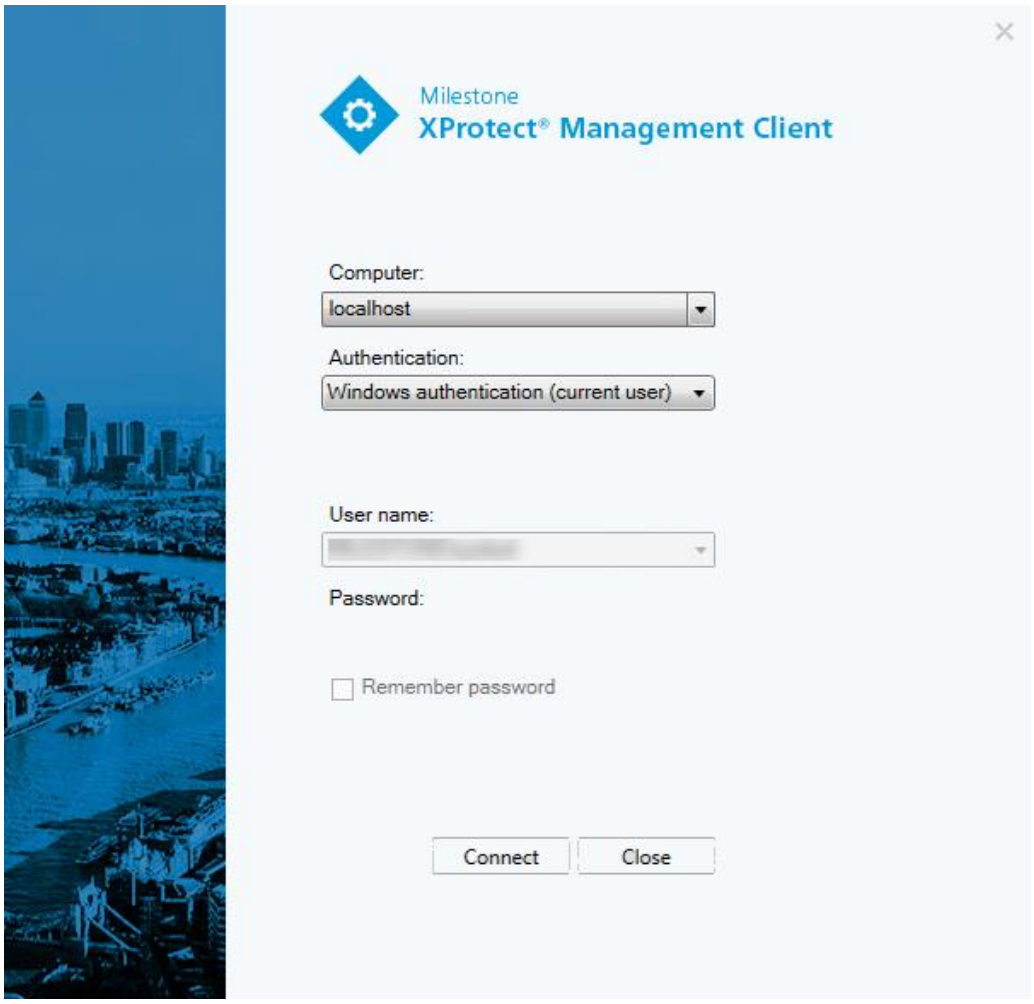


Ilustración 8: Interfaz gráfica para administrar el servidor.

XProtect Smart Client

XProtect Smart Client es una aplicación de escritorio diseñada para ayudarle a gestionar y ver vídeos desde las cámaras conectadas a su sistema VMS de XProtect. A través de XProtect Smart Client tendrá acceso a vídeo en directo y grabado, control instantáneo de cámaras y dispositivo de seguridad conectados. Puede realizar búsquedas avanzadas para encontrar cualquier dato de vídeo y metadatos compatibles almacenados en el servidor.

Disponible en varios idiomas locales, XProtect Smart Client tiene una interfaz de usuario adaptable que puede ser optimizada para las tareas del operador individual y ser ajustada de acuerdo con habilidades específicas y niveles de autoridad.

El sistema XProtect incorpora una página web de instalación pública. Que permite descargar e instalar XProtect Smart Client en cualquier otro ordenador de la red.

En XProtect Smart Client, puede ver vídeo en directo en modo directo y vídeo grabado en modo reproducción. En modo directo, su XProtect Smart Client se conecta al servidor del sistema de vigilancia y muestra vídeo en directo grabado con las cámaras de la vista seleccionada.

