Universidad de Lima

Facultad de Ingeniería

Carrera de Ingeniería de Sistemas

GESTIÓN Y MITIGACIÓN DE RIESGO CIBERNÉTICO

Trabajo de suficiencia profesional para optar el Título Profesional de Ingeniero de Sistemas

Frank Manuel Ramirez Castañeda

Código 19993045

Asesor

Christiam Javier Ortiz Pachas

Lima – Perú

Setiembre de 2024

Cyber Risk Management and Mitigation Plan

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El profesional de la Universidad de Lima cuenta con una formación integral y multidisciplinaria que le permite desempeñarse el campo tecnológico de su preferencia. Esta formación me ha permitido desempeñarme en diversos segmentos de la industria. Que van desde la creación de software en compañías transnacionales como IBM Perú, hasta la industria financiera y de servicios americana Citibank NA, Royal Caribbean Cruise Lines, y actualmente para una Top 50 en la industria de venta al por menor.

Al egresar, desempeñé un rol técnico empleando las capacidades técnicas fundamentales adquiridas durante mis estudios. Mi buen desempeño técnico me permitió liderar y gestionar cambios.

Un profesional nunca deja de aprender. La capacitación continua me ha facilitado adquirir los nuevos conocimientos que acompañan la evolución tecnológica, y desarrollar las habilidades blandas necesarias para gestionar. Además, a obtener once certificaciones en seguridad y gestión de la información, gestión de proyectos, regulaciones de la industria de tarjetas de pago y arquitectura empresarial.

Como líder, entendí que se lidera con el ejemplo, actuando con ética, integridad, y ofreciendo igual trato y oportunidades sin favorecer ni discriminar por ningún motivo. Así he conformado equipos de trabajo donde los miembros cuentan con habilidades, conocimientos y personalidades complementarias para completar los proyectos exitosamente.

Asimismo, ha sido útil para mí y mis equipos de trabajo, implementar lecciones aprendidas al final de cada experiencia laboral, proyecto e interacción con otros equipos. Esto ha permitido continuar con prácticas eficientes, mejorar las áreas débiles, evitar repetir errores, y fortalecer la sinergia con otros equipos.

Finalmente, recordemos que siempre debemos buscar un balance en nuestras vidas y dedicarle tiempo al trabajo, a la familia y a nosotros mismos. Después de todo, nuestra salud física y mental determinarán nuestra calidad de vida a largo plazo.

Palabras clave: Seguridad de la información, Gestión de equipos, Dirección de proyectos, Riesgo cibernético, Habilidades blandas, Arquitectura de seguridad, Arquitectura empresarial.

ABSTRACT

The professional profile of a graduate from the University of Lima embodies a comprehensive and multidisciplinary preparation, enabling them to excel in their preferred technology field.

This enablement allowed me to work across various segments of the industry, ranging from software development at multinational companies like IBM Peru to the financial and services industry in the United States at Citibank NA and Royal Caribbean Cruise Lines, and lately, in a US Top 50 within the retail industry.

Upon graduating, I began my professional journey in a technical role, leveraging the technical skills acquired as a student. My strong performance allowed me to lead and drive change.

As a professional, I recognize the importance of continuous learning. Continuous learning allowed me to acquire the knowledge that accompanies technological advancements and to develop the soft skills necessary for effective management. Nowadays, I hold eleven certifications in security, project management, payment card industry regulations, enterprise architecture, and security management.

As a leader, I realized that one must lead by example, act ethically and with integrity, and provide equal treatment and opportunities without bias. Therefore, I build project teams by assembling members with the complementary skills, knowledge, and personalities necessary to complete projects successfully.

In addition, implementing lessons learned after each work experience, project, and collaboration with other teams has professionally benefited my teams and myself. This approach allows us to maintain efficiency, address weaknesses, avoid repeating mistakes, and strengthen cross-team partnerships and synergy.

Lastly, let's remember that we should always seek balance in our lives, dedicating time to work, family, and ourselves. Ultimately, our physical and mental health will determine our quality of life in the long term.

Keywords: Information Security, Team Management, Project Management, Cyber Risk, Soft Skills, Security Architecture, Enterprise Architecture.

INTRODUCCIÓN

Luego de realizar mis prácticas en la universidad, mi carrera profesional se inició como especialista de software.

En el año 2000 como practicante para Volvo Group, actualicé el sistema de facturación y lo integré con el sistema contable global residente en el mainframe en Suiza.

En el año 2001 ingresé a una nueva práctica en IBM Perú como parte del Software Group, creando y ejecutando pruebas de concepto para clientes.

En el año 2002 fui escogido para liderar el centro de innovación de IBM en Perú, donde se realizarán sesiones de capacitación para asociados de negocio de IBM y pruebas de concepto para clientes con miras a cerrar nuevos negocios de licenciamiento.

En el año 2004 fui contratado por Systems Support and Services, uno de los integradores más grandes en Perú como jefe de producto de software IBM y Oracle, liderando negocios de licenciamiento y servicios para clientes. Mi relación previa con IBM y sus asociados de negocios fue instrumental para cerrar negocios exitosos y tercerizar los servicios no disponibles internamente.

En el año 2007 decidí emigrar a los Estados Unidos en donde se inició mi desarrollo profesional en el área de Ciberseguridad y gestión de riesgo, rol que ha continuado madurando hasta el presente año 2024. Estos 17 años se componen de 10 años en el sector de banca, seguido de 4 años en el sector de hotelería y turismo, y actualmente por casi 4 años en el sector de venta al por menor.

En el 2007 ingresé a Pacific National Bank (PNB) ubicado en Miami como administrador de sistemas. PNB es una dependencia del banco central del Ecuador con una sola agencia en Miami, Florida. Tuve a mi cargo la estabilidad de todos los sistemas computacionales del banco, y fuí intermediario y coordinador de las actividades de seguridad informática.

En el 2010 ingresé a Ocean Bank como oficial de seguridad de datos, siendo responsable de la seguridad informática del banco, creando y actualizando políticas de seguridad, estándares y procedimientos. Así mismo, negocié contratos de licenciamiento de software y servicios de seguridad. Adicionalmente, lideré la resolución de hallazgos de auditoría interna, auditoría externa y auditoría del estado (FDIC).

En el 2011 fui contratado por Citibank NA como VP de seguridad de la información, liderando un equipo de 12 ingenieros de ciberseguridad (ethical hackers). Estuve a cargo del área de pruebas de seguridad, encargada de identificar vulnerabilidades en las aplicaciones del banco, reportarlas al vicepresidente respectivo y presentar recomendaciones para mitigar el riesgo o eliminar la vulnerabilidad. En este rol tuve que crear indicadores de performance y de distribución de la carga de trabajo entre los miembros del equipo para poder cumplir con los SLA y gestionar el backlog.

En el 2016 ingresé a Royal Caribbean Cruise Lines liderando el área de arquitectura de seguridad. Aquí tuve la oportunidad de crear y contratar el equipo en Manila, Filipinas para conducir las pruebas automatizadas e identificar vulnerabilidades en las aplicaciones de la compañía. Así mismo gestioné el diseño de patrones de seguridad reutilizables a ser implementados en los proyectos y soluciones del área digital. Adicionalmente, creé y actualicé políticas y estándares de seguridad. Durante este tiempo logré incluir la arquitectura de seguridad como parte de la fase de diseño de los proyectos, reduciendo los costos y tiempos asociados a la inclusión de los controles de seguridad.

En el 2020 fui contratado por una de las 50 compañías más grandes de los Estados Unidos como oficial de seguridad de la información para el negocio, por sus siglas en inglés, Business Information Security Officer (BISO). BISO es un rol de seguridad cibernética de alto nivel y actúa como enlace entre seguridad de la información y el área de negocios de una organización. Se encarga de gestionar riesgos e implementar las estrategias de seguridad. En este rol coordino con el vicepresidente de tecnología y directores para gestionar la hoja de ruta de seguridad, priorizando iniciativas y asegurando la participación de equipos multidisciplinarios para lograr los objetivos propuestos, en el margen de tiempo y costo definidos. Nuevamente tuve la oportunidad de liderar la estrategia shift-left para incluir la arquitectura de seguridad en paralelo al diseño de la arquitectura de solución. En este rol se hace más evidente la vital importancia de las habilidades blandas, ya que la asociación y la buena relación de confianza con el vicepresidente de tecnología y directores es lo que hace posible que apoyen estas iniciativas de seguridad y que dediquen los recursos necesarios para la ejecución de estas.

Algunos logros durante mi trayectoria:

- Logré la adjudicación de la licitación de la Cancillería del Perú a Systems Support and Services.

- Inicié el proyecto de virtualización en PNB, reduciendo los costos de mantenimiento y energía en un 25%.
- En el lapso de un año, y coordinando estrechamente con los auditores del Office of the Comptroller of the Currency (OCC) logré incrementar la calificación de seguridad de PNB de C a A.
- Gestioné nuevos estándares de seguridad en Ocean Bank, elevando los niveles de gestión de acceso en el mainframe a nivel de objeto y extendí el monitoreo, lo cual cerró los hallazgos de seguridad del FDIC (Federal Deposit Insurance Corporation).
- Diseñé y comuniqué nuevos patrones de arquitectura de seguridad reutilizables en Royal Caribbean Cruise Lines disminuyendo los costos de rediseño en 15%.
- Creé la hoja de ruta para asegurar el centro de cómputo de RCL en Manila y reducir el indicador de riesgo informático en 80%
- Diseñé e introduje el "Análisis de Amenazas" (Threat Analysis) como parte de la arquitectura de seguridad, lo que permitió priorizar la implementación de controles de seguridad antes de ir a producción, reduciendo el tiempo de rediseño y recodificación por seguridad en 65%.
- Contribuí a la gestión del shift-left de la arquitectura de seguridad con VPs, directores y gerentes de producto.
- Creé la hoja de ruta con las diferentes iniciativas de seguridad para la organización de retail. Durante los primeros cinco meses de implementación, el riesgo cibernético ha disminuido en 12%.

En el siguiente capítulo mostraré cómo he utilizado las capacidades técnicas para generar la información que categorizará y describirá el riesgo cibernético de la empresa.

En el capítulo de capacidad de gestión contaré como he venido interactuando con los interesados del proyecto para fomentar una buena asociación y mantener su apoyo. También explicaré el plan de comunicación con los interesados de acorde con su interés e influencia.

El capítulo de aprendizaje cuenta la historia de lo que me ha ayudado a adquirir el conocimiento para poder identificar las fuentes de información de activos, conocer los riesgos cibernéticos, poder proponer recomendaciones de seguridad, así como gestionar la planificación y ejecución de las actividades para mitigar el riesgo cibernético corporativo.

En el capítulo de conducta ética detallo los principios que me han ayudado a lo largo de mi trayectoria profesional y como pueden influenciar positivamente a los demás.

En el capítulo de lecciones aprendidas incluyo sugerencias tanto para los recién egresados como para los profesionales con años de experiencia.

Luego de 20 años de experiencia en tecnología, considero que cada día, cada proyecto, cada persona, y cada nueva experiencia pueden enseñarnos algo nuevo que nos ayude a crecer.

Tengo varios proyectos aún por realizar dentro y fuera del área de tecnología y soy consciente que para poder materializarlos necesito ponerle esfuerzo, dedicación y rodearme de gente capaz, energética y positiva.

1. CAPACIDAD TÉCNICA

Para poder lograr los objetivos de negocio tenemos que apoyarnos y elegir las capacidades técnicas que nos ayudarán a conseguir dichos objetivos.

En la industria de venta al por menor (retail) es imprescindible la mejora continua de la experiencia del cliente y poner en producción nuevos servicios lo más pronto posible, anticipando a la competencia, reduciendo costos y satisfaciendo los requerimientos de seguridad de los clientes.

En el campo de seguridad de la información, desarrollaremos los siguientes puntos de capacidad técnica:

- Definición de requerimientos
- Identificación de interesados
- Identificación de brechas
- Estándares y marcos de referencia tecnológicos
- Metodología de calificación de riesgo
- Tecnologías seleccionadas

1.1 Definición de Requerimientos

Ante el significativo incremento de ataques cibernéticos y empresas afectadas como Dell, Ticket Master, ATT, Marriot, Splunk, MGM, etc. Y a los $9.5 trillones pronosticados en costos asociados a ciberataques a nivel global en el 2024 (Morgan, 2023). Se presentaron los requerimientos a continuación.

- Reducir progresivamente el riesgo cibernético hasta llevarlo a niveles par con la industria.
- Reducir el costo del seguro cibernético que cubre los gastos ante un compromiso de la infraestructura o exfiltración de datos.

1.2 Identificación de Interesados

Procedí a integrar conocimientos de áreas afines. Empezando con la identificación de las partes interesadas (stakeholders), siguiendo la guía de gestión de proyectos de Project Management Institute (PMI), por sus siglas en inglés.

Además del VP de tecnología, la plana ejecutiva con interés en seguridad está conformada por el vicepresidente senior (SVP) que es un alto cargo ejecutivo que típicamente reporta al ejecutivo con máxima autoridad administrativa en una organización. El Chief Information Secutiy Officer (CISO) es un ejecutivo de alto nivel que se encarga de definir las estrategias de seguridad, gestionar el riego y responder a incidentes cibernéticos. El Chief Information Officer (CIO) es un ejecutivo de alto nivel que se encarga de gestionar la tecnología y los sistemas de una organización. Define la estrategia y gestiona presupuestos de TI.

La tabla 1.1. muestra la identificación y objetivos de los interesados.

