



**Universidad
Europea**

ESCUELA DE ARQUITECTURA, INGENIERÍA Y DISEÑO

ÁREA INGENIERÍA INDUSTRIAL

**MÁSTER UNIVERSITARIO EN INGENIERÍA DE
ORGANIZACIÓN, DIRECCIÓN DE PROYECTOS Y EMPRESAS**

TRABAJO FIN DE MÁSTER

**REDUCCIÓN DEL RIEGO CIBERNÉTICO EXISTENTE EN UN
PROCESO DE DESVINCULACIÓN LABORAL**

ALUMNO: LAURY FERNANDA OSORIO PAGOAGA

DIRECTOR: JOSEP LLEDÓ

JULIO 2023

AUTOR: LAURY FERNANDA OSORIO PAGOAGA

RESUMEN.

A lo largo de este trabajo de fin de máster se llevará a cabo un análisis exhaustivo del proceso de desvinculación laboral en la empresa hondureña TECNO SOLUTIONS, especializada en el desarrollo e implementación de soluciones tecnológicas. El objetivo principal será identificar posibles brechas de seguridad existentes en el proceso, así como evaluar su impacto y riesgo en términos de seguridad y privacidad cibernética. Estas brechas podrían incluir accesos no autorizados, robo de datos y violaciones de la propiedad intelectual de la empresa, lo que conllevaría una pérdida significativa de información crítica, daños a la reputación y costos financieros.

Para lograrlo, se utilizará la metodología DMAIC Lean Six Sigma, con el fin de mejorar el proceso, aumentando su eficiencia y reduciendo los riesgos cibernéticos asociados. De esta manera, se pretende fortalecer la seguridad de la empresa y evitar posibles vulnerabilidades que podrían afectar negativamente su posición competitiva en el mercado.

Palabras clave: Ciberseguridad, Ataque cibernético, vulnerabilidades de seguridad, talento humano, desvinculación.

ABSTRACT.

Throughout this master's thesis, a comprehensive analysis of the employee disengagement process will be conducted in the Honduran company TECNO SOLUTIONS, specialized in the development and implementation of technological solutions. The main objective will be to identify possible security gaps in the process and assess their impact and risk in terms of cybersecurity and privacy. These gaps may include unauthorized access, data theft, and violations of the company's intellectual property, leading to a significant loss of critical information, reputation damage, and financial costs.

To achieve this, the DMAIC Lean Six Sigma methodology will be employed to improve the process, enhance its efficiency, and reduce cybersecurity risks. The aim is to strengthen the company's security measures and prevent potential vulnerabilities that could adversely affect its competitive position in the market.

Keywords: Cybersecurity, Cyber attack, Security vulnerabilities, Human resources, disengagement.

ÍNDICE

RESUMEN.....	2
ABSTRACT.	2
ÍNDICE	3
ÍNDICE DE FIGURAS.....	6
ÍNDICE DE TABLAS.....	7
CAPÍTULO 1. INTRODUCCIÓN.....	8
1.1 Planteamiento del problema	9
1.1.1. Definición del problema.....	9
1.1.2. Preguntas de Investigación	9
1.2 Antecedentes.....	10
1.3 Objetivos del proyecto.....	11
1.4.1. Objetivo General.....	11
1.4.2. Objetivos Específicos	12
CAPÍTULO 2. INTRODUCCION AL SECTOR	13
2.1 Ciberseguridad.....	13
2.2 ¿Quién está detrás de los ciberataques?.....	14
2.3 ¿Por qué las amenazas internas son particularmente peligrosas?.....	15
2.4 Tipos de amenazas internas.....	16
2.5 ¿Cuál es la frecuencia con la que ocurren los ciberataques?	17
2.6 ¿Cuál es la razón por la cual las personas realizan ciberataques?	18
2.7 Cómo los estafadores utilizan información privilegiada vulnerable.....	18
2.1 ¿A qué se dirigen los atacantes cibernéticos?	19
2.2 ¿Cuáles son los tipos habituales de ciberataques?	20
2.3 ¿Qué pueden hacer los ciberataques?	22
2.4 Data los prevention.....	22
2.5 Desvinculación laboral	23
2.6 Tipos de desvinculación laboral en Honduras	24
2.7 Lean Six Sigma.....	25
CAPÍTULO 3. ANALISIS DE RIESGO CIBERNETICO ASOCIADOS AL PROCESO DE DESVINCULACIÓN	

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL
LAURY FERNANDA OSORIO PAGAOGA