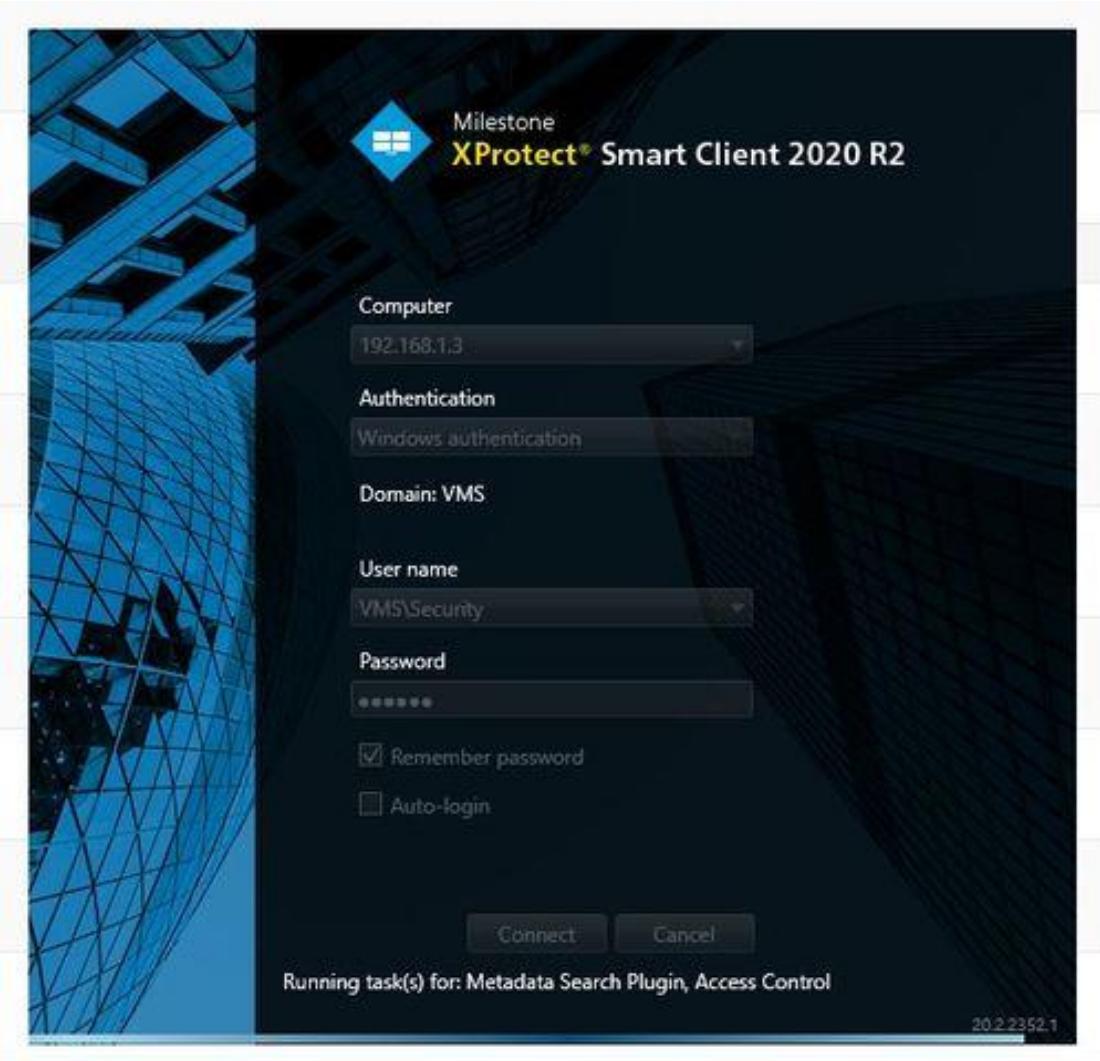


Ilustración 9: Interfaz gráfica cliente para el monitoreo de las cámaras.

2.6.2.1.3 Principales características

Los NVR tienen varias características representativas que son importantes tenerlas en cuenta para especificar la opción correcta en proyectos de videovigilancia, estas son:

Resolución

Generalmente se especifica en píxeles y se compone mínimo de dos valores, la resolución con la cual el equipo puede procesar imágenes para el video en vivo y la resolución de grabación por cámara o por el total de las cámaras que puede admitir. Es importante tener en cuenta este valor que se puede encontrar en las hojas técnicas del equipo y compararlos con la resolución máxima de las cámaras que el sistema tendrá que procesar, de modo que la capacidad máxima del NVR no sea superada por la del conjunto de cámaras.

Capacidad de almacenamiento

También se deben tener en cuenta dos parámetros, la capacidad de unidades de discos duros que se pueden instalar en el equipo y la capacidad de almacenamiento de disco duro que puede soportar el NVR. Esto podrá indicar cuánta capacidad total de almacenamiento puede tener el equipo.

Capacidad de procesamiento

Al igual que el ancho de banda la capacidad de procesamiento o throughput se mide en Mbps y lo que indica es que tantos datos el sistema puede procesar, tal como ocurre con los switches de red. El throughput no debe ser inferior a la suma del total de los anchos de banda de las cámaras que estarán configuradas en el NVR. De lo contrario se podrán tener visualizaciones lapsadas, y problemas en las grabaciones del sistema.

Formato de compresión soportado

Usualmente los NVR pueden soportar varios formatos de codificación, algunos estándares del mercado son: MPEG4, MJPEG, H264, H265 y dependiendo del fabricante podrán soportar otros que pueden ser incluso más eficientes.

Interfaz física de red

Son las conexiones disponibles para la comunicación de datos entre el NVR y la red Ethernet, usualmente son de velocidades de 100 Mbps y 1000 Mbps pero también hay modelos que soportan 10.000 Mbps.