Tabla 1.1

Identificación y Objetivos de los Interesados (stakeholders)

STAKEHOLDER	NIVEL	OBJETIVOS
Nombre1	CISO	Reducir el Riesgo cibernético, Reducir el Costo del seguro cibernético
Nombre2	CIO	Incrementar las ventas mediante la mejora de experiencia del cliente en línea.
Nombre3	SVP producto	Agilizar el tiempo de puesta de servicios en producción
Nombre4	VP ingeniería	Mantener los niveles de servicios y las aplicaciones operativas para que sigan generando ingresos o soportando el negocio.
Nombre5	Director ingeniería	Mantener la estabilidad de los sistemas y aplicaciones.
Nombre6	Manager ingeniería	Proveer los entregables según el cronograma de planeamiento.

1.3 Identificación de Brechas

Según el marco referencial de arquitectura empresarial definido por el Open Group más conocido como TOGAF por sus siglas en inglés, las brechas (GAPS) son aquello que falta para llegar al estado final deseado. Estas brechas generarán paquetes de trabajo, los que a su vez estarán constituidos de tareas.

Las principales brechas en las que tenemos que enfocarnos en este proyecto de gestión y mitigación de riesgo:

- Visibilidad: Se requiere categorizar y representar apropiadamente la información relacionada a las desviaciones de los estándares de seguridad.
- Priorización: Identificar aquellas categorías y subsegmentos que producen el mayor impacto/beneficio al remediar. Disminuyendo el riesgo en mayor cuantía.
- Cobertura: Identificar e incorporar los activos de la organización, como servidores, aplicaciones, y bases de datos.

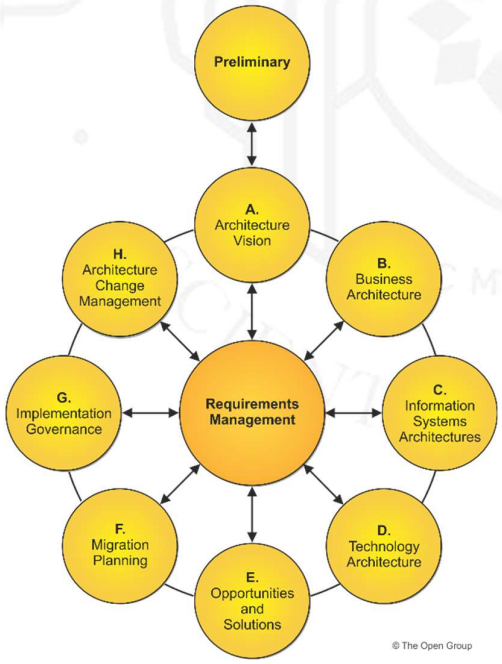
1.4 Estándares y Marcos de Referencia Tecnológicos

- **TOGAF**: Es un marco referencial de arquitectura empresarial que proporciona un enfoque para diseñar, planificar, implementar y gobernar la arquitectura de una solución. Mejora la eficiencia empresarial y la comunicación (Hornford et al., 2022).

  La figura 1.1 muestra el método de desarrollo de arquitectura y sus fases según TOGAF.

Figura 1.1

TOGAF (Método de desarrollo de arquitectura)



Nota. De *An introduction to the TOGAF® standard, 10th edition*, por D. Hornford, N. Hornford, M. Lambert & K. Street, 2022, The Open Group (https://pubs.opengroup.org/architecture/w212/).

- **NIST CSF**: Según National Institute of Standards and Technology (NIST), propuso el marco de trabajo sobre ciberseguridad. NIST, está basado en estándares, guías y prácticas para mitigar el riesgo cibernético y tomar decisiones basadas en ese riesgo.

  En la figura 1.2 se muestran los cinco aspectos de dicho marco de referencia: Identificar, Proteger, Detectar, Responder y Recuperar.

Figura 1.2

Cybersecurity Framework 2.0

Nota. De *The NIST Cybersecurity Framework (CSF) 2.0* (p. 5), por National Institute of Standards and Technology, 2024 (https://doi.org/10.6028/nist.cswp.29)

- **NIST 800-53**: Es un estándar de seguridad de la información que proporciona un catálogo de controles de privacidad y seguridad para sistemas de información. Este estándar ayuda a proteger las operaciones, activos e individuos frente a los ataques cibernéticos, desastres y riesgos de privacidad (Computer Security Resource Center, 2020).

  En la figura 1.3 se muestran las categorías de los controles publicados por NIST y que son empleados por la gran mayoría de organizaciones de gobierno y entidades privadas para mitigar el riesgo cibernético existente en sus ambientes tecnológicos.

Figura 1.3

Categorías de Controles de Seguridad

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

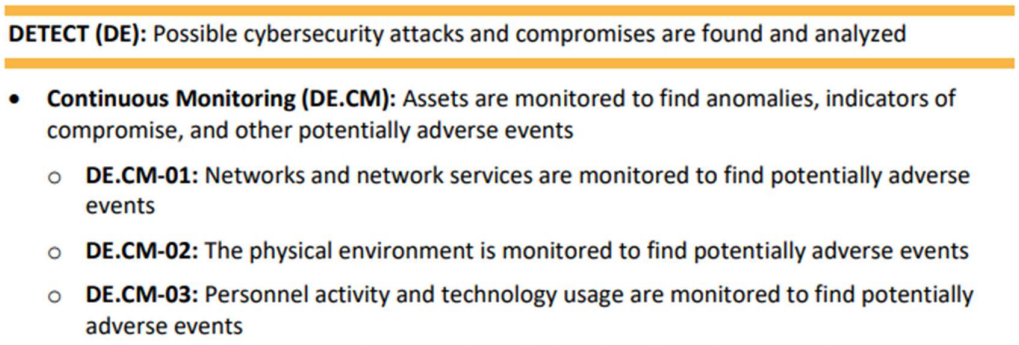
Nota. De *The NIST Cybersecurity Framework (CSF) 2.0*, por National Institute of Standards and Technology, 2024 (https://doi.org/10.6028/nist.cswp.29)

Cada categoría de controles NIST tiene controles específicos que mitigan un riesgo específico. Por ejemplo, en la categoría de Monitoreo Continuo, existe un control para detectar la creación de una conexión no autorizada que pretende exfiltrar la información de una base de datos de clientes (National Institute of Standards and Technology, 2024).

En la figura 1.4 se muestra un fragmento del marco NIST con los controles para monitorear y detectar eventos anómalos.

Figura 1.4

Ejemplo de subcategorías de Controles NIST



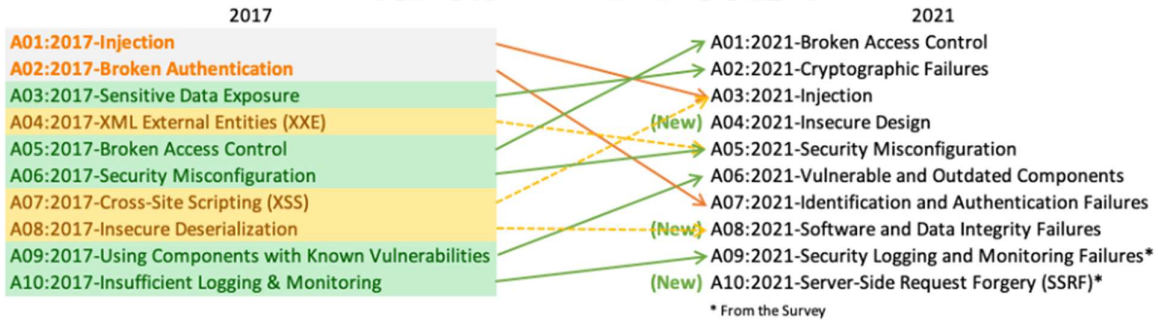
Nota. De *The NIST Cybersecurity Framework (CSF) 2.0,* por National Institute of Standards and Technology, 2024 (https://doi.org/10.6028/nist.cswp.29)

- Payment Card Industry Security Standards Council (**PCI-DSS)** que es un compendio de estándares de seguridad para proteger la información de tarjetas de crédito y débito. Las organizaciones que procesan, almacenan o transmiten datos de tarjetas de pago usan este estándar. Sirve para proteger contra el robo de datos y proteger la seguridad de las transacciones con tarjeta (Hancock, 2024).

- Open Web Application Security Project (OWASP) publicó **OWASP TOP 10** que es el compendio de los riesgos de seguridad más críticos para las aplicaciones web (Botwright, 2024). En la figura 1.5 se muestran las diez categorías de vulnerabilidades según OWASP.

Figura 1.5

OWASP Top 10 – Categorías de Riesgos en Aplicaciones Web



Nota. De *OWASP top 10 vulnerabilities: Beginner's guide to web application security risks*, por R. Botwright, 2024. Pastor Publishing.

Los estándares mostrados arriba, NIST CSF/800-53, PCI, OWASP nos proporcionan las bases para categorizar los riesgos, identificar vulnerabilidades y proponer los controles adecuados de seguridad. Mientras que TOGAF (Hornford et al., 2022) nos permite gestionar el proyecto y comunicar de manera oportuna y efectiva a través de los diferentes niveles de la organización, generando valor al término del proyecto y de manera incremental luego de haberlo puesto en marcha.

1.5 Metodología de calificación de Riesgo

Cuantitativa

Para calcular la severidad de las vulnerabilidades empleamos el método de Common Vulnerability Scoring System (CVSS) que es un sistema de puntuación utilizado para estimar el impacto de vulnerabilidades en sistemas informáticos. Este método nos permitirá priorizar las vulnerabilidades a remediar. Así al remediar primero las vulnerabilidades de mayor riesgo se logrará el mayor impacto de reducción de este, el cual se reflejará y comunicará en el scorecard. (Common vulnerability scoring system, s.f.).

Cualitativa

El scorecard y el dashboard usan los colores a continuación para proporcionar el estado general del riesgo, además de valores porcentuales indicadores de progreso continuo.

- Rojo (Alto)
- Amarillo (Medio)
- Verde (Bajo)

1.6 Tecnologías Seleccionadas

Las tecnologías seleccionadas cumplen con los siguientes requerimientos:

- Han sido probadas en el medio y por lo tanto tienen revisiones técnicas por parte de expertos y opiniones positivas de empresas usuarias.
- Son mencionadas en el cuadrante mágico de Gartner o en revisiones tecnológicas confiables.

- Son integrables con los productos de desarrollo, como bitbucket, servicios cloud y kubernetes.
- Tienen amplia cobertura de activos, por ejemplo, servidores Windows, Linux; estaciones de trabajo Windows y MAC; dispositivos de redes.
- Son de fácil adopción y baja curva de aprendizaje.

En la tabla 1.2, muestran las tecnologías (herramientas) que nos ayudan a identificar los activos (sistemas) de la empresa y las vulnerabilidades en la infraestructura y aplicaciones.

Tabla 1.2

Matriz de Tecnología, Justificación técnica y Alineación

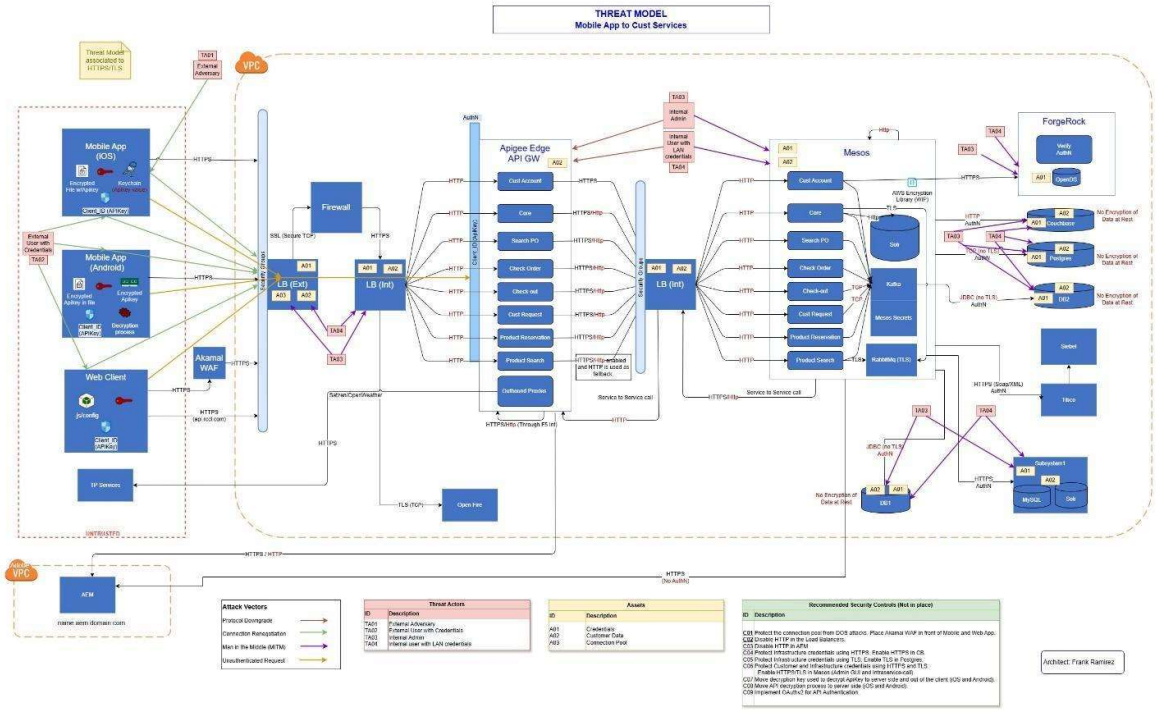
Tecnología	Justificación Técnica	Alineación
Nexpose	Identifica vulnerabilidades en la infraestructura	Scorecard, Dashboard
Snyk	Identifica vulnerabilidades en el código fuente	Scorecard, Dashboard
Burp Suite	Captura el tráfico web, ayuda a identificar vulnerabilidades dinámicamente en aplicaciones	Scorecard, Dashboard
Tanium	Identifica desviaciones de la línea base de configuración segura.	Scorecard, Dashboard
Flexera	Identifica y registrar los activos de la empresa (servidores, aplicaciones)	Scorecard, Dashboard
Archer	Contiene el registro de las soluciones y los servidores y tecnologías de la solución	Scorecard, Dashboard
Jira	Abrir los tickets para conducir las tareas técnicas de mitigación de riesgo.	Scorecard, Dashboard
Bitsight	Identifica el riesgo cibernético desde la perspectiva externa	Seguro Cibernético
Modelamiento de Amenazas	Identifica el impacto de un riesgo en distintas soluciones y sus componentes individuales	Seguro Cibernético
Patrones de Seguridad	Son artefactos reutilizables que disminuyen el tiempo y errores de implementación	Mitigación de riesgo

En la figura 1.6 se muestra un ejemplo de modelo de amenazas, como tal, identifica los vectores de ataque (puntos de ingreso) por los que una solución o sistema podría ser atacada. También se identifican los componentes que podrían ser impactados por dicho ataque. Finalmente,

nos ayuda a priorizar la mitigación de riesgos basado en el impacto que produciría un ataque exitoso.