LABORAL	28
3.1 Proceso actual de Despido laboral	29
3.2 Proceso actual de renuncia laboral.....	30
3.3 Etapas del proceso de desvinculación laboral a analizar y mejorar.	31
3.3.1 Riesgo cibernético previo a la desvinculación laboral.	31
3.3.2 Riesgo cibernético asociado al proceso de baja de accesos lógicos y físicos.	32
CAPÍTULO 4. REDUCCIÓN DE RIESGOS CIBERNETICOS EN PROCESO DE DESVINCULACIÓN LABORAL	33
4.1 Análisis y disminución del riesgo cibernético previo a la desvinculación laboral.....	33
4.2 análisis y mejora del subproceso de baja de accesos mediante metodología DMAIC.....	36
4.2.1 DEFINE.....	36
4.2.1 Problem Statement.....	36
4.2.2 Goal Statement	37
4.2.3 Project Charter.....	37
4.2.4 SIPOC.....	38
4.2.5 Process Map.....	39
4.2.6 Critical to Quality	40
4.3 MEASURE	41
4.3.1 KPI's (Key Performance Indicators.....	41
4.3.2 Data Collection.....	42
4.3.3 Medidas Lean.....	42
4.3.4 Matriz de Causa y Efecto (Fishbone Diagram).....	44
4.4 ANALIZE.....	45
4.4.1 Lead Time.....	45
4.4.2 Wait Time.....	45
4.4.3 Processing Time	47
4.4.4 Diagrama de Pareto	48
4.4 IMPROVE.....	50
4.5 CONTROL.....	54
4.5.1 Incidentes de seguridad.....	54
4.5.2 Tasa de bloqueo de accesos. (como se puede medir este KPI)	54
4.5.3 Tiempo promedio de eliminación de accesos	55
4.5.4 Tasa de eliminación de accesos completados	55

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL
LAURY FERNANDA OSORIO PAGAOGA

4.5.5 Tasa de auditorías regulatorias pasadas satisfactoriamente,.....	56
4.5.6 Porcentaje de accesos documentados y registrados correctamente.....	56
4.5.7 Porcentaje de satisfacción interna	56
4.5.8 Nivel de conocimiento sobre seguridad informática.....	57
CAPÍTULO 5. IMPLANTACIÓN	58
CAPÍTULO 6. PLAN FINANCIERO	64
6.1 Valoración del riesgo financiero sin herramientas y conocimiento de protección de seguridad informática.....	64
6.2 Inversión Inicial para la implementación de mejoras para reducción de riesgo cibernético en el proceso de desvinculación laboral.....	68
6.3 Impacto financiero por riesgo cibernético VS inversión en herramientas para reducir el riesgo cibernético	70
6.3.1 Impacto financiero por un riesgo cibernético	70
6.3.2 Inversión para prevenir el riesgo cibernético	70
CAPÍTULO 7. LEGAL	71
7.1 La Protección de Datos en Honduras.....	71
CAPÍTULO 8. CONCLUSIONES Y FUTURAS LINEAS DE TRABAJO.....	75
8.1 Conclusiones:	75
8.2 Futuras Lineas:.....	76
CAPÍTULO 9. ANEXOS	77
Anexo 1 – Correo electrónico para solicitar baja de accesos.	77
Anexo 2 - Proceso actual de despido parte 1.	78
Anexo 3 - Proceso actual de despido parte 2	79
Anexo 4- Proceso actual de renuncia parte 1.....	80
Anexo 5 -Proceso actual de renuncia parte 2.....	81
Anexo 6 -Propuesta de nuevo proceso de renuncia parte 1	82
Anexo 7 -Propuesta de nuevo proceso de renuncia parte 2	83
Anexo 8 -Propuesta de nuevo proceso de despido parte 1	84
Anexo 9 -Propuesta de nuevo proceso de despido parte 2	85
Anexo 10 -Propuesta de nuevo proceso de baja de accesos.....	86
CAPÍTULO 9. BIBLIOGRAFIA.....	87



ÍNDICE DE FIGURAS

Ilustración 1 - Proceso actual de despido	29
Ilustración 2 - Proceso actual de renuncia laboral.....	30
Ilustración 3- Project Charter	37
Ilustración 4 - SIPOC.....	38
Ilustración 5 - Process Map	39
Ilustración 6- Critical To Quality	40
Ilustración 7 - KPI Key Performance Indicators.....	41
Ilustración 8 - Matriz de Causa y Efecto.....	44
Ilustración 9 - Lead Time	45
Ilustración 10 - Diagrama pastel Lead Time.....	45
Ilustración 11 - Wait Time	46
Ilustración 12 - Processing Time	47
Ilustración 13 - Cycle Time	47
Ilustración 14 - Diagrama de Pareto	48
Ilustración 15 - Proceso actual de desvinculación laboral, por despido.....	58
Ilustración 16 - Proceso actual de desvinculación labora, por renuncia	58
Ilustración 17 - Propuesta de proceso de desvinculación laboral por despido	59
Ilustración 18 - Propuesta de proceso de desvinculación laboral, por renuncia.....	60
Ilustración 19 - Proceso actual de baja de accesos.....	61
Ilustración 20 - Propuesta de proceso de baja de accesos	62