Un punto importante en los NVR es que cuantas más cámaras pueden admitir, es posible que tenga más de una interfaz de red para funciones como: balanceo de carga, segmentación de redes, conexiones LAN y WAN, etc., estos puertos son configurables según la necesidad.

Sistema operativo

Los NVR usualmente tienen el sistema operativo embebido y en esos casos es muy común encontrar equipos con Linux como sistema operativo, sin embargo hay gran variedad de NVR's con sistema operativo Windows el cual es optimizado para el procesamiento de video y generalmente son servidores dedicados a gestión de video en red que también soportan y procesan funciones de análisis de contenido de video de alto perfil.

Protocolos de comunicación soportados

Los protocolos de comunicación son cruciales para que los NVR puedan transmitir las tramas de datos de forma segura sobre las diferentes tecnologías de comunicación, por ejemplo; protocolos de sincronización de tiempo, protocolos para transferencias de archivos, comunicación desde y hacia equipos móviles en donde se deban ver imágenes y gestionar los equipos, entre otros. Los más comunes son: IPv6, HTTPS, UPnP, SNMP, NTP, SADP, SMTP, NFS, iSCSI, PPPoE, DDNS.

2.6.2.1.4 Cámaras QND-8080R

Características principales

- Máx. 5 megapíxeles de resolución (2592 x 1944)
- 3,2 ~ 10 mm (3,1x) objetivo varifocal motorizado
- 0,15 lux (Color), 0 Lux (B/N, LED IR encendido)

- Máx. 30 ips a 5 MP (H.265, H.264)
- Compatible con los códecs H.265, H.264 y MJPEG, y flujos de datos múltiples
- Día / Noche y WDR (120 dB)
- Manipulación, detección de movimiento y detección de desenfoque
- Ranura para tarjetas de memoria Micro SD, SDHC y SDXC (máx. 128 GB)
- Visualización pasillo y compatibilidad con WiseStream II
- Longitud visible IR 30 m
- IP66, IK10, PoE

Ilustración 10: QND-8080R

2.6.2.1.5 Cámaras QNV-8080R

Características principales:

- Máx. Resolución de 5 megapíxeles (2592 x 1944)
- Lente varifocal motorizada de 3,2~10mm(3,1x)
- 0.15Lux (Color), 0Lux (B/N, LED IR encendido)
- Máx. 30fps@5MP (H.265 / H.264)
- Compatible con códecs H.265, H.264 y MJPEG, transmisión múltiple
- Día y noche, WDR (120 dB)

- Manipulación, Detección de movimiento, Detección de desenfoque
- Ranura de memoria Micro SD / SDHC / SDXC (máx. 128 GB)
- Vista de pasillo, compatibilidad con WiseStream II
- Longitud visible IR 30m
- IP66, IK10, PoE

Ilustración 11: Cámara QNV-8080R

2.6.2.1.6 Fisheye XNF-8010R

Características principales:

- Resolución máx. 2048 x 2048 de resolución
- Compatible con los códecs H.265, H.264 y MJPEG
- Ojo de pez, Panorámica simple, Panorámica doble, Vista cuádruple
- Dewarping integrado, PTZ digital (8x), Audio bidireccional
- WDR real (120 dB), compatibilidad con WiseStream Ⅱ
- Manipulación, merodeo, detección direccional
- Detección de audio, Clasificación de sonido, Mapa de calor
- Conteo de personas, Gestión de filas

Ilustración 12: Cámara Fisheye XNF-8010R

2.6.2.2 Instalación física de los equipos

En primer lugar, la instalación de los equipos en general, estará a cargo del proveedor, los cuales deberán fijarlo en el lugar predestinado para esta implementación acorde al espacio existente.

Seguidamente el servidor Milestone Husky deberán ser instalados en el rack acorde al diseño del proyecto.

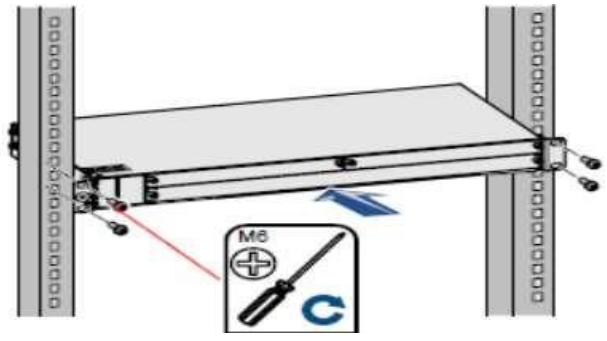


Ilustración 13: Fijado del Husky en el rack

Para realizar las conexiones entre el servidor - Switch y Switch – cámaras, para esto se requiere utilizar Patch Cord del tipo UTP Cat 6 de diferentes distancias.

Ilustración 14: Patch Cord UTP Cat6

2.6.2.3 Configuración de equipos

Para la configuración del servidor Husky Milestone se instalará Windows server 2019, sobre el cual se instalará el aplicativo Core del Milestone Xprotect managerment (Ilustración 8) y con una base de datos dedicada en otro servidor.