Figura 1.6

Ejemplo de Modelamiento de Amenazas (Threat Model)



Los patrones de arquitectura son artefactos reutilizables, útiles para desarrollar o configurar los componentes de una solución de manera estándar. Un patrón de arquitectura de seguridad explica la correcta implementación de un control de seguridad en un componente de tecnología.

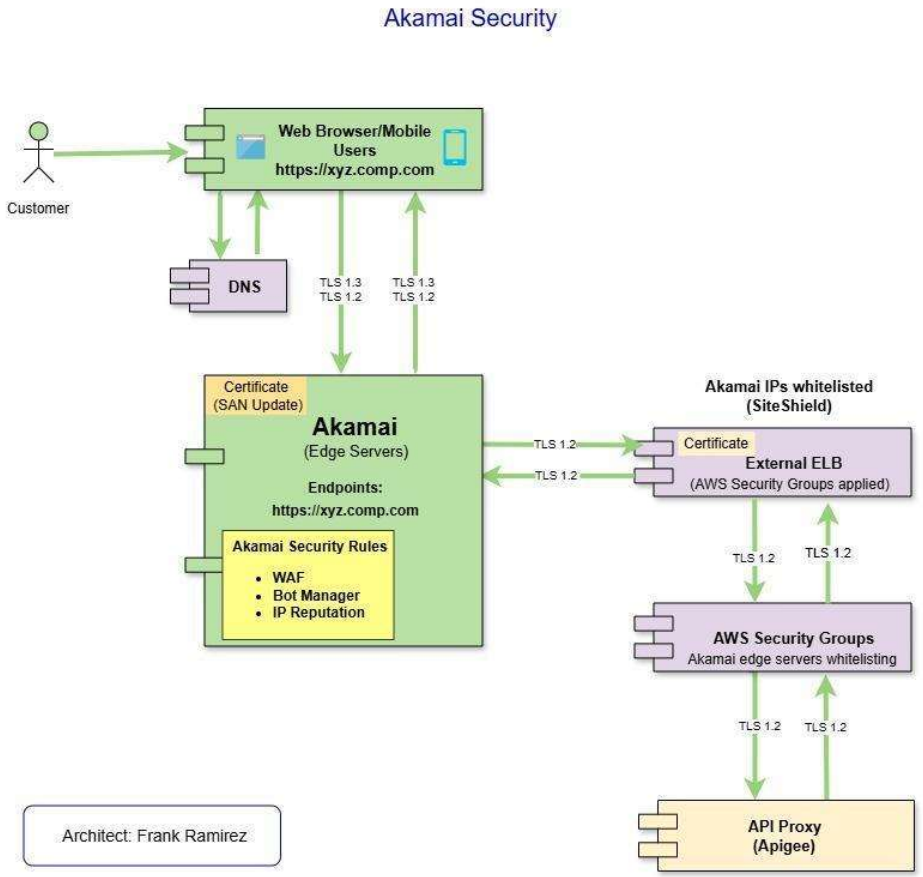
Cuando introducimos patrones de seguridad en la fase de diseño ahorramos tiempo y costos de rediseño y recodificación si es que tuviéramos que incorporarlos cuando la fase de desarrollo ya está avanzada o terminada. Finalmente, reducimos el riesgo cibernético de manera temprana en el ciclo del proyecto.

El cortafuegos de aplicaciones web (WAF) es una capa de protección contra ataques cibernéticos, que intentan inundar la aplicación con tráfico malicioso para colapsar el servicio y negar su respuesta a usuarios legítimos.

En la figura 1.7 se muestra un patrón de seguridad para la implementación de Akamai WAF y así proteger una aplicación web de ataques cibernéticos externos que pretenden saturar su capacidad de respuesta.

Figura 1.7

Ejemplo de Arquitectura de Seguridad para WAF (Akamai)

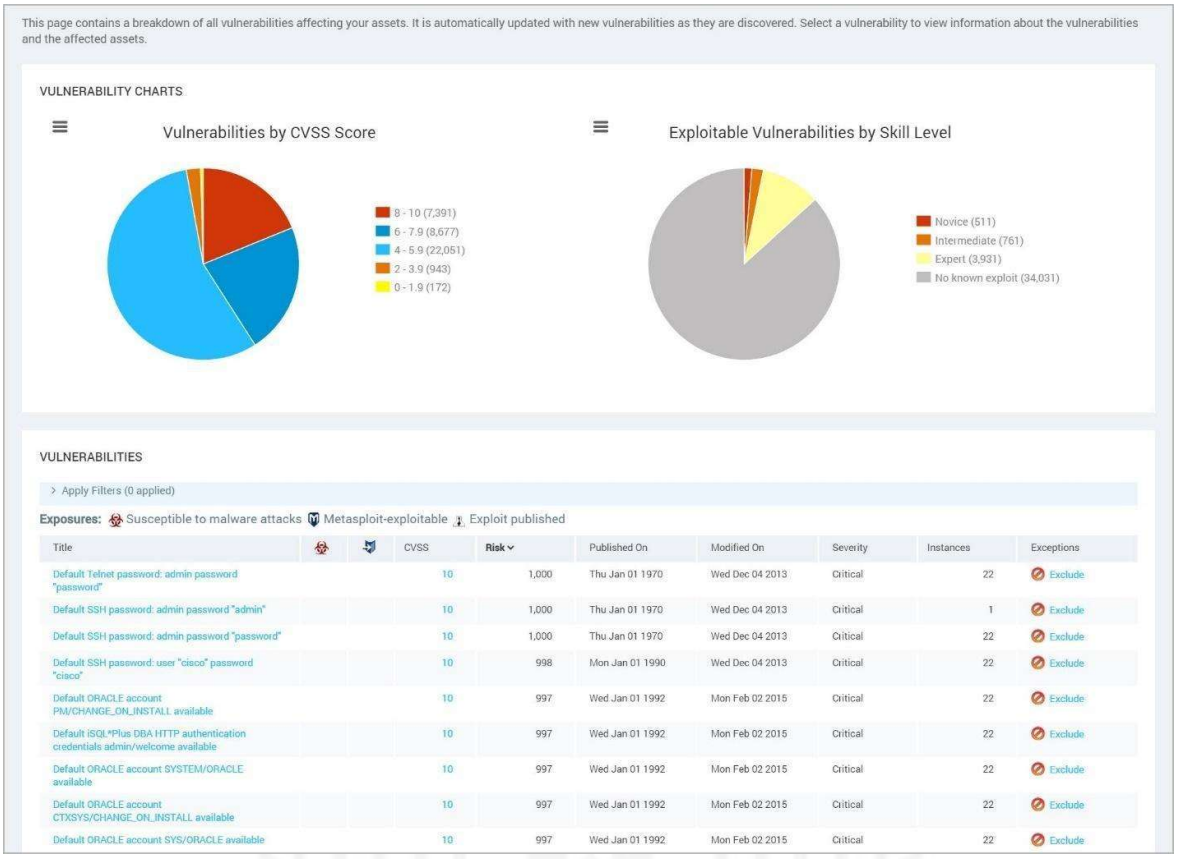


La identificación continua de vulnerabilidades es de vital importancia para mantener la infraestructura y las aplicaciones seguras y así mitigar la probabilidad de que un ataque cibernético sea exitoso al explotar dichas vulnerabilidades.

En la figura 1.8 se muestra el dashboard de Nexpose, una herramienta que escanea los activos de TI desde una perspectiva interna. Reporta las vulnerabilidades encontradas, clasificándolas por orden de criticabilidad usando la metodología de CVSS explicada anteriormente (Working with vulnerabilities, s.f).

Figura 1.8

Ejemplo de vulnerabilidades identificadas por Nexpose



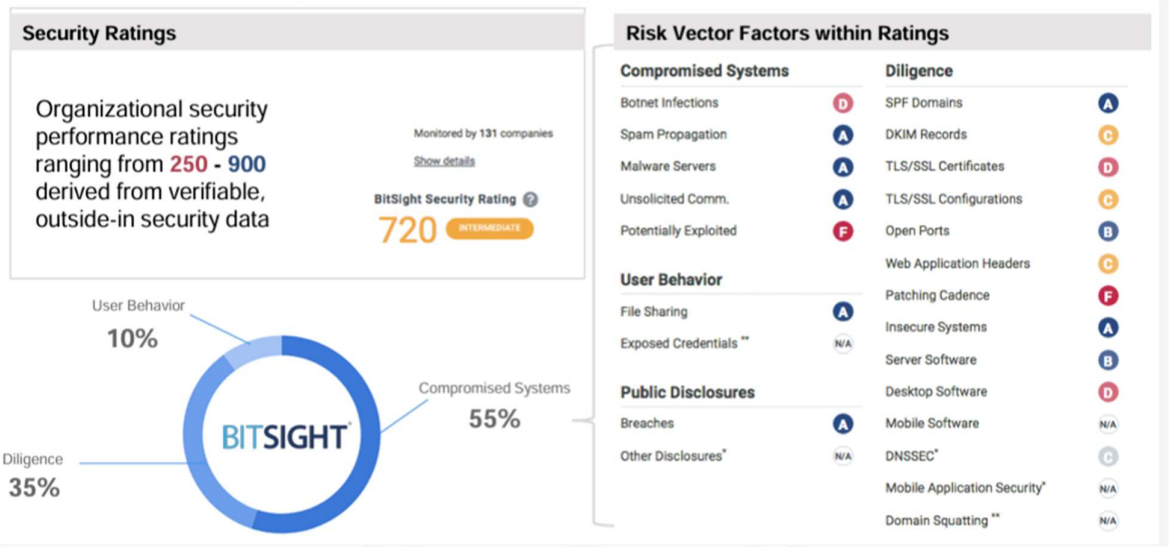
Nota. De *Working with vulnerabilities,* por Rapid7.com, s.f. (https://docs.rapid7.com/nexpose/working-with-vulnerabilities)

Para completar la identificación de vulnerabilidades tenemos que agregar la perspectiva externa, aquello que cualquier actor malicioso puede ver desde el internet. El objetivo es priorizar la resolución o mitigación de estas vulnerabilidades que presentan riesgo para la organización (Cyber Resilience Presentation, 2019). Cabe mencionar, que la calificación que de una compañía de seguridad externa es lo que va a influenciar el costo del seguro cibernético.

En la figura 1.9 se muestran las vulnerabilidades reportadas por Bitsight, un servicio y herramienta que reporta desde una perspectiva externa.

Figura 1.9

Ejemplo de vulnerabilidades identificadas por Bitsight (perspectiva externa)



Nota. De *Cyber Resilience Presentation,* por BSIGROUP, 2019, Bitsightech (https://rb.gy/iwmo60)

Todo lo mencionado en el presente capítulo converge para generar la data de vulnerabilidades y desviaciones de los estándares de configuración de seguridad. Esta data es compilada y agrupada en subcategorías de acuerdo con los estándares de seguridad de la industria como los provistos por NIST. Luego, esta información es agrupada en las diferentes categorías de seguridad del dashboard de cobertura holística en la organización. La metodología de TOGAF/ADM será empleada para capturar los requerimientos detallados de los stakeholders; comunicar apropiadamente las brechas identificadas y el plan a seguir para mitigar el riesgo cibernético en la organización.

2. CAPACIDAD DE GESTIÓN

Luego de recibir los requerimientos y de identificar a los interesados, como ha sido explicado en el capítulo anterior, tenemos que establecer:

- Plan de Gestión de los Interesados
- Estrategia de Comunicación
- Indicadores de Gestión (KPIs)
- Indicadores de Control
- Hoja de Ruta de Iniciativas
- Presentación de Resultados

2.1 Plan de Gestión de los Interesados

Para lograr el objetivo final de proveer valor al reducir el riesgo cibernético es vital mantener la interacción necesaria con los interesados. A nivel ejecutivo con el patrocinador, quien validará el diseño hacia el producto final, asegurando que provee el valor deseado. Con los líderes de portafolio, que respaldan el esfuerzo con la asignación de tiempo y recursos. Con los líderes de desarrollo, que llevarán a cabo las actividades específicas de implementación y que a su vez nos mantendrán informados del estado del progreso. La tabla 2.1 muestra el plan de gestión de los interesados.