ÍNDICE DE TABLAS

Tabla 1 - Medidas Lean	43
Tabla 2 - Riesgo financiero de un Puesto estratégico.....	65
Tabla 3 - Riesgo financiero de un Puesto Comercial.....	66
Tabla 4 - Riesgo financiero de un puesto de HFC Support, 1st line.	67
Tabla 5 - Riesgo financiero de un puesto de Ingeniero de red core.....	68
Tabla 6 - Inversión - Generación de accesos a herramienta de tickets	69
Tabla 7 - Inversión en plataforma Knowbe4.....	69
Tabla 8 - Inversión en Forcepoint DLP	69
Tabla 9 - Impacto financiero por un posible riesgo cibernético asociado a un puesto laboral	70
Tabla 10 - Inversión para reducción del riesgo cibernético	70

CAPÍTULO 1. INTRODUCCIÓN

En el presente documento se analizarán los riesgos cibernéticos asociados al proceso de desvinculación laboral de la empresa hondureña TECNO SOLUTIONS especializada en el desarrollo e implementación de soluciones tecnológicas. Se identificarán las debilidades que este tiene y el impacto que podría ocasionar en la empresa. Con el objetivo de tomar acciones y realizar las mejoras pertinentes para reducir los riesgos en términos de seguridad y privacidad de los sistemas de información, así como también garantizar la confidencialidad, integridad y disponibilidad continuada de la información.

Actualmente es un proceso que en las empresas no se le brinda la relevancia e importancia que requiere. Pasa desapercibido el gran impacto que podría ocasionar si no es gestionado de manera correcta y oportuna. Las cuentas pueden ser comprometidas, lo que aumenta considerablemente las vulnerabilidades de seguridad.

Si este proceso no es realizado de una manera correcta, es decir, los accesos no se eliminan oportunamente, el ex empleado aún podría tener acceso no autorizado a información confidencial de la empresa, como datos de clientes, estrategias comerciales y datos secretos de la compañía, lo cual puede tener un impacto negativo en la posición competitiva de la empresa.

Por lo tanto, se requiere una correcta gestión del proceso de desvinculación de empleados para evitar grandes consecuencias en términos de seguridad y privacidad cibernética, así como en la propiedad intelectual de la empresa. Es importante que las empresas tengan políticas y procedimientos simplificados y claros para la gestión de la desvinculación de empleados, incluyendo la eliminación adecuada de sus credenciales de acceso y la protección de la información confidencial de la empresa.

1.1 Planteamiento del problema

1.1.1. Definición del problema

El siguiente proyecto tiene como objetivo abordar la problemática existente en la empresa hondureña TECNO SOLUTIONS, especializada en el desarrollo e implementación de soluciones tecnológicas, que actualmente se encuentra vulnerable a riesgos cibernéticos asociados con el proceso de desvinculación laboral. El proceso actual no es eficiente y presenta brechas que pueden generar vulnerabilidades, poniendo en riesgo la seguridad y privacidad de la información, así como la operación de la empresa, lo cual podría ocasionar daños a su reputación y costos financieros.

1.1.2. Preguntas de Investigación

1. ¿Cuáles son los principales riesgos cibernéticos asociados al proceso de desvinculación de colaboradores en una empresa?
2. ¿Cómo se puede mejorar el proceso de desvinculación de empleados para reducir y mitigar las vulnerabilidades que están provocando una brecha de seguridad?
3. ¿Qué medidas o protocolos de seguridad se pueden implementar para disminuir los riesgos cibernéticos durante y posterior al proceso de desvinculación de empleados, para que no puedan tener acceso no autorizado a datos de la empresa?
4. ¿Cuáles son las consecuencias financieras y de reputación de posibles vulnerabilidades de seguridad en un proceso de desvinculación de empleados?
5. ¿Qué mecanismos educativos o tecnológicos se pueden utilizar para proteger la información de la empresa durante el proceso de desvinculación de los colaboradores?