Se requiere instalar un software en la máquina de los administradores que funciona como terminal para el acceso y configuración de los equipos, en este caso, sería el Milestone Xprotect Client (Ilustración 9).

2.6.2.4 Gestión de Equipos y monitoreo

El software de gestión y monitoreo actual, aunque es funcional y se actualiza cada cierto tiempo, será descartado, por la solución Milestone Xprotect Client (Ilustración 9) que brinda el fabricante, ya que, esta brinda una interfaz más intuitiva y amigable al cliente.

XProtect Smart Client es una aplicación de escritorio diseñada para ayudarle a gestionar y ver vídeos desde las cámaras que están conectadas a su sistema VMS de XProtect. Desde la aplicación de escritorio XProtect Smart Client, tiene acceso a espacios de trabajo y características como:

- Pestañas estándar como Vistas, Exportaciones, Buscar, Gestor de alarmas y Monitor del sistema, situadas en la esquina superior izquierda de XProtect Smart Client.
- Paneles estándar para configurar vistas y cámaras, ubicadas debajo de las pestañas estándar.
- La barra de herramientas global con acceso a la Lista de bloqueo de evidencias, el Perfil de usuario y Ajustes y más, ubicada en la esquina superior derecha.
- La barra de herramientas del área de trabajo con acceso a Exportar, Bloqueo de evidencias y Configuración, ubicada justo debajo de la barra de herramientas global.
- Línea temporal principal. La línea temporal principal está disponible si se selecciona la pestaña Vistas. Se encuentra en la parte inferior de la ventana.

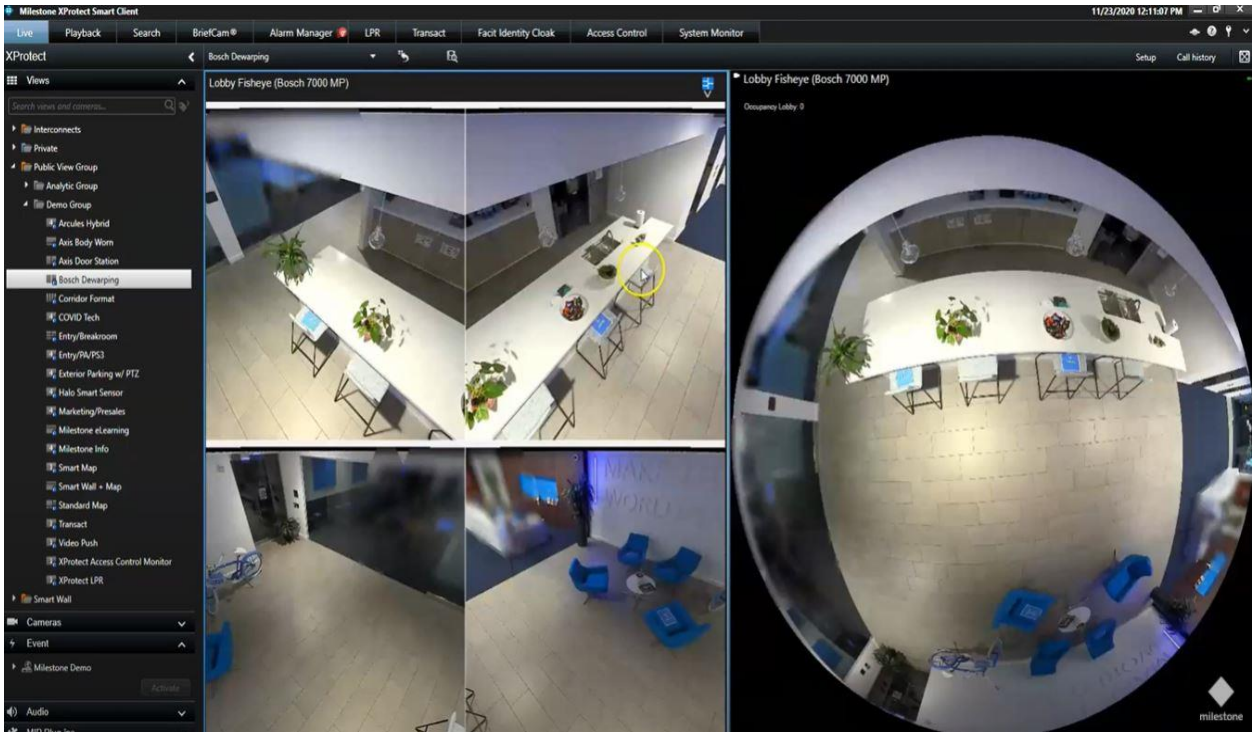


Ilustración 15: Vista desde la aplicación de monitoreo.

2.7 Limitaciones o dificultades presentadas

Durante el periodo de la pasantía surgieron algunos factores que en su momento ocasionaron que el cronograma se detuviera. Sin embargo, el proyecto de renovación del sistema de videovigilancia tuvo un flujo de trabajo normal y se cumplió con el periodo acordado.