Tabla 2.1

Matriz plan gestión de los interesados (Stakeholders)

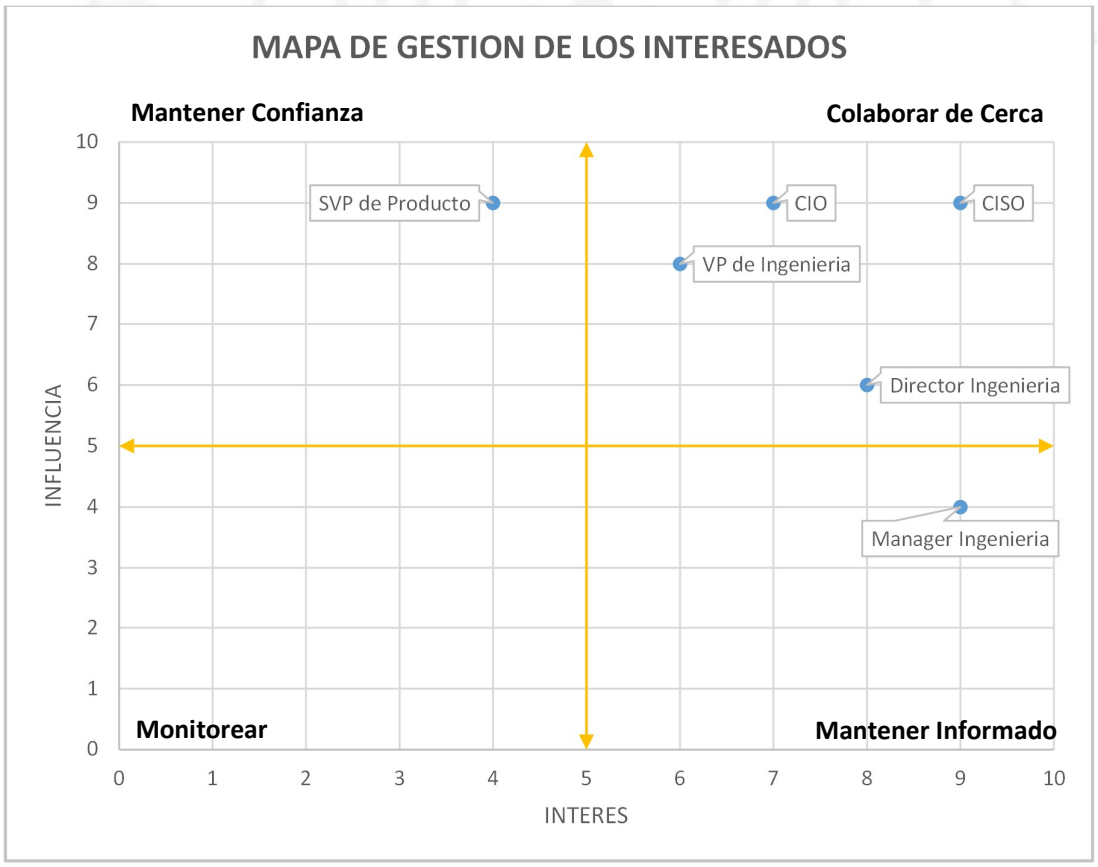
INTERESADO	NIVEL	OBJETIVOS	INFLUENCIA	INTERÉS	CONTRIBUCIÓN	MEJOR MEDIO INTERACCIÓN	FRECUENCIA INTERACCIÓN
Nombre1	CISO	Reducir el riesgo cibernético, Reducir el costo del seguro cibernético	9	9	Soporte ejecutivo inicial y esporádico	Videoconferencia	Mensual al inicio Trimestral revisión
Nombre2	CIO	Incrementar las ventas mediante la mejora de experiencia del cliente en línea.	9	7	Soporte ejecutivo inicial	Presentación del scorecard	Semianual
Nombre3	SVP de Producto	Agilizar el tiempo de puesta de servicios en producción	9	4	Ninguna	Presentación del scorecard	Semianual
Nombre4	VP de Ingeniería	Mantener los servicios y las aplicaciones operativas, generando ingresos y soportando el negocio.	8	6	Soporte ejecutivo recurrente.	Presentación del scorecard	Trimestral
Nombre5	Director Ingeniería	Mantener la estabilidad de los sistemas y aplicaciones.	6	8	Asignación y realineación de prioridades	Videoconferencia, email, chat	Mensual
Nombre6	Manager Ingeniería	Proveer los entregables según el cronograma de planeamiento.	4	9	Asignación de paquetes de trabajo	Videoconferencia, email, chat	Mensual

Para mantener el progreso del proyecto, y las disrupciones y conflictos al mínimo debemos gestionar a los interesados acorde a su influencia (poder) e interés en el proyecto, en la figura 2.1 se muestra la gestión de los interesados:

- A los que tienen mayor influencia e interés, debemos colaborar y gestionar de cerca.
- A los que tienen influencia, pero menor interés, debemos mantenerlos satisfechos, confiando que el proyecto progresa según lo esperado y sin mayor impacto.
- A los que tienen mucho interés, pero poca influencia debemos mantenerlos informados de las decisiones que afectarán sus actividades y solicitar su opinión acerca de los nuevos planteamientos, pues son ellos los que conocen los detalles técnicos y el potencial impacto de los cambios que se quieren generar.
- Aquellos con poca influencia e interés, debemos monitorearlos para detectar cuando esta situación pueda cambiar y poder gestionarlos de acorde a su nuevo estado.

Figura 2.1

Mapa de Gestión de Interesados



2.2 Estrategia de Comunicación

Para mantener los objetivos claros, validar el plan de implementación, estimar adecuadamente el nivel de esfuerzo (tiempo, recursos) y proveer información sobre el estado de progreso, así como resolver impedimentos, fue y es vital mantener los canales de comunicación abiertos con los interesados y gestionar la estrategia de comunicación explicada a continuación.

2.2.1 Basado en el Nivel Organizacional, Influencia e Interés

Se estableció una cadencia inicial de reuniones con la plana ejecutiva, de dirección y de jefatura según lo ilustrado en la tabla 2.1 anterior (semianual, trimestral y mensual). Así mismo, fue y continúa siendo importante mantener a la vista y en constante evaluación, los indicadores de influencia e interés de los interesados tal y como se muestra en la figura 2.1 anterior. Es con la combinación de estos criterios que se pudo ejecutar efectivamente la estrategia de comunicación, mantener el progreso, minimizar las disrupciones y resolver rápidamente los inconvenientes que se presentaron durante la ejecución del proyecto.

Cabe mencionar que la cadencia de reuniones varió con el tiempo, siendo más frecuente al inicio del proyecto con la plana ejecutiva y más esporádica a través de las subsiguientes iteraciones del proyecto; mientras que con los managers y los directores estas reuniones fueron más frecuentes en las siguientes iteraciones del proyecto.

Al mismo tiempo y aunque con menor frecuencia, el nivel de interés varió a lo largo del proyecto. Por ejemplo, conforme se fueron ejecutando las acciones de mitigación de riesgo, y según éstas pudieron impactar las integraciones de las distintas soluciones y los niveles de servicio, los managers y directores incrementaron su interés; prestaron más atención, consultaron más, y hubo la necesidad de hacer un planeamiento más detallado para ejecutar dichas actividades y continuar reduciendo el riesgo cibernético.

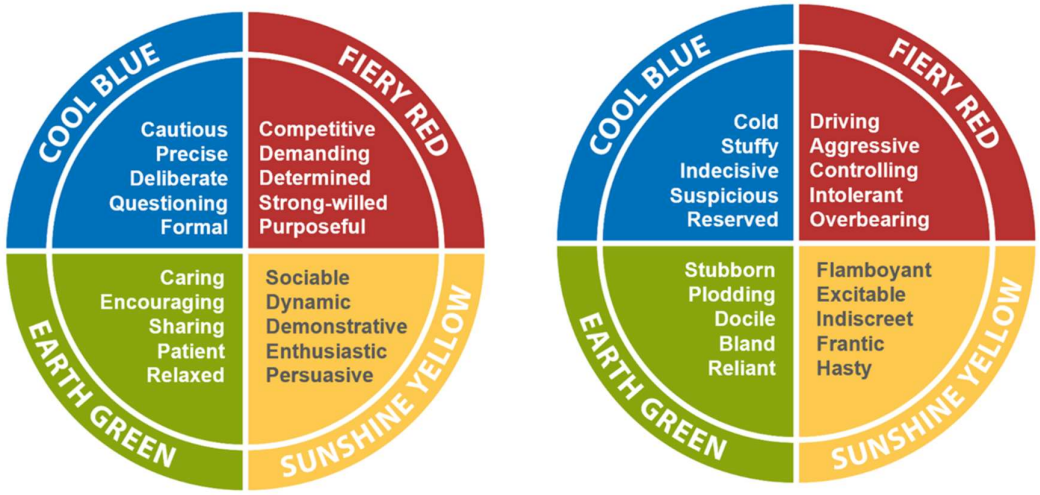
2.2.2 Identificación de Personalidades basado en “Insights Discovery”

El perfil de personalidad de Insights Discovery está basado en la tipología de Carl Jung. Emplea un sistema de colores para identificar las características de la personalidad, como fortalezas, debilidades, conducta y preferencias de comunicación (Insights Group, 2021).

En la figura 2.2 se muestran los cuatro tipos de personalidad y sus respectivas energías en un buen y en un mal día.

Figura 2.2

Los Cuatro Tipos de Personalidades de Insights Discovery (Buen día a la izquierda y Mal día a la derecha)



Nota. De *Validating Insights Discovery,* por The Insights Group, 2021, Insights (https://www.insights.com/media/2728/insights-discovery-validating-the-system-factsheet.pdf)

Me ha sido muy útil en la práctica para poder comunicarme y motivar a los profesionales con los que interactúo. Ya que me ayuda a identificar que motiva, que molesta, las preferencias de trabajo, y las preferencias de cómo gestionar a cada miembro del equipo o colaborador cros-funcional.

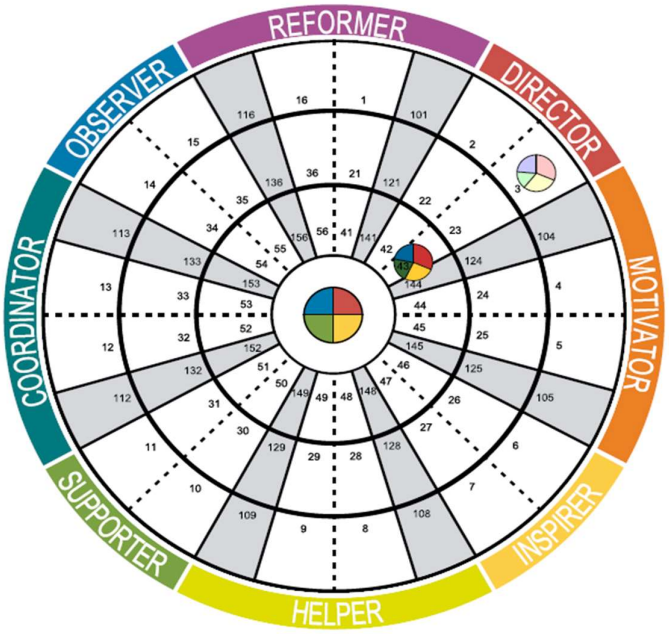
Igualmente, me ha ayudado al autoconocimiento de mí mismo. Entendiendo cuales son las fortalezas que me ayudan en lo profesional y que debo mantener, así como cuáles son los aspectos que pudieran influenciar positiva o negativamente a otros. Facilitándome la calibración de estas energías según sea necesario y según la situación lo demande para liderar el proyecto exitosamente, manteniendo relaciones de confianza y buena colaboración.

Cabe mencionar que todos tenemos mayor o menor cuantía de las cuatro energías. A continuación, el esquema visual que representa mi personalidad, preferencias y energías. Mi perfil es representado en orden de significancia por los colores, Rojo, Amarillo, Azul y Verde.

Tomando como referencia los cuatro tipos de personalidad previamente expuestos, la figura 2.3 presenta una representación visual de mi personalidad.

Figura 2.3

Resultado Visual del Análisis de mi Personalidad



2.2.3 Empleo de Habilidades Blandas

El desarrollo de habilidades blandas me ha servido para poder comunicarme e interactuar de manera efectiva en el ambiente laboral. Es más, lo descrito anteriormente sobre los tipos de personalidades y el autoconocimiento me han provisto con una visión amplia y al mismo tiempo específica de cómo poder interactuar de manera efectiva con mis colaboradores. Dentro de las habilidades blandas podemos destacar:

- **Comunicación asertiva**

  Forma parte de las habilidades blandas y juega un rol fundamental conforme se va escalando profesionalmente. Para este proyecto, ser concreto, claro y proveer actualizaciones sobre el estado de este, manteniendo enfoque en los objetivos de cada interesado ha sido instrumental para el éxito del proyecto.

- **Trabajo en equipo**

Se enfoca en construir relaciones profesionales con nuestros colegas, dentro de nuestro equipo y con los equipos con los que interactuamos.

A lo largo de mi trayectoria, me ha sido muy útil reconocer las fortalezas y debilidades de los diferentes profesionales con los que trabajo. Me sucedió en el pasado que tuve que escoger un líder para mi equipo, para lo cual tenía dos candidatos. El primero de personalidad carismática y hábil. El segundo de personalidad más seria y hábil. Aunque todo parecía indicar una preferencia por el primer candidato debido a su carisma, yo opté por elegir al segundo candidato dada su ligera mayor dedicación y más significativa fiabilidad. Mi director escogió al otro candidato para liderar otro equipo similar al mío. Luego de alrededor de mes y medio, el candidato carismático decidió regresar a mi equipo por voluntad propia porque no estaba personalmente preparado para aceptar mayor responsabilidad. El candidato que yo escogí para liderar el equipo ha escalado nuevamente y hoy es un gerente en aquella gran compañía financiera.

- **Negociación**

Para encontrar un balance adecuado entre los objetivos que queremos lograr y al mismo tiempo evitar fricción tanto como sea posible en las operaciones de otros grupos.

Me ha sido de mucha utilidad poner en conjunto el mapa de gestión de los interesados y conocer sus objetivos para poder negociar y encontrar un punto intermedio a la hora de introducir los controles de seguridad dentro de las aplicaciones y soluciones que forman parte de sus portafolios.