1.2 Antecedentes

Actualmente, las empresas dan mucha prioridad al proceso de onboarding, es decir al proceso a través del cuales los colaboradores se suben a bordo del barco de la empresa, con el objetivo de mostrarles y hacerles parte de la tripulación, estimularles el sentido de pertenencia y orientarlos a cumplir un objetivo en común.

En la mayoría de las empresas, este proceso está bien claro y estructurado, se preocupan por brindarle al colaborador todos los recursos necesarios para desempeñar su trabajo de manera efectiva, proporcionarle la información necesaria, lectura de los manuales de la compañía, estación de trabajo, herramientas tecnológicas, accesos físicos y lógicos, kit de bienvenida, en fin, brindarle la mejor bienvenida posible.

Esto no ocurre cuando se trata de un proceso tan crítico como lo es el offboarding, es decir a las acciones que se deben tomar cuando hay una desvinculación laboral, ya sea cuando el colaborador deja la empresa voluntaria o involuntariamente. En muchas empresas este proceso no se le da la importancia que requiere, por lo tanto, no está claramente definido, esto debido a que su enfoque está en el reclutamiento, por la falta de comprensión de la importancia que requiere, no existe una gestión adecuada, falta de seguimiento, entre otras causas. Pasa desapercibido, que la falta de atención este proceso puede tener consecuencias graves para la empresa, como afectación a la moral del colaborador; problemas legales, pérdida o fuga de información; datos sensibles y conocimientos; ataques cibernéticos para violar la seguridad de los sistemas de la empresa. Todo esto puede ocasionar costos financieros, daños de reputación, o incluso paro de operaciones.

Según (paloaltonetworks, 2022) las amenazas internas representaron un alto porcentaje de los incidentes manejados por Unit 42, "son significativos porque involucran a un actor malintencionado que sabe exactamente dónde buscar para encontrar datos sensibles", según el informe. El 75% de los casos de amenazas internas involucraron a un ex empleado descontento que se llevó datos de la empresa, destruyó datos de la empresa o accedió a las redes de la empresa después

de su partida, lo que claramente demuestra que el enemigo está más cerca de lo que se cree.

Justamente, comprender la importancia e impacto que tiene un riesgo cibernético en un proceso de offboarding es lo que ha generado mi interés de analizar dicho proceso, evaluar el impacto para la empresa e implementar las mejoras correspondientes. Para lo cual, se ha seleccionado el proceso de desvinculación laboral de la empresa hondureña TECNO SOLUTIONS, en el cual algunas de sus etapas no están siendo efectivas, permitiendo que en algunas de ellas se de apertura para fuga o robo de información, a causa de una incorrecta gestión previa, falta de seguimiento y control en la eliminación de permisos y accesos, no existen acuerdos de confidencialidad, falta de educación sobre seguridad de la información, falta de comunicación entre departamentos interesados en la baja de accesos, entre otros.

1.3 Objetivos del proyecto

1.4.1. Objetivo General

- 1 Reducir el riesgo cibernético asociados al proceso de desvinculación laboral de la empresa Tecno Solutions, mediante el análisis y mejora de este, haciendo uso de la metodología Lean Six Sigma, para maximizar la seguridad y privacidad de los sistemas de información, así como también garantizar la confidencialidad, integridad y disponibilidad continua de la información mientras se mantiene la eficiencia operativa.
- 2 Reducir el impacto financiero que podría sufrir la empresa a causa de un potencial ataque cibernético.
- 3 Mejorar la eficiencia del proceso de desvinculación de colaboradores, con esto será más fácil de manejar y se reducirán los tiempos.
- 4 Garantizar la seguridad de los datos: Asegurar que no habrá fuga o pérdida de datos, así como también garantizar que todos los accesos del empleado se han dado de baja de manera segura y que no haya un posible riesgo de violación de seguridad.

1.4.2. Objetivos Específicos

1. Reducción de riesgos cibernéticos debido a vulnerabilidades del proceso de desvinculación laboral en un 60%.
2. Reducir el tiempo del subproceso de baja de accesos del excolaborador en un 60%.
3. Mejorar la eficiencia del proceso de baja de accesos de colaboradores en un 50% en resultados obtenidos.
4. Mejorar el lead time del proceso de desvinculación laboral en un 30%
4. Garantizar que todos los accesos del empleado se eliminen de manera segura y permanente de los sistemas de información, en un plazo de 2:40 horas después de la desvinculación con el empleado.
5. Reducir los riesgos legales en el proceso de desvinculación al asegurarse de que todos los empleados hayan firmado acuerdos de confidencialidad y no competencia.
6. Garantizar que los colaboradores tienen una formación sobre seguridad informática y que la evaluación de este conocimiento sea mayor al 90%.