Entre estos factores se pueden señalar los siguientes:

- Retraso por parte del proveedor al momento de coordinar el personal asignado al proyecto.
- Retraso en la configuración del servidor, a causa que, la versión del Windows server no era compatible con el hardware.
- Retraso por parte de las autoridades en otorgar los permisos correspondientes de accesos a los IDC.

Como parte del equipo de analistas de seguridad Jr. – Pasante, no contaba con los permisos de administrador en todas las herramientas por el periodo de la pasantía, lo cual, limitaba las herramientas a la cuales podía acceder y gestionar.

2.8 Relación de la pasantía profesional con la carrera estudiada

Puedo observar que luego de analizar los objetivos principales a cumplir durante la pasantía, considero que hemos cumplido con cada uno de ellos, ya que, logramos aplicar los conocimientos teórico-prácticos adquiridos en la UNICyT durante la pasantía en la empresa, mejorando así las habilidades a través de la experiencia práctica en un entorno real y producción.

En retrospectiva, la pasantía realizada en la empresa Telered SA, una empresa dedicada a ser la autopista transaccional de Panamá y enfocada en un continuo crecimiento tecnológico, es el entorno correcto para desarrollar mis habilidades como Ingeniero en redes de comunicaciones con énfasis en Seguridad, ya que, aparte de poseer una robusta área de comunicaciones, también posee un área seguridad enfocada en los

diferentes aspectos de la misma, con la cual, desarrollé una mayor afinidad y está directamente ligada con la carrera que estudio.

Esto me permitirá desarrollarme de manera integral, adquiriendo amplio dominio y conocimientos en los temas que se ofrecen a sus clientes, añadiendo destrezas y habilidades, para realizar actividades necesarias y cumplir con el rol dentro de la empresa.

De esta manera, crecer en conocimiento profesional dentro del rubro de la tecnología.

2.9 Cronograma de Actividades

Cronograma de actividades									
	Agosto - septiembre 2023								
Actividades	Sem 1	Sem 2	Sem 3	Sem 4	Sem 5	Sem 6	Sem 7	Sem 8	Sem 9
Gestión de analista Jr.									
Atención de solicitudes	✓	✓	✓	✓	✓	✓	✓	✓	✓
Creación de usuarios y accesos	✓	✓	✓	✓	✓	✓	✓	✓	✓
Aprobación de certificados	✓	✓	✓	✓	✓	✓	✓	✓	✓
Monitoreo de herramientas	✓	✓	✓	✓	✓	✓	✓	✓	✓
Proyecto de renovación del sistema de videovigilancia									
Preparación del servidor Husky	✓	✓							
Asignación de puertos en el switch de	✓	✓							

seguridad para las cámaras nuevas									
Instalación de aplicativo de administración	✓	✓							
Cableado de nuevos puntos Panamá Pacifico		✓	✓	✓	✓				
Cableado de nuevos puntos Centro de procesamientos de cheques						✓	✓		
Cableado de nuevos puntos IDC Howard								✓	
Cableado de nuevos puntos IDC Clayton									✓
Desinstalación de cámaras obsoletas		✓	✓	✓	✓	✓	✓	✓	✓
Instalación de nuevas cámaras en Panamá Pacifico		✓	✓	✓	✓				
Configuración de las cámaras en el aplicativo de monitoreo		✓	✓	✓	✓				
Instalación de nuevas cámaras en Centro de procesamientos de cheques						✓	✓		
								✓	

Instalación de nuevas cámaras en el IDC Howard									
Instalación de nuevas cámaras en el IDC Clayton									✓
Apagado del viejo sistema									✓
Preparación de la documentación	✓	✓	✓	✓	✓	✓	✓	✓	✓
Entrega de documentación									✓

CAPÍTULO III

Diagnostico Observacional

3.1 Descripción de la problemática

En la actualidad, la empresa Telered se encuentra en un plan continuo de crecimiento y expansión de su red como la autopista transaccional de Panamá, por lo que se hace de carácter mandatorio contar con un mejor sistema de videovigilancia, con el objetivo principal de reducir los puntos físicos de vulnerabilidad que pueda tener la empresa y tener un mejor alcance de las personas que entran a la misma.

Otra principal problemática con los constantes eventos fortuitos en la red de videovigilancia que ponen en riesgo la integridad y disponibilidad del servicio actual como lo son las cámaras sin señal o dañadas, perdida de grabación en varias fechas intercaladas y otras de forma continuas han propiciado esta nueva implementación.

3.2 Alternativas de solución a la problemática planteada

La solución principal plantea diseñar e implementar un nuevo sistema de videovigilancia que reemplace el sistema actual de la empresa en una estructura de alta disponibilidad y totalmente desde cero, donde tendrá una base de datos y servidor totalmente dedicados a este nuevo sistema.