Para este proyecto de mitigación de riesgo surgieron diversos imprevistos durante la ejecución de la hoja de ruta que contiene las diferentes iniciativas para mitigar el riesgo en la organización. Uno de estos imprevistos fue que una de las aplicaciones debido a su tecnología antigua, no soporta la integración con los sistemas de gestión de identidad modernos de la empresa para ejecutar la autenticación y autorización de manera segura. Más aún el sistema es provisto por un tercero, y para poder integrarlo con la solución empresarial de gestión de identidades, esta aplicación necesitaría cambios fundamentales en su código fuente, lo cual conllevaría a nuevas órdenes de cambio y los costos asociados para generar estos cambios en el código fuente. Dada la situación recurrí a un plan de mitigación de riesgo que requirió la negociación entre seguridad, el área de negocio y el proveedor de software. Ya no se requirieron cambios significativos en el código fuente para la integración con el sistema empresarial de gestión de identidades, sin embargo, el

proveedor se comprometió a integrar su sistema con el protocolo ligero de acceso a directorios (LDAP) que facilita el almacenamiento y búsqueda de la información sobre usuarios, recursos y aplicaciones de la empresa de manera segura.

De esta manera se mitigó el riesgo cibernético de una aplicación de significativa importancia para el negocio y a cero costos para la empresa.

- **Empatía**

Se refiere a considerar las emociones y sentimientos de los demás.

He aprendido durante mi trayectoria que las personas con las que colaboramos puede que no recuerden los detalles específicos de una situación en particular, sin embargo, siempre recordarán lo que sintieron al interactuar con nosotros.

En este proyecto, así como en muchos otros, he podido construir relaciones duraderas de trabajo poniéndome en el lugar de mi colaborador. Pensando en las diferentes maneras en las que he podido hacer su trabajo más sencillo o resolviendo los inconvenientes de la manera más eficiente para ellos, sin dejar de lado los objetivos de seguridad.

- **Resolución de Problemas**

Es normal y esperado que en algún momento durante un proyecto o a lo largo de nuestras carreras surjan desacuerdos o problemas. La resolución constructiva de estas situaciones conlleva a una evolución de estas relaciones, fortaleciéndolas aún más.

Cuando estaba en Citibank, uno de los miembros del equipo se acercó mencionando que le tocaba hacer pruebas de vulnerabilidad a una aplicación demasiado grande y que esa carga de trabajo sumada a la existente sobrepasaba significativamente su capacidad semanal. Sucede que la mayoría de las aplicaciones en las que se iba a trabajar la siguiente semana ya habían sido autoasignadas. Al inspeccionar las asignaciones de cada uno de los miembros del equipo, noté que la aplicación de este colaborador tenía zona horaria en Singapur. Por lo tanto, procedí a intercambiar una aplicación pequeña asignada en Singapur pero que tenía zona horaria en Estados Unidos con la de este colaborador.

Los resultados de esta resolución fueron dos. Primero, que la carga de trabajo fue distribuida de manera más eficiente. Segundo, este miembro del equipo notó una preocupación por su bienestar personal e interés en apoyarlo para que logre un mejor desempeño, por lo cual la relación de confianza se fortaleció.

2.3 Indicadores de Gestión (KPIs)

Se identificaron nueve indicadores de gestión mostrados a continuación:

- **Administración de la configuración**

  El porcentaje de activos que se adhieren a las líneas base de seguridad mínima, generan registros de actividad y utilizan imágenes aprobadas por el departamento de seguridad.

- **Vulnerabilidades**

  El porcentaje de activos con el agente Nexpose instalado que efectúa búsquedas locales de vulnerabilidades.

- **Seguridad de endpoints**

  El porcentaje de activos con software de gestión de dispositivos y agentes de Antivirus y Antimalware instalados.

- **Remediación**

  El porcentaje de hallazgos de seguridad remediados dentro de los plazos establecidos.

- **Gestión de Identidad y Acceso (IAM)**

  El porcentaje de aplicaciones con “single sign on”, “administración de acceso privilegiado” y certificados gestionados por el departamento de seguridad.

- **Seguridad de aplicaciones**

  El porcentaje de aplicaciones sin secretos en el código y con vulnerabilidades de código fuente remediadas.

- **Conciencia de seguridad**

  Porcentaje de usuarios que han completado los entrenamientos de seguridad en línea. Así como el porcentaje de usuarios que ha hecho clic en enlaces de Phishing.

- **Gestión de riesgos de terceros**

  Porcentaje de proveedores de soluciones de software que han sido validados por el departamento de seguridad y que han completado su revisión de seguridad y sin incidentes.

- **Gestión de activos**

  Porcentaje de activos con sistemas operativos y software bajo soporte.

2.4 Indicadores de Control

Incluidas en los nueve indicadores de gestión (KPI), se incluyen 24 indicadores de control. Solo mencionaremos un indicador de control por KPI para mantener la concisión del presente documento.

- Administración de la configuración
    - Activos que generan registros
- Vulnerabilidades
    - Escaneos autenticados de vulnerabilidad
- Seguridad de endpoints
    - Activos con agentes de Antivirus y Antimalware instalado
- Remediación
    - Remediaciones a tiempo
- IAM
    - Aplicaciones con single sign on
- Seguridad de Aplicaciones
    - Secretos en el código fuente
- Conciencia de Seguridad
    - Entrenamiento de seguridad de desarrollo completado a tiempo
- Gestión de Riesgo de Terceros
    - Proveedores sin incidentes
- Gestión de Activos
    - Sistemas operativos con soporte

2.5 Hoja de Ruta de Implementaciones

Para mitigar el riesgo cibernético fue necesario crear una hoja de ruta con las diferentes iniciativas. Las iniciativas de seguridad llenarán las brechas y nos llevarán al estado deseado de seguridad. Cada iniciativa se encarga de elevar la postura de seguridad cibernética de la organización y afectará positivamente cada uno de los indicadores de control y gestión.

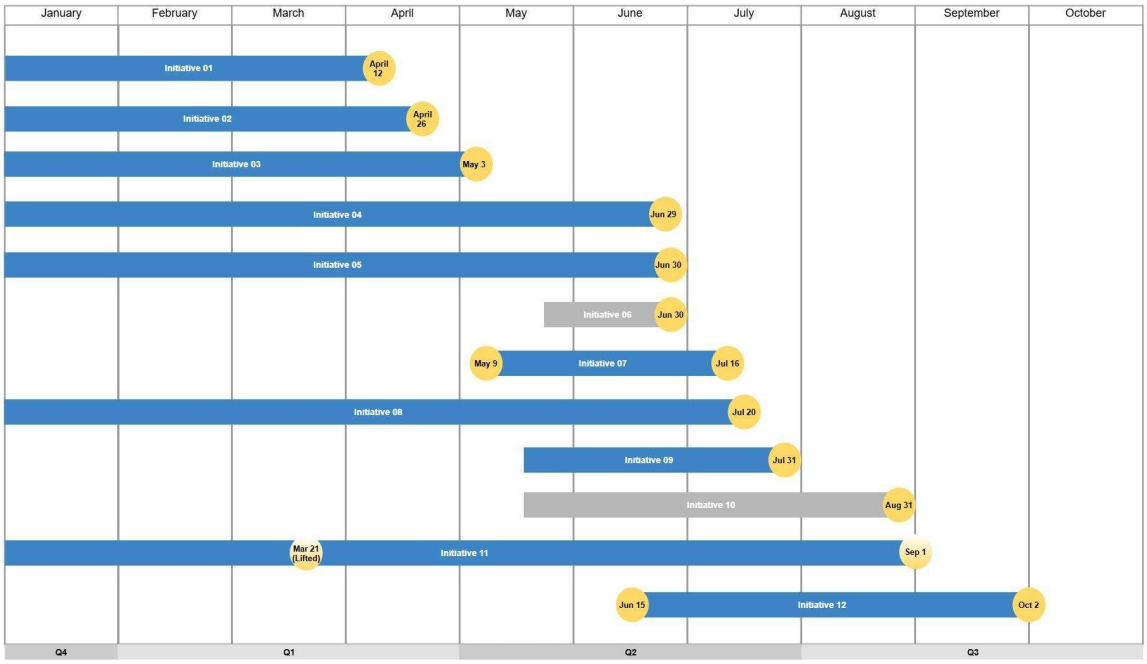
Ejemplos de iniciativas:

- Actualización o migración de sistemas operativos cerca a perder soporte.
- Escaneo de vulnerabilidades de componentes en la nube.
- Migración de la Autoridad de certificados.
- Eliminación de secretos en el código fuente
- Migración de la solución de Integración Continua

La figura 2.4 muestra la hoja de ruta con las iniciativas de seguridad, detallando el trimestre, mes y día de vencimiento. La hoja de ruta es presentada al VP de ingeniería y a sus directores. El detalle de cada iniciativa está anonimizado dado el grado de sensibilidad de la información.

Figura 2.4

Hoja de Ruta con las Iniciativas de Seguridad



2.6 Presentación de Resultados

Recordemos que tenemos dos requerimientos, disminuir el riesgo y disminuir el costo del seguro cibernético. El segundo requerimiento es prácticamente una consecuencia del primero; sin embargo, tendremos que expandir ligeramente el alcance de las remediaciones y actividades para cumplir con el segundo requerimiento.

A continuación, en la tabla 2.2 se muestran los tipos de calificadores elegidos para comunicarnos con los VPs (colores del scorecard) y directores (porcentajes en el dashboard). Así como, el alcance de cada calificador a nivel de la empresa, portafolio de aplicaciones o de aplicaciones individuales.

Tabla 2.2

Matriz de Calificadores, Tipo, Alcance y Presentación

Calificador	Tipo	Nivel de Alcance	Medio de Presentación
Cualitativo	Rojo (Alto) Amarillo (Medio) Verde (Bajo)	Empresa Portafolio	Scorecard Dashboard
Cuantitativo	Porcentual	Empresa Portafolio	Scorecard Dashboard
	Numérico/CVSS	Portafolio Aplicación Vulnerabilidad	Dashboard Tablas

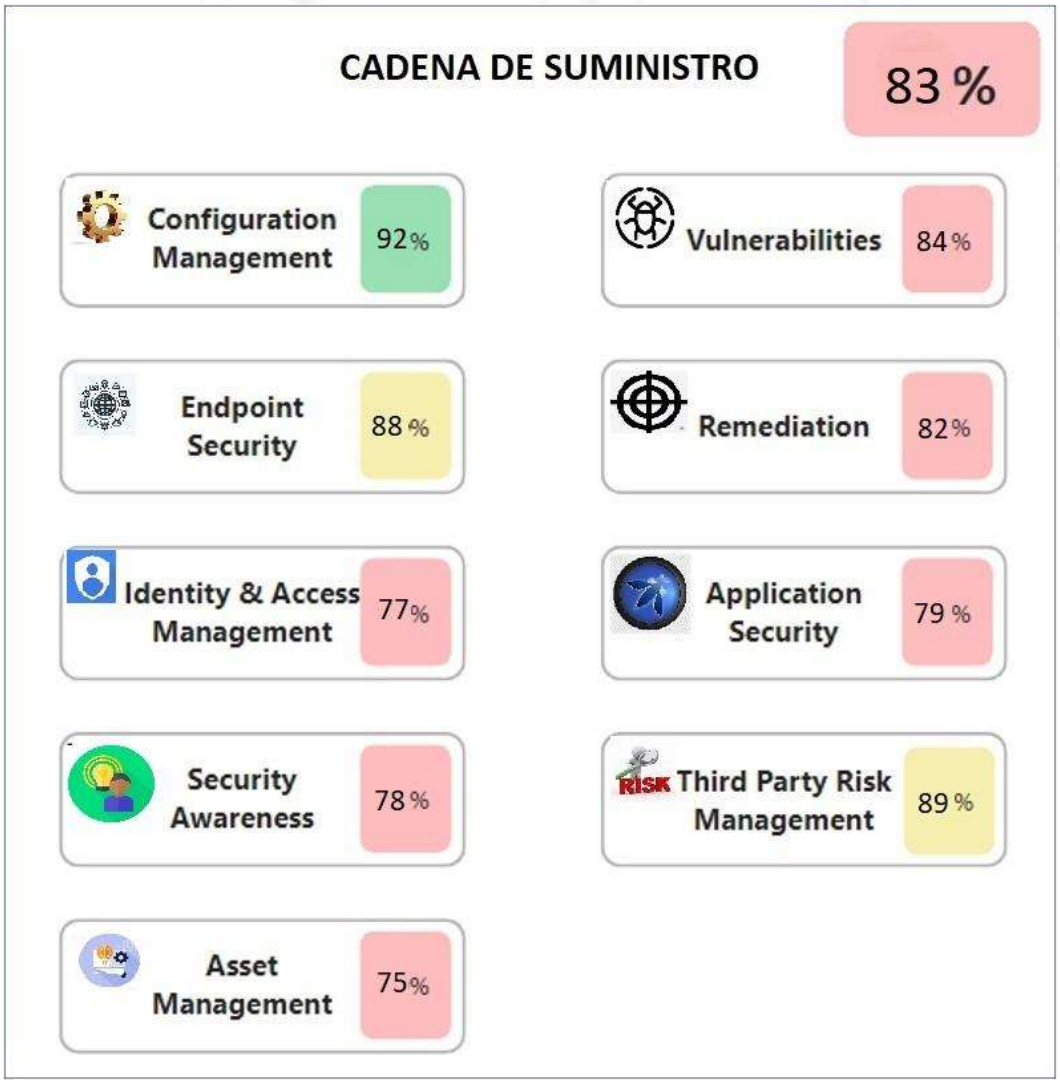
2.6.1 Scorecard

El scorecard es el producto final, presentado a directores, VP, SVP, CISO y CIO. Muestra los indicadores de gestión en colores y porcentajes. El scorecard puede mostrar resultados para toda la empresa o por área de negocio. Cada área de negocio tiene un VP responsable.