Esquema distribuido de todas las cámaras implementadas

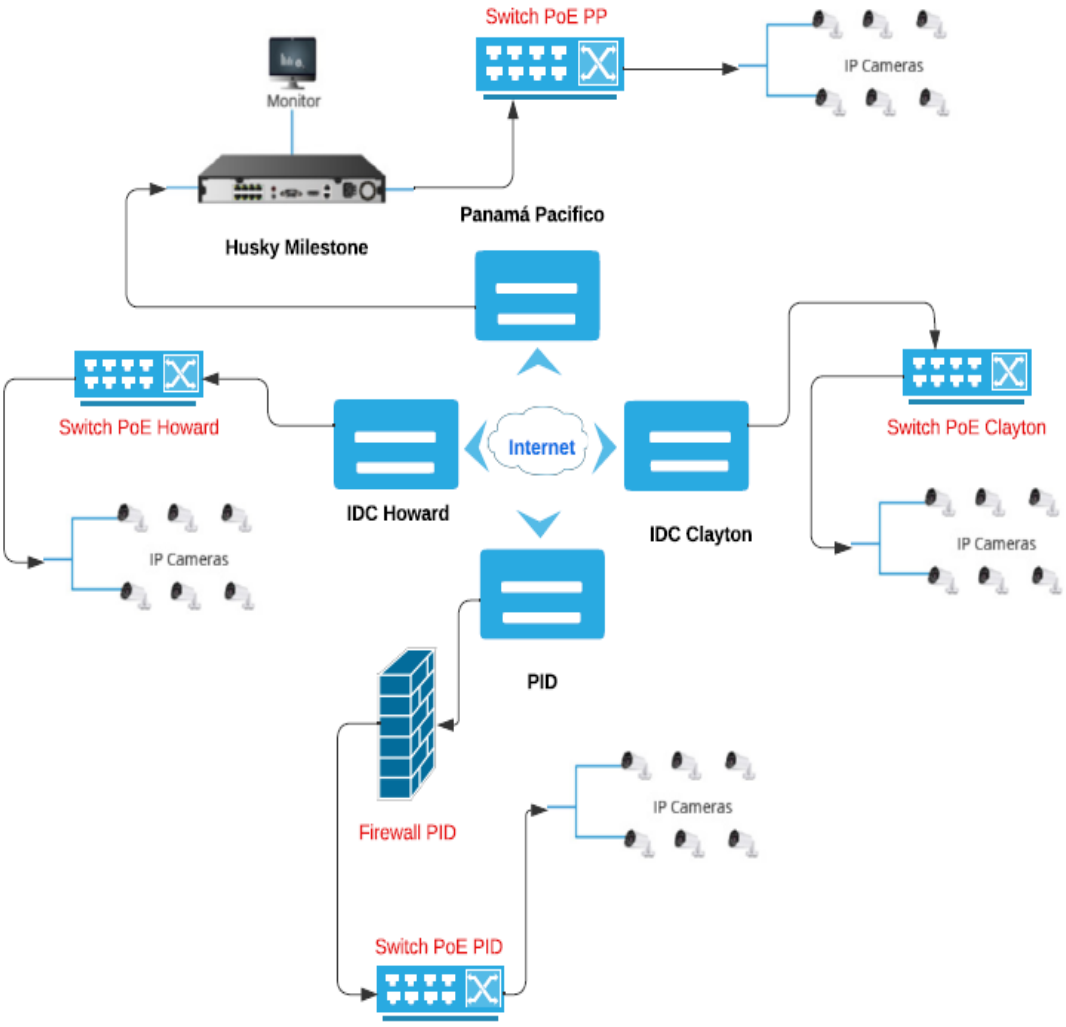


Ilustración 16: Esquema de implementación del sistema de videovigilancia.

Conclusiones

Durante el desarrollo de este proyecto, se realizó la renovación del sistema de videovigilancia tomando en cuenta una necesidad real que tenía la empresa Telered, Se planteó una la mejor alternativa para un sistema que presentaba fallos cada vez más críticos en la operación y a nivel de auditorías afectando la gestión empresarial.

Se presento pérdida de grabación durante el reemplazo de cada cámara, lo cual están dentro de los parámetros establecidos en el trayecto de la implementación.

Se logro validar imagen en todas las cámaras instaladas, grabación en tiempo real, almacenamiento continuo de las grabaciones y minimización de puntos ciegos en todos los recintos.

Se vieron los siguientes procesos: la instalación del servidor físico y la configuración de las políticas de hardening para reducir las vulnerabilidades del servidor, la instalación en físico y configuración en el sistema de manejo central y el acceso a estas cámaras desde la herramienta cliente y los procesos que el nuevo sistema debe llevar.

De los modelos de cámaras, se puede comentar que las mismas tienen una buena calidad de imagen y que la posibilidad de establecer listas negras de Mac address aumentan la seguridad del sistema, permitiéndole al administrador definir desde el servidor, quienes tendrán permiso de acceso.

Finalmente, la ejecución de este proyecto ayudo a ampliar y aplicar losconocimientos obtenidos durante la carrera dentro de la UNICyT y a su vez pudimos ayudar a la empresa a tener una mejora de seguridad y vigilancia.

Recomendaciones

Como analista de seguridad:

- Restringir el uso de dispositivos USB. Esto ayudará a evitar la propagación de malware a través de dispositivos de almacenamiento extraíbles.

- Establecer una política de contraseñas seguras. Esto incluye establecer reglas para la fuerza y la frecuencia de cambio de contraseñas.

- Establecer controles de acceso. Esto significa establecer reglas para el acceso a los recursos de la empresa y asegurar que los usuarios solo tengan acceso a los recursos que necesitan para realizar su trabajo.

- Seguir recomendaciones básicas de seguridad. Por ejemplo: evitar abrir archivos y enlaces sospechosos, no conectar dispositivos sospechosos a la red o desconfiar de los correos electrónicos no solicitados.

- Utilizar conexiones seguras. Es decir, ya sea durante el trabajo remoto o en la oficina, deben utilizarse conexiones VPN seguras a redes inalámbricas para una navegación segura.

Proyecto de cámaras:

- La mejor práctica ideal es asignar una contraseña única y larga no obvia para cada cámara. Un proceso tan meticuloso lleva tiempo de preparación, es más difícil de administrar y es muy difícil de seguir. Por ello, muchos instaladores, lamentablemente, utilizan una única contraseña para todas las cámaras de una cuenta.

- Lo ideal es NO conectar su servidor desprotegido a Internet. Si expone su sistema a Internet, «reenvíe» el menor número de puertos posible y utilice un cortafuegos de última generación que analice el protocolo y bloquee los protocolos incorrectos enviados por el puerto equivocado. En una situación ideal, despliegue también un IDS/IPS para una mayor protección.

- Lo mejor es asignar a un experto profesional en seguridad de redes para que verifique y configure un cortafuegos moderno.

- Es crucial tener una documentación clara sobre la configuración del cortafuegos, y supervisar e implementar regularmente cualquier cambio necesario en la configuración del cortafuegos.

- Mantenga seguros: sus armarios; los cables; y la sala donde se encuentran los DVR/NVR/VMS, los conmutadores y los servidores de almacenamiento de vídeo. Proporcionar un control de acceso seguro a la sala, incluida la seguridad por vídeo para vigilarla. Esta práctica no sólo protege su red, sino que previene los robos en sus instalaciones, donde el DVR/NVR de grabación es robado junto con cualquier otro artículo.

- Pregunte a su proveedor de VMS sobre su política para mantener actualizados y seguros los componentes que utiliza. Compruebe si hay actualizaciones periódicas e instálelas. Sea proactivo a la hora de vigilar las vulnerabilidades de seguridad conocidas en el sector y póngase en contacto con su integrador o proveedor cuando se entere de nuevas infracciones.

- Además, establezca políticas y procedimientos para cambiar las contraseñas. Por ejemplo, la contraseña de administrador raíz debe cambiarse cada vez que un empleado con acceso a la contraseña deje la empresa o cambie de función.

REFERENCIAS

M López Ramírez (2018), Análisis de riesgos en un sistema de gestión de seguridad informática (SGSI) con metodologías complementarias,Disponible en: https://repository.unipiloto.edu.co/handle/20.500.12277/2913

HubSpot, Inc, (2024), 10 herramientas de seguridad informática para tu empresa Disponible en: https://blog.hubspot.es/website/herramientas-de-seguridad-informatica

Euroinnova International Online Education, (2012), Sistemas de monitoreo de cámaras), Disponible en: https://www.euroinnova.pa/blog/monitoreo-de-camaras

Mi Próximo Paso es patrocinado por la Administración de Empleo y Capacitación del Departamento de Trabajo de EE.UU., (Sitio actualizado el 21 de mayo de 2024), ¿Qué quiere hacer para ganarse la vida?, Disponible en: https://www.miproximopaso.org/profile/summary/151212.00#:~:text=Pueden%20ocuparse%20de%20la%20implementaci%C3%B3n,los%20ataques%20de%20virus%20inform%C3%A1ticos.

Protek Seguridad, (2022), ¿En qué consiste el monitoreo de cámaras de seguridad?, Disponible en: https://www.protek.com.py/novedades/monitoreo-de-camaras-de-seguridad/

Centro de Estudios, (Jun 28, 2023), ¿Qué funciones tiene un Departamento de Seguridad?, Disponible en: https://centrovigilant.com/que-funciones-tiene-un-departamento-de-seguridad

FJ Valencia-Duque, M Orozco-Alzate, (2017), Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000, Disponible en: https://scielo.pt/pdf/rist/n22/n22a06.pdf

CMP Barón, AFA Garzón, (2018), Las buenas prácticas metodológicas en gestión de proyectos aplicadas a una compañía de seguridad informática, Disponible en: https://www.semanticscholar.org/paper/Las-buenas-pr%C3%A1cticas-metodol%C3%B3gicas-en-gesti%C3%B3n-de-a-Bar%C3%B3n-Garz%C3%B3n/e40dd13a20afd227dc0d768472ffef2bc51b4cf0?p2df

Milestone Systems A/S, (2024), Milestone Husky IVO 1800R guía de primeros pasos y mantenimiento, disponible en: https://doc.milestonesys.com/latest/es-ES/portal/htm/chapter-page-h-ivo1800r-getting-started-maintenance.htm

ANEXO

Glosario

a) **Tercerizar:** Se trata de cambiar la vieja forma de trabajar, que consistía en que una empresa que necesitase, por ejemplo, soluciones informáticas de algún tipo, creaba un departamento específico por otra en la que contrata una empresa especializada para ahorrar dinero y tiempo.