En la figura 2.5 se muestra una imagen del scorecard con los indicadores de gestión y sus porcentajes.

Figura 2.5

Scorecard de la Cadena de Suministro mostrando una vista general de los indicadores de gestión



2.6.2 Dashboard

Los directores se ubican organizacionalmente debajo del VP. El dashboard es presentado y entregado a los directores y muestra los indicadores de gestión de cada uno de sus portafolios.

En la figura 2.6 se muestra el dashboard con los indicadores de gestión representados por medidores semicirculares y haciendo uso de los calificadores cualitativos (colores) y cuantitativos (porcentajes). Los colores muestran visualmente que tan cerca, se está de cada umbral y el porcentaje provee información más precisa de cuánto queda por ejecutar.

Figura 2.6

Dashboard mostrando los indicadores de gestión y su progreso

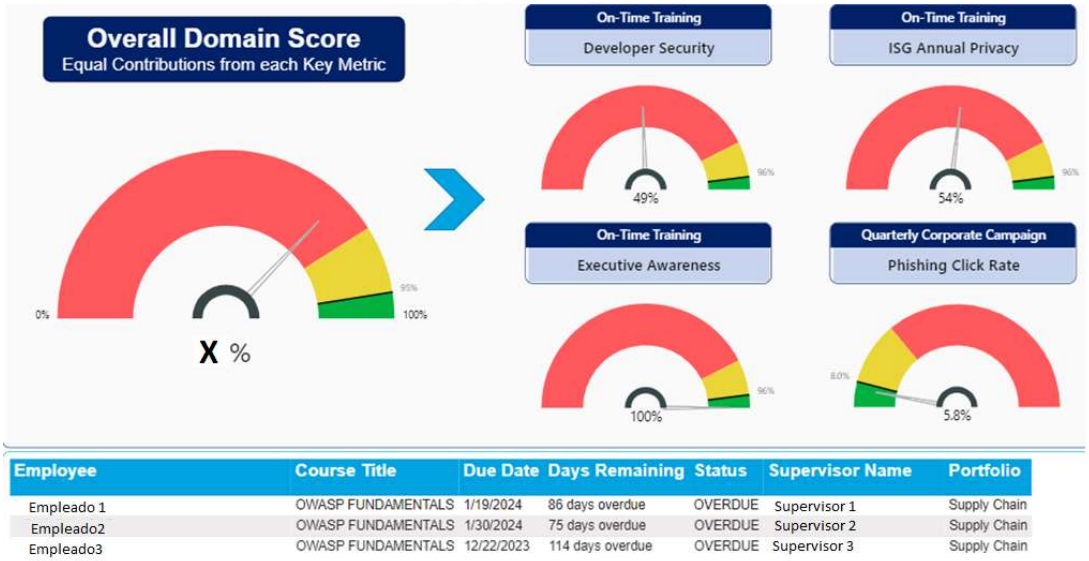
2.6.3 Tablas

Los directores tienen la opción de exportar la información detallada de los indicadores de control en tablas de hojas de cálculo y entregarla a los managers de desarrollo que les reportan. Son los managers quienes liderarán las actividades técnicas de remediación y sus equipos los que ejecutarán e implementarán los paquetes de trabajo.

En la figura 2.7 muestra cómo los directores pueden acceder a los indicadores de control y decidir cuáles priorizar. Luego pueden exportar el detalle mostrado en la tabla al pie del indicador de control y asignarlo al manager respectivo. El manager finalmente asignará las tareas técnicas específicas para la remediación.

Figura 2.7

Indicadores de Control



Employee	Course Title	Due Date	Days Remaining	Status	Supervisor Name	Portfolio
Empleado 1	OWASP FUNDAMENTALS	1/19/2024	86 days overdue	OVERDUE	Supervisor 1	Supply Chain
Empleado2	OWASP FUNDAMENTALS	1/30/2024	75 days overdue	OVERDUE	Supervisor 2	Supply Chain
Empleado3	OWASP FUNDAMENTALS	12/22/2023	114 days overdue	OVERDUE	Supervisor 3	Supply Chain

Al riesgo cibernético existente, se aúnan las nuevas amenazas cibernéticas que emergen prácticamente a diario. La gestión de mitigación de riesgo cibernético es un proceso continuo y con cada iteración se seguirá reduciendo más el riesgo.

Finalmente, se lograron los dos requerimientos inicialmente entregados. Primero, se disminuyó el riesgo cibernético en 12% durante los primeros cinco meses. Segundo, se logró renegociar el seguro cibernético y disminuir su costo en un 25%.

3. APRENDIZAJE CONTÍNUO

Mi trayectoria profesional puede ser resumida de la siguiente manera. Los primeros 5 años enfocado en el área comercial y servicios. Los 17 años posteriores en seguridad de la información.

3.1 Capacitación técnica y de Gestión

Desde el inicio me fue evidente que para poder mejorar y progresar profesionalmente era necesario continuar preparándome y aprendiendo. Durante los años en comercial y servicios tuve la oportunidad de certificarme en los diferentes portafolios de software IBM, Websphere, Lotus, Content Management, Tivoli. Este conocimiento aunado a las relaciones interpersonales con los partners de IBM me ayudó a entender la naturaleza del negocio comercial de software y a poder integrar a estos partners en proyectos que yo gestionaba.

Los últimos 17 años en seguridad de la información se han caracterizado por un aprendizaje continuo de las diferentes áreas del campo, como hacking ético, regulaciones de tarjetas de crédito, numerosos webinars, generación y gestión de la arquitectura empresarial, gestión de seguridad de la información, y el desarrollo de habilidades blandas.

A continuación, se presenta la tabla 3.1, que detalla las capacitaciones realizadas en los últimos 11 años, incluyendo certificaciones, cursos y conferencias

Tabla 3.1

Listado de Capacitaciones del 2014 al 2024

Período	Curso / Institución	Alcance	Resultado
2014	Ethical Hacking (CEH) / EC-Council	Habilidades fundamentales para hallar vulnerabilidades	Certificación
2014	Web Application Security / Securosis	Entrenamiento específico para identificar vulnerabilidades en aplicaciones web	Aprendizaje
2015	ITIL Foundation / Axelos	Gestión de servicios de TI	Certificación
2015	Project Management (PMP) / PMI	Gestión de Proyectos	Certificación
2016	Payment Card Industry (PCIP) / PCI-DSS	Regulación de la información de tarjetas de crédito	Certificación

continuará

continua

Período	Curso / Institución	Alcance	Resultado
2016	Azure Cloud Fundamentals / Microsoft	Tecnología de la nube de Microsoft	Aprendizaje
2016	Time Management / Royal Caribbean HR	Administración efectiva de tiempo. Provisto por el departamento de RH.	Aprendizaje
2017	AWS Architect / Amazon	Tecnología de la nube de Amazon	Certificación
2017	Blackhat Conference / BlackHat Training	Tres días de conferencias de seguridad donde se informan las nuevas tendencias de subversión de sistemas	Aprendizaje
2017	Team Management / Royal Caribbean HR	Gestión de nuestro equipo de trabajo. Cómo motivar y cómo resolver conflictos. Provisto por el departamento de RH.	Aprendizaje
2018	Cloud Security Professional (CCSP) / ISC2	Consideraciones generales de cómo gestionar e implementar seguridad en la nube	Certificación
2018	Factored Analysis of Information Risk (FAIR) / The Open Group	Estimación del riesgo cibernético en valor monetario	Certificación
2019	GIAC Strategic Planning, Policy, and Leadership (GSTRT) / SANS Institute	Elaboración de la estrategia de seguridad de la información	Certificación
2019	Blackhat Conference / BlackHat	Tres días de conferencias de seguridad donde se informan las nuevas tendencias de subversión de sistemas	Aprendizaje
2020-2022	Executive MBA / UF Warrington	Maestría en Administración de Negocios. 19 cursos en total	Maestría
2023	Leading with Stories / Linkedin Autoestudio	Cómo motivar al equipo de trabajo	Aprendizaje
2023	TOGAF Foundations / EA Principals	Elementos básicos para generar arquitectura empresarial	Certificación
2024	TOGAF Practitioner / EA Principals	Cómo gestionar y comunicar la arquitectura empresarial.	Aprendizaje
2024	Insights Discovery / Betsy Blanchard	Descubrimiento de los diferentes perfiles de personalidad.	Aprendizaje

Adicionalmente, para mantener las certificaciones activas, las organizaciones emisoras de estas como EC-Council, ISC2, GIAC y SANS, exigen someter a través de sus portales en promedio 30 horas de entrenamiento continuo al año. Dentro de los cuales hay numerosos webinars y presentaciones de proveedores de tecnología.

3.2 Contribuciones

Como parte de mi desempeño laboral, he tenido la oportunidad de contribuir tanto académicamente como profesionalmente.

Durante mi preparación para la certificación de profesional de la industria de tarjetas de pago (PCIP) estuve usando el libro oficial de PCI-DSS, el cual contiene los requerimientos de PCI y una amplia relación de preguntas y respuestas como práctica previa al examen de certificación. Mientras progresaba con la lectura del libro, pude identificar cerca de nueve errores en diferentes respuestas, así que procedí a hacer una relación detallada de los errores, la cual sometí como referencia a la organización PCI-DSS para que condujeran su propia revisión. Luego de cerca de una semana recibí un email de agradecimiento, confirmando la consiguiente actualización del libro.

En lo profesional y en mi calidad de líder del equipo de vulnerabilidad tuve la oportunidad de entrenar a nuestros nuevos miembros en técnicas de ethical hacking (hacking ético) para que descubran las vulnerabilidades en las aplicaciones y estas vulnerabilidades sean corregidas antes de ser explotadas por actores maliciosos. Además, mediante coaching pude ayudarles a madurar su capacidad profesional, tanto en habilidades técnicas, como de conducta organizacional y de trabajo en equipo.

En otra oportunidad en la que estaba trabajando con un proveedor de scorecard de seguridad, al percatarme que dicha solución carecía de información gráfica apropiada para niveles ejecutivos. Procedí a generar mi propia versión inicialmente para uso interno pero que posteriormente compartí con el representante del proveedor, y con su equipo de desarrollo. Como resultado, incluyeron por primera vez en su producto de software (scorecard) el infográfico que les proveí y además agregaron algunos gráficos adicionales orientados a un nivel ejecutivo.

3.3 Aplicación de Conocimientos

Como práctica regular, programe una sesión mensual de lecciones aprendidas. Durante estas sesiones cada miembro del equipo tenía la oportunidad de compartir que había ido bien, que funcionó mejor de lo esperado, y que no funcionó en cada uno de sus proyectos. El objetivo de estas reuniones es identificar lo que debíamos seguir haciendo como equipo para mantener la eficiencia, así como para compartir que soluciones funcionaron frente a problemas técnicos o de interrelación personal.

Comparativamente, resolver problemas técnicos tiende a ser mucho más “sencillo” que resolver conflictos laborales.

Para resolver problemas técnicos puede que baste poner a los ingenieros juntos en una sala y no demorarán mucho en presentar opciones de solución, o un plan de desarrollo de conocimientos. Mientras que, los conflictos laborales tienden a estar rodeados de emociones, objetivos y expectativas personales. Para resolver conflictos laborales, hay que reconocer personalidades, los botones rojos de cada persona y siempre se lidia con emociones que pueden estar elevadas en determinado momento, y es imprescindible el uso de habilidades blandas para poder comunicar apropiadamente, ya que no siempre lo que se intenta decir es lo que el receptor ha entendido. Las diferencias organizacionales y culturales juegan un rol muy importante. Las compañías americanas se caracterizan por su multiculturalidad y es muy común encontrar colaboradores de diferentes partes del mundo, cada uno con su modo particular de trabajar y de conducirse. Un ejemplo es el modelo de reportar de un recurso de Asia versus un recurso de las Américas. Típicamente un recurso de las Américas se siente empoderado para actuar y luego informar, mientras que un recurso del continente asiático solicitará mayormente la aprobación de su supervisor antes de realizar cualquier acción. Hay múltiples consideraciones para gestionar en un ambiente multicultural, en donde el beneficio es la originalidad y diversidad de ideas.

Como parte de mis planes de aprendizaje continuo, tengo programado para este año certificarme en TOGAF Practitioner. Y en el 2025 planeo llevar el curso de C-CISO con miras a la certificación. En mi rol actual de BISO (nivel de director) y con la certificación de C-CISO me encontraré mejor posicionado para buscar el siguiente nivel de responsabilidad alineado bajo el título de director en una organización mediana a grande o CISO en una organización pequeña a mediana.

En el área de *Analítica de Datos*, ya no es novedad pensar que Machine Learning con sus modelos de lenguaje es la tecnología que posiblemente crecerá más durante la siguiente década. Y es que, para los que estamos en el campo por varios años hemos podido apreciar nuevas revoluciones tecnológicas en periodos de no más de 15 años. La inteligencia artificial se está desarrollando a pasos ágiles, así como su adopción por soluciones comerciales y por empresas, generando nueva información que les permita incrementar su participación en el mercado. ChatGPT, seguido de Gemini (Google), Grok (X), y LLAMA (Meta AI) presentan nuevas herramientas de crecimiento empresarial y explotación del mercado.

Compañías como las de retail, emplean hoy en día la analítica descriptiva para tomar decisiones de negocio informadas. Y los equipos de desarrollo emplean segmentación de la

información para trasladar información anonimizada del ambiente de producción al ambiente de stage, con la finalidad de proceder con pruebas funcionales y unitarias previas a una nueva versión de su aplicación.

El campo de seguridad de la información también emplea machine learning, y está presente en varias de sus herramientas de seguridad. Herramientas que se apoyan en aprendizaje supervisado como aprendizaje no-supervisado.