b) **E-commerce:** Consiste en la distribución, venta, compra, marketing y suministro de información de productos o servicios a través de Internet, El comercio electrónico funciona al conectar a compradores y vendedores a través de varios canales electrónicos. Por ejemplo, necesitas un canal, como un sitio web o redes sociales, para que los clientes puedan encontrar productos y servicios que puedan comprar.

c) **ISO:** Un formato de archivo digital que replica un CD, DVD o BD físico. La extensión de archivo ISO no solo almacena archivos y carpetas, sino que aloja además toda la información vital de sistema de archivos acerca de la estructura del disco.

d) **SIEM:** La administración de eventos e información de seguridad, SIEM, para abreviar, es una solución de seguridad que ayuda a las organizaciones a detectar y analizar amenazas y responder a ellas antes de que afecten a las operaciones del negocio.

e) **Generación:** Una generación se refiere a la mejora en el proceso de desarrollo del producto. Con cada generación, los circuitos han sido más pequeños y avanzados que en generaciones previas. Como resultado de la miniaturización, velocidad, poder y capacidad de memoria han crecido proporcionalmente.

f) **Listas negras o Blacklist:** Es un grupo de páginas web o direcciones de correo que han sido denunciadas previamente por tener un comportamiento fraudulento o por el envío de correo electrónico considerado como publicidad no deseada.

g) **Lista blanca o Whitelist**: en su esencia, es una lista de elementos que están previamente aprobados y considerados seguros o permitidos. Estos elementos pueden variar desde direcciones de correo electrónico y dominios de internet hasta aplicaciones de software.

h) **IDC**: Un centro de datos es una ubicación física que almacena máquinas de computación y sus equipos de hardware relacionados. Contiene la infraestructura computación que requieren los sistemas de TI, como servidores, unidades de almacenamiento de datos y equipos de red.

i) **Sitios confinados**: Los espacios confinados son áreas que, por su diseño, presentan limitaciones en términos de acceso y salida, y que no están diseñadas para una ocupación continua.

j) **Sitio Alterno:** Centro de continuidad con espacios de trabajo acondicionados como oficina alterna, permitiendo mantener la operación principal del cliente ante eventos fortuitos.

k) **Resolución**: es el número de píxeles que es capaz de mostrar una pantalla. La resolución se calcula multiplicando el número de filas y columnas de píxeles.

l) **Sockets:** es un extremo de comunicación, es decir, un objeto a través del cual una aplicación de Windows Sockets envía o recibe los paquetes de datos a través de una red. Un socket tiene un tipo y se asocia a un proceso en ejecución y puede tener un nombre.

m) **Hardening**: este proceso tiene la misión de reducir las posibles vulnerabilidades que pueda tener el sistema. En otras palabras, consiste en establecer las medidas de seguridad necesarias para conseguir alejar posibles peligros y amenazas, existentes o futuras

Anexo 2

Ilustración 17: Configuración de la cámara en el servidor del NVR

Ilustración 18: Revisión de puertos disponibles en el Switch.

Ilustración 19: Instalación de cámara.

Ilustración 20: Instalación con el proveedor.

Ilustración 21: Reemplazo de cámara en el IT ROOM Sitio alterno

Ilustración 22: Reemplazo de cámara en el exterior del Sitio alterno

Ilustración 23: Puertos asignados en el Switch

Ilustración 24: Atendiendo asignaciones de Analista Jr.

Ilustración 25: Equipo de seguridad Telered

Ilustración 26: Foto del mes de la seguridad

Telered
INNOVACIÓN QUE TRANSFORMA

Panamá, 29 de septiembre de 2023.

Sra. Miroslaba Martínez
Secretaria General
UNICYT
E. S. M.

Respetada Sra. Martínez:

Reciba un cordial saludo de nuestra parte.

Certificamos que el joven **Gilberto Abraham Rodríguez Arrocha**, con cédula de identidad personal N° **8-825-1169,** realizó su práctica profesional en Telered, S.A., en el departamento de Seguridad de la Información, haciendo las siguientes tareas: Proyecto de reemplazo del Sistema de Video-Vigilancia en Panama Pacifico, PID y Centros de Datos; Gestión Operativa en relación a: Accesos Lógicos de Clientes externos para accesos a sitios de Telered. Flujos de MOPER (gestión de accesos de colaboradores), Atención de plantillas de Seguridad de Lookwise. Destacamos que en el mes de agosto, Gilberto gestiono el 43% de las solicitudes recibidas a través del SIG, entre otras; cumpliendo satisfactoriamente con las asignaciones y las horas estipuladas, desde el 01 de agosto hasta el día de 30 de septiembre de 2023, haciendo un total de 2 meses.

Se extiende la presente a solicitud del interesado.

Atentamente,

Eyra Villarreal
Gerente de Recursos Humanos
Telered, S.A.

+507 306-8000 | telered.com.pa | International Business Park. Edificio 3835. Piso 6. Panamá Pacífico, Panamá. | Apartado: 0816-01035

Ilustración 27: Carta de Finalización de la pasantía