Los sistemas de prevención de intrusiones (IDS) emplean el *aprendizaje supervisado* de machine learning, por el cual paquetes individuales IP de datos son manualmente identificados y marcados como tráfico normal o malicioso. Como BISO proporciono guías y parámetros que deben configurarse en el IDS para detectar ataques y tráfico malicioso. Luego de entrenar un modelo de machine learning con esos paquetes ya marcados, el modelo se pondrá en marcha y podrá identificar por sí mismo los paquetes maliciosos y generar alertas para el centro de operaciones de seguridad (SOC). En mi rol de BISO solicito la generación de alertas a nivel empresarial, solicito que los registros (logs) generados por el IDS sean enviados al SOC, y este genere las alertas que serán revisadas por el equipo de detección de intrusiones. En caso de que alguna actividad salga de los parámetros normales, se me comunica para revisión y mitigación inmediata. Luego del afinamiento de estos parámetros el ruido (false positives) disminuyó en 30%.

Otros sistemas de seguridad, como Akamai Bot Manager, emplean el *aprendizaje no-supervisado* de machine learning para identificar actividades maliciosas como web scraping. Web scraping tiene como objetivo identificar y extraer la data de los artículos y sus precios de venta, típico escenario que sufre una compañía de venta al por menor (retail). El aprendizaje no-supervisado usa a su vez algoritmos de clustering para identificar y categorizar grupos similares de información (registros), de modo que cualquier instancia (registro) que no quepa en una de esas categorías, será considerado como tráfico o actividad maliciosa. En este caso, Akamai Bot Manager, haciendo uso del aprendizaje no-supervisado generará un perfil del origen de la aplicación cliente sin hacer uso de etiquetas y así podrá detener muchos de los intentos de web scraping. Por ejemplo, una de las últimas implementaciones de Akamai WAF fue para proteger el portal de reservas de cruceros para clientes (el dominio principal, .com), diseñé la arquitectura para que el WAF este delante del Website para clientes y solicité la habilitación de los controles de umbrales de tráfico, renegociación de conexiones TLS, y de geolocalización para excluir tráfico IP de países listados como terroristas por los Estados Unidos de América. Luego de elaborar la arquitectura y de la implementación de los controles y especificaciones que diseñé, el consumo de los recursos de CPU y red de los servidores web disminuyó en 15%.

En lo referente a *presupuestación de capital*, durante mi MBA Ejecutivo, tuve la oportunidad de adquirir conocimientos financieros. Dentro de ellos la *proyección de flujos de efectivo y económico*, FCF por sus siglas en inglés Free Cash Flow. El Flujo de Caja Libre (FCF) representa la cantidad de efectivo que una empresa genera después de deducir los gastos operativos y las inversiones de capital.

Este conocimiento me ha sido particularmente útil para hacer crecer mi portafolio de acciones. El FCF me ha permitido hacer una proyección más realista que la que provee la utilidad neta, pues el FCF incluye el costo del capital y el costo del equity (embebido en el WACC). Empleando el método del FCF se obtiene una valuación más precisa de la acción de una compañía, de modo que nos ayuda a determinar si una acción está sobrevaluada o por debajo de su valor real para comprar barato.

Es cierto que antes de comprar hay que hacer una evaluación más integral de la salud de una empresa, especialmente si es una de las no tan conocidas o de ser una empresa que recién cotiza en la bolsa de valores. Esos factores de salud son comunicados a través de los indicadores F (Piotroski) o Z (Altman), para ver la salud financiera o la posibilidad de bancarrota, respectivamente. Aunado a los indicadores de múltiplos de valoración de la industria a la que pertenece la compañía, a sus Balances y a su Estado de Ingresos, podemos estimar la valoración de la compañía y determinar si es conveniente comprar sus acciones.

También debemos considerar los riesgos intrínsecos de estos métodos financieros. Por ejemplo, el FCF se basa en una proyección estable y constante de crecimiento de la empresa, sin embargo, como para cualquier compañía, los ingresos podrían verse afectados por múltiples factores, como mala gestión o condiciones inesperadas del mercado o de la naturaleza.

Usando este método y estos indicadores de valuación, pude lograr en el año 2021 un crecimiento de mi portafolio del 19%.

Mi aprendizaje además de continuo ha estado alineado a los requerimientos del rol que desempeñaba o alineado a los requerimientos de la siguiente posición a la que deseaba crecer. Recordemos que la suerte no existe, y aquello a los que algunos llaman suerte no es otra cosa que la intersección de preparación y oportunidad. Es así como debemos planear nuestra capacitación de manera anticipada para poder aprovechar una nueva oportunidad de crecimiento profesional.

4. CONDUCTA ÉTICA

Las decisiones que tomamos durante nuestras vidas, tanto en lo personal como en lo profesional van a definir el tipo de profesionales que seremos en el futuro y van a influenciar a las personas y profesionales a nuestro alrededor.

Proceder éticamente siempre va a constituir uno de los retos más grandes de nuestras vidas, ya sea porque el declinar la ganancia personal puede algunas veces representar un desafío o porque la presión laboral de obtener resultados en tiempos más cortos podría exponer nuestra capacidad laboral como no idónea. Sin embargo, recordemos que nos debemos a nosotros mismos el estar orgullosos y satisfechos con nuestra manera de actuar. Adicionalmente, contamos con nuestros supervisores y el departamento de recursos humanos, que nos invitan a reportar cualquier potencial falta ética y a presentar cualquier consulta al respecto.

4.1 Responsabilidad

Como ingeniero de sistemas y líder en el campo de seguridad de la información siempre busco maneras de apoyar a los nuevos profesionales y hacerles coaching para que puedan madurar sus habilidades de manera responsable y ética. Los valores profesionales que transmitamos a la gente que tengamos a nuestro cargo o a nuestros colaboradores van a influenciar su conducta y ética futura.

Como líder de seguridad informática, me es importante distribuir la carga laboral de la manera más eficiente, pero al mismo tiempo, lo más equitativamente posible. Tenemos que atender los requerimientos de nuestros usuarios y proveer los entregables en el plazo comprometido. Al mismo tiempo he tenido que velar por el bienestar del equipo, ya que mucha carga laboral para un miembro eficiente y muy poca carga laboral para un miembro más junior podría mal entenderse como favoritismo, también podría limitar las capacidades de desarrollo del nuevo miembro del equipo, y más aún podría resultar en su desmotivación.

La manera en la que personalmente distribuyo la carga laboral es permitir que cada miembro escoja las asignaciones de su preferencia siguiendo los lineamientos de distribución esperados, en otras palabras, es mi expectativa que cada miembro del equipo se autoasigne la carga que le corresponde.

Como he podido mencionar anteriormente, las compañías norteamericanas se caracterizan por su diversidad de recursos humanos. El mensaje es recurrente y muy claro, no discriminar por razones de sexo, raza, credo, o preferencias de identificación de género. Esta filosofía permite

aceptar a cualquier colaborador de manera abierta y permite la generación prolifera de ideas. En lo profesional, siempre evalúo a cada profesional por sus conocimientos, energía, iniciativa y contribución al equipo. De la misma manera, siempre he tratado de que mi conducta hacia proveedores de software o servicios sea justa, evaluando como la solución que ofrecen cumple con los requerimientos de negocios, funcionales y técnicos, así como su tiempo en el mercado y los casos de éxito que hayan tenido. La comunicación y manejo de stakeholders la baso en la criticalidad y priorización de objetivos de negocio.

Como líder de equipo, he aprendido los beneficios de dar crédito por el trabajo realizado, después de todo, como líder estoy para servir a mi equipo. Apoyándolo para desarrollar las capacidades que los harán exitosos en los proyectos y en sus carreras. La experiencia me ha demostrado que, al reconocer el esfuerzo y éxito del equipo, este se siente motivado y empoderado para continuar con energía. Al mismo tiempo, el sentimiento de apreciación fortalece el vínculo de confianza.

Referente a los sistemas y soluciones, la confidencialidad es uno de los pilares más importantes de mi rol. Es mi deber diseñar sistemas que solo capturen la información indispensable para el propósito que han sido creados. Por ejemplo, si el número de pasaporte no es necesario para el caso de uso o el sistema, este no debe capturarse. Más aún, si no es necesario, debe ser excluido del diseño. Muchas veces sucede que, es más fácil capturar todos los campos de una tabla que excluir algunos de un query, o es más fácil transmitir información que incluye un campo con data confidencial que consultar si es necesario excluirlo, y se termina incluyendo más datos confidenciales de los necesarios. Velar por la privacidad requiere de cuidado y dedicación, así como de pasos adicionales para aclarar el caso de uso, pero es necesario garantizar la confidencialidad de nuestros usuarios y clientes. Aunado a esto van las consideraciones de control de acceso a los sistemas y bases de datos, solo aquellas personas autorizadas deben ser provistos de las credenciales necesarias. Un modelo de Role Based Access Control (RBAC), limita el acceso de los usuarios y procesos programáticos haciendo uso de roles en la aplicación, permitiendo otorgar únicamente el acceso mínimo imprescindible a los sistemas de información basado en necesidades de negocio específicas.

4.2 Liderazgo

Como líder de equipo, debo velar por que cada miembro se sienta dueño de las obligaciones y asignaciones que les corresponde. Para esto trato de liderar con un buen ejemplo de conducta profesional, presentando mis entregables a tiempo y con la calidad esperada. Aunque

en la actualidad los equipos han adoptado un sistema más flexible y autónomo de trabajo, es importante para mí y mi equipo ser conscientes que la expectativa es trabajar las ocho horas diarias y atender honestamente a nuestros clientes internos y externos.

Aunque mayormente he participado en proyectos que son de mi dominio, alguna vez hubo un proyecto que requirió de una mayor profundidad en área de IAM, en esa oportunidad tuve que integrar una solución con diferentes proveedores de sistemas de identidad y acceso, en esa ocasión solicité el apoyo de un experto dedicado solo a IAM para evitar cualquier error u omisión en el diseño y al mismo tiempo evitar después rediseño y consumo de tiempo innecesario. Decir "necesito ayuda" no nos convierte en profesionales de menor valor, en realidad ningún buen líder espera que alguien sepa de todo (es imposible), y al pedir ayuda, se sienta el ejemplo para que otros también se puedan sincerar en beneficio de la colaboración.

El desarrollo de sistemas de información tiene que cumplir con regulaciones y estándares de la industria. Los procesos de estos sistemas deben cumplir, por ejemplo, con las regulaciones de PCI-DSS si el sistema procesa, transmite o guarda información de tarjetas de crédito, típico escenario al pagar con tarjeta de crédito. Una regulación como PCI tiene 12 requerimientos, entre ellos describe que identificadores de la tarjeta de crédito se pueden guardar y cuáles no deben guardarse bajo ningún motivo, también proporciona requerimientos de seguridad en los endpoints donde está instalada la solución, requerimientos de monitoreo, y reglas de administración de firewalls. Otra regulación es Global Data Protection Regulation (GDPR) y la deben cumplir las compañías con presencia en la Unión Europea, bajo esta regulación las aplicaciones deben proveer la capacidad técnica de exportar la información personal del cliente o eliminar dicha información a solicitud del cliente.

Así mismo, como parte de las iniciativas de seguridad informática, existe el requerimiento de actualizar o retirar los sistemas que estén fuera de soporte del fabricante, como versiones obsoletas de CentOS, Windows, o Linux. Para esto creamos un comunicado detallado y establecimos un plan que reiteraba el mensaje repetidas veces, previo al retiro automático de los sistemas con la finalidad de evitar un impacto negativo en los niveles de servicio al usuario interno y externo.

4.3 Cumplimento de Código

Cada organización, ya sea mediante el departamento de recursos humanos o el departamento de ética, cuenta generalmente con al menos dos medios de comunicación para reportar eventos que se desvíen de los estándares de ética y para consultar sobre los lineamientos éticos. Uno de los

medios es un buzón de correo electrónico; el segundo medio suele ser un número de teléfono, ambos dedicados a denuncias y consultas éticas. Cuando un empleado necesita discutir un tema de ética, este puede recurrir inicialmente a su supervisor, alternativamente puede recurrir al email o llamar por teléfono.

Para fortalecer y promover la buena conducta ética, existe la política de no-represalias, esto es, cuando un empleado reporta una preocupación ética, el supervisor no puede tomar represalias en contra del empleado. Represalias contra el empleado, podrían fácilmente conllevar a que el supervisor sea separado permanentemente de la organización.

Ya es muy conocido el lema, “si ves algo, di algo”, como método de dar confianza a los empleados para expresar cualquier preocupación referente a conducta ética profesional.

Las políticas de ética y los canales para comunicar preocupaciones al respecto son ampliamente soportados por el departamento de recursos humanos, el liderazgo ejecutivo, y el sistema legal del estado.

5. LECCIONES APRENDIDAS

La experiencia laboral, la familia y amistades son fuentes valiosas de lecciones. Como profesional he aprendido de mis propias experiencias y a través de las experiencias de los demás. Manteniendo la mente abierta y estando dispuesto a recibir críticas constructivas me ha ayudado a mejorar.

Inicialmente desarrollé mis habilidades técnicas y establecí relaciones de confianza y colaboración con aquellos que tenían habilidades mayores que las mías en algún área técnica. Aprendí a preguntar sin temor y a poner en práctica lo aprendido. Con el tiempo pase a ser nivel tres de consultoría, es decir, a quien recurrían cuando había alguna pregunta que los dos primeros niveles de ingenieros no podían responder. Aprendí que el transferir conocimiento fortalece los lazos de confianza con los compañeros y mejora la imagen profesional.

Posteriormente desarrollé mis habilidades de gestión de proyectos para poder distribuir la carga laboral y disminuir el backlog. Aprendí que el solicitar feedback continuo ayuda a afinar los procesos y a obtener los resultados esperados.

Luego aprendí a elaborar hojas de ruta y establecer estrategias de portafolio. Al mismo tiempo estuve desarrollando mis habilidades blandas. Aprendí que el expresar ideas de manera pausada y clara, ayuda a proyectar una imagen de profesional senior, alguien a quien se debe escuchar cuando comparte una opinión.

El aprender a gestionar mi tiempo me permitió ser más efectivo conmigo mismo, y el aprender a gestionar el equipo me ayudó a aprender métodos de resolución de conflictos.

En mi rol actual me tengo que comunicar a nivel de VP, y continuar desarrollando mis habilidades de comunicación es de vital importancia. Al respecto, me queda por mejorar el acento y la pronunciación fina del inglés. Por ejemplo, para mí no es fácil identificar y reproducir las cinco maneras diferentes de pronunciar la “a” en inglés. Existen lugares para mejorar la oratoria como Toast Masters y lugares para suavizar el acento a los que planeo asistir en el corto plazo.

Comparto a continuación algunas lecciones aprendidas en las buenas y malas experiencias, todas ellas enfocadas desde un punto de vista positivo. Y comparto mis recomendaciones tanto para los recién egresados como para los profesionales de amplia trayectoria que aspiran a seguir escalando:

- Definir y decidir a dónde queremos llegar lo antes posible. Solo de esa manera podremos plantearnos los hitos importantes de progreso para los próximos diez años.

- Planifique a detalle en el corto plazo, por ejemplo, ¿que necesito para dar el siguiente salto profesional? Y proceda a complementar el conocimiento que le falta y generar las relaciones que necesita para llegar a ese siguiente objetivo.
- Ser consciente de mis áreas débiles y rodearme de gente que tenga fortalezas en esas áreas me ha ayudado a mejorar. Rodéese de gente positiva y con iniciativa.
- Aléjese de aquellos que no cumplen sus responsabilidades o que siempre están criticando. El mal ejemplo también es contagioso y he presenciado como una "buena manzana" se ha visto negativamente influenciada por una "manzana podrida". Lo más triste, aquel que fue negativamente influenciado fue separado de la compañía y el originador (manzana podrida) continuó en la organización.
- Tener confianza de decir, "necesito ayuda", "explícame", "No". Múltiples veces me he percatado durante la presentación de alguna tecnología, que se hace uso de algún concepto que desconozco. Inicialmente pensé que era el único sin saber el significado y al terminar la presentación pregunté a mis colaboradores cuál era el significado, a lo que ninguno me pudo responder. Entendí que la mayoría de las personas tiene temor de preguntar, y que los demás piensen que no son tan buenos profesionales. La realidad es que si usted tiene buen nivel en lo que hace y no entendió algo, lo más probable es que nadie más lo haya entendido tampoco. Hoy, soy el primero en levantar la mano y preguntar en público, luego los demás se sienten en confianza y también preguntan, enriqueciendo la experiencia y conocimiento para todos los participantes.
- Si su buen desempeño técnico lo llevó a un nivel de jefatura. No espere que aquellos que le reportan tengan el mismo desempeño. Ayúdelos a mejorar y no los micro gestione.
- Si ya está liderando equipos, aprenda a delegar y empiece a desarrollar sus habilidades blandas.
- Aprender a reconocer diferentes tipos de personalidades me ha ayudado a establecer mejores relaciones de colaboración en todos los niveles y a obtener mejores resultados.
- Nunca envíe un email o responda cuando está en un estado alterado o iracundo. Con seguridad lamentará su respuesta y es imposible desdecir lo dicho.
- Piense en cómo quiere vivir cuando se retire, aunque tenga 25 años, planee sus objetivos para el futuro y ejecute su plan de acción paso a paso. Deténgase a revisar de tiempo en tiempo cómo va el progreso en su propio plan de vida.

- Busque un balance en su vida. Darle tiempo a su trabajo, familia y desarrollo personal le ayudarán a mantener su salud mental y física a largo plazo.
- Lea libros que lo ayuden a mejorar o escuche la versión en audiobook. Los audiobook son de mi preferencia personal. A continuación, recomiendo tres libros que lo sorprenderán si los pone en práctica.
    - Cómo hacer amigos e influir sobre las personas. Dale Carnegie
    - Power. Jeffrey Pfeffer
    - Padre rico, padre pobre. Robert T. Kiyosaki

Nuestra vida profesional empieza al graduarnos y nuestro aprendizaje nunca termina. La Universidad de Lima nos proporciona las herramientas necesarias para poder desempeñarnos en el futuro y poder construir por nosotros mismos. No se desanime con los tropiezos, son ellos los que le ayudarán más en su vida. El éxito depende de nosotros, de que estemos preparados y siempre planificando para obtener los resultados que deseamos alcanzar.

6. GLOSARIO DE TÉRMINOS

- Activo de TI: Es hardware, sistemas de software o información que tienen valor para una organización (Atlassian, 2022).
- BlackHat: La Conferencia Black Hat es un evento de seguridad informática que reúne a profesionales y expertos de todo el mundo. Blackhat también se refiere al actor que ejecuta actos maliciosos en el ámbito de seguridad informática.
- Ciberseguridad: Es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio (Cisco Security, 2024).
- CCISO: Certified CISO es una certificación de alto nivel que se enfoca tanto en conocimiento técnico como en la aplicación de principios de seguridad desde una perspectiva ejecutiva.
- Cloud: Se refiere a los servidores a los que se accede a través de Internet y al software y las bases de datos que se ejecutan en esos servidores (Cloudflare Inc., 2024).
- Coaching: Apoyo que brinda una persona en el desarrollo de otra.
- EC-Council: Es la entidad más grande a nivel mundial en certificaciones de seguridad (EC-Council, 2024).
- Firewall: Un equipo de cortafuegos (Firewall) convierte las diferentes redes a las que se conecta en independientes. Al contrario que un router, no se conforma con transmitir la petición. Un cortafuegos segmenta los flujos asumiendo él mismo las peticiones. Para esto establece dos conexiones y puede realizar una acción de autentificación. (Dordoigne, 2005).
- GIAC: Global Information Assurance Certification es una organización de certificación en seguridad de la información (GIAC Certifications, 2024).
- Habilidades blandas: Se entienden como el resultado de una combinación de habilidades sociales, de comunicación, de forma de ser, de acercamiento a los demás, entre otras, que hacen a una persona dada a relacionarse y comunicarse de manera efectiva con otros (Chaca & Contreras, 2022).

- IAM: Conjunto de tecnologías y políticas que garantiza que los usuarios tengan el acceso adecuado a los recursos de la organización
- ISC2: International Information Systems Security Certification Consortium. Es una organización que se dedica a la certificación y promoción de la seguridad de la información (ISC2, s.f.).
- ITIL: Del inglés, Information Technology Infrastructure Library, es una guía de buenas prácticas para la gestión de servicios de tecnologías de la información (ServiceNow, 2024).
- PCI-DSS: El estándar de seguridad de datos para la industria de tarjetas de pago es un compendio de normas de seguridad para proteger la información de las tarjetas de pago durante la transmisión, procesamiento o almacenamiento de dicha información.
- PCIP: Profesional de la industria de tarjetas de pago. Es un certificado que se otorga al profesional con conocimiento en seguridad de tarjetas de crédito y débito (PCI Security Standadrs Council, 2022).
- PMP: Acrónimo de Project Manager Profesional, que es la certificación en proyectos que brinda el Project Manager Institute (PMI, 2024).
- Recursos humanos: Se refiere al conjunto de trabajadores en una organización, un determinado sector, así como una economía en su conjunto. Cualquier persona física que posea una vinculación a una organización, sector o economía, se considera un recurso humano. A su vez, dentro de la administración de empresas, el concepto hace referencia a la gestión que la empresa realiza con sus trabajadores (Chiavenato, 2000).
- Retail: Venta al por menor de bienes al consumidor, a través de tiendas y en línea.
- SANS: Es una organización internacional especializada en capacitación y certificaciones en seguridad de la información (SANS, 2024).
- Stakeholders: Se le conoce como stakeholders, grupos de interesados o interesados a aquellos actores que tienen algún tipo de relación con una empresa; de manera que cualquiera de las decisiones estratégicas de la compañía puede afectarles de forma directa o indirecta. Algunos ejemplos más comunes de stakeholders son: los empleados, los accionistas, los clientes, los proveedores, los gobiernos y las comunidades (Eskerod, 2020).

- Threat Modeling: Modelamiento de Amenazas. Es el proceso en el que se identifican y evalúan las amenazas potenciales para un sistema, aplicación o infraestructura. Durante el modelado de amenazas, se analizan los activos, los riesgos, los adversarios y las capacidades de estos últimos.
- TLS: Seguridad en la capa de transporte, es un protocolo criptográfico que se emplea para proteger los datos que viajan a través del canal de comunicación entre el servidor y cliente.
- WACC: Weighted Average Cost of Capital, o costo promedio ponderado del capital. Es fundamental para la valoración de proyectos y empresas. Es lo que la empresa debe pagar por su capital, tanto de deuda como capital propio (CFI Team, 2015).

REFERENCIAS

Atlassian. (2022). *¿Qué es la gestión de activos de TI?* Una guía. https://www.atlassian.com/es/itsm/it-asset-management

Eskerod, P. (2020). A stakeholder perspective: Origins and core concepts. In Oxford Research Encyclopedia of Business and Management. Oxford University Press. https://doi.org/10.1093/acrefore/9780190224851.013.3

Botwright, R. (2024). *OWASP top 10 vulnerabilities: Beginner's guide to web application security risks*. Pastor Publishing.

CFI Team. (2015). *WACC. Corporate Finance Institute*. https://corporatefinanceinstitute.com/resources/valuation/what-is-wacc-formula/

Chiavenato, I. (2000). *Administración de recursos humanos* (5.a ed.). McGraw-Hill Companies.

Cisco Security. (2024, March 12). *What is Cybersecurity? Cybersecurity*. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

Cloudflare, Inc. (2024). *¿Qué es la nube? | Definición de nube*. Cloudflare.com. https://www.cloudflare.com/es-la/learning/cloud/what-is-the-cloud/

Cyber Resilience Presentation. (2019). BSIGROUP. https://www.bsigroup.com/globalassets/localfiles/en-ie/csir/resources/exchange/bitsight---bsi-cyber-resilience-presentation.pdf

Computer Security Resource Center. (2020). *NIST SP 800-53 Rev. 5*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Contreras, A., & Chaca, L. (2022). *Habilidades blandas y desempeño laboral de los trabajadores administrativos en el trabajo remoto* [Tesis de Maestría, Universidad Continental]. Repositorio Institucional de la Universidad Continental. https://repositorio.continental.edu.pe/bitstream/20.500.12394/10572/1/IV_PG_MRHGO_TE_Chaca_Contreras_2022.pdf

Dordoigne, J. (2005). *Networking Essentials*. Laxmi Publications.

GIAC Certifications. (2024). *Acerca de*. https://www.giac.org/about/company-info/.

Hancock, S. (2024). *PCI DSS version 4.0: A guide to the payment card industry data security standard*. Itgp.

Hornford, D., Hornford, N., Lambert, M. & Street, K. (2022). *An introduction to the TOGAF® standard, 10th edition*. The Open Group. https://pubs.opengroup.org/architecture/w212/

ISC2. (s.f.). *Isc2*. https://www.isc2.org

Morgan, S. (2023). Cybercrime to cost the world $9.5 trillion USD annually in 2024. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/nist.cswp.29

PCI Security Standards Council. (2022, 25 de Marzo). *PCI professional (PCIP) qualification*. https://www.pcisecuritystandards.org/program_training_and_qualification/pci_professional_qualification/

PMI. (2024). *Project Management Professional (PMP)®.* https://www.pmi.org/certifications/project-management-pmp

SANS. (2024). *About SANS Institute*. https://www.sans.org/about

ServiceNow. (2024). *What is ITIL (IT Infrastructure Library)?* https://www.servicenow.com/products/itsm/what-is-itil.html

The Insights Group. (2021). *Validating Insights Discovery*. Insights. https://www.insights.com/media/2728/insights-discovery-validating-the-system-factsheet.pdf

Rapid7. (s.f.). *Working with vulnerabilities*. https://docs.rapid7.com/nexpose/working-with-vulnerabilities

BIBLIOGRAFÍA

ACM Code of Ethics and Professional Conduct. (s.f.). https://www.acm.org/about-acm/code-of-ethics-in-spanish

Géron, A., & O'Reilly Media. (2018). *Hands-on machine learning with Scikit-Learn and TensorFlow: Concepts, tools, and techniques to build intelligent systems*. O'Reilly.

Hastie, T., Tibshirani, R., & Friedman, J. H. (2010). *The elements of statistical learning: Data mining, inference, and prediction.* Springer.

Han, J. (2012). *Data mining: concepts and techniques*. Morgan Kaufmann.

Kuhn, M., & Johnson, K. (2013). *Applied predictive modeling.*

Jordan, B., Westerfield, R., & Ross, S. (2018). *Fundamentals of Corporate Finance* (12.a ed.). McGraw Hill.

Brigham, E., Houston, J. (2018). *Fundamentals of Financial Management* (15.a ed.). Cengage Learning.

Brigham, Eugene F. (2018). *Finanzas Corporativas: Enfoque central*. Cengage Learning.

Gitman, Lawrence J. (2016). *Principios de Administración Financiera* (14.a ed.). Pearson.

Van Horne, James, J. (2010). *Fundamentos de Administración Financiera* (13.a ed.). Pearson.

4% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado

Exclusiones

- N.º de coincidencias excluidas

Fuentes principales

3%	Fuentes de Internet
0%	Publicaciones
4%	Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Texto oculto
0 caracteres sospechosos en N.º de página
El texto es alterado para mezclarse con el fondo blanco del documento.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.