CAPÍTULO 2. INTRODUCCION AL SECTOR

En este capítulo se presenta una visión general de los conceptos esenciales de ciberseguridad, los riesgos cibernéticos, desvinculación laboral, y la metodología Lean Six Sigma como un enfoque sólido para gestionar y mejorar procesos.

2.1 Ciberseguridad

Según (Ibm, 2023), La práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales se conoce como ciberseguridad. Las medidas de ciberseguridad o seguridad cibernética, también conocidas como seguridad de la tecnología de la información (TI), están diseñadas para combatir las amenazas contra sistemas en red y aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización. En la era digital, la ciberseguridad ha evolucionado a pasos agigantados y se ha convertido en un tema fundamental para proteger la información de las amenazas diarias. Se ha convertido en uno de los mayores desafíos para las empresas de todo el mundo y también en uno de los mayores desafíos pendientes en la era del teletrabajo. La pandemia ha acelerado el cambio digital de las empresas y ha afectado significativamente la ciberseguridad.

Conforme a (Ibm, 2023), A nivel mundial, una brecha de seguridad de datos costó en promedio \$3.86 millones. Estos costos incluyen descubrir y responder an una brecha de seguridad, el tiempo de inactividad y la pérdida de ingresos, así como dañar la reputación y la marca de una empresa a largo plazo. También puede causar pérdida de confianza de los clientes, multas regulatorias e incluso acciones legales. Los ciberdelincuentes buscan nombres, direcciones y números de identificación nacional (PII) de los clientes. (por ejemplo, números de seguridad social en los Estados Unidos y códigos fiscales en Italia) e información de tarjeta de crédito para luego vender estos registros en mercados digitales clandestinos. La pérdida de la confianza del cliente, las multas regulatorias e

incluso las acciones legales son resultados comunes de PII comprometidos.

Además, como lo indica (Ibm, 2023), La guerra cibernética o el ciberterrorismo, como los hacktivistas, también pueden referirse a los ciberataques. En otras palabras, las razones pueden diferir. Hay tres categorías principales dentro de estas motivaciones: criminal, política y personal. Los delincuentes motivados por el crimen buscan obtener dinero robando dinero, robando datos o interrumpiendo negocios. De manera similar, aquellos que están motivados personalmente, como empleados descontentos actuales o anteriores, tomarán dinero, datos o cualquier oportunidad para interrumpir el sistema de una organización. Pero buscan principalmente compensación. Los atacantes con motivación sociopolítica buscan atención por sus motivos. Como resultado, informan a la audiencia de sus ataques, también conocidos como hacktivismo. El espionaje, obtener una ventaja injusta sobre los competidores y el desafío intelectual son otras motivaciones de los ciberataques.

2.2 ¿Quién está detrás de los ciberataques?

Comprender mejor quien está detrás de los ciberataques es de vital importancia para saber de quienes debemos protegernos, como lo indica (mundoseguros, 2018), los atacantes pueden ser:

El despedido. Los usuarios de Internet que tienen acceso a programas o aplicaciones para hackear o tienen un mínimo de conocimiento de cómo llevar a cabo un ciberataque se denominan hackers. Sobre todo, se trata de empleados despedidos injustamente que utilizan sus propios conocimientos de la empresa para llevar a cabo ciberataques o clientes que no están satisfechos con una compra o devolución que buscan "vengarse".

El despistado. Se trata de los ataques que han sido creados fuera de la empresa, pero que alguien de nuestro propio equipo los ha facilitado accidentalmente, ya sea por correo electrónico o descarga. Los trabajadores son fáciles de atacar debido a la falta de capacitación en ciberseguridad.

El hacktivista. Es un movimiento novedoso que está ganando cada vez más influencia en el mundo digital. Denunciar abusos o injusticias es su principal motivación. Aunque estos hacktivistas utilizan las mismas herramientas y técnicas que los hackers, lo hacen por razones políticas o sociales.

Por ejemplo, publicar un mensaje en la página principal de un organismo público o iniciar un ataque de denegación de servicio para detener el acceso a una página web.

El pirata informático. Los "hackers de sombrero negro" son expertos en programación. Su objetivo es usar programas como el "ransomware" para violar la seguridad de un computador o una red y, de esta manera, perjudicar al usuario, obligándolo en la mayoría de los casos a pagar para recuperar su información.

El terrorista cibernético. Los hackers suelen ser miembros de grupos organizados que tienen como objetivo generar temor en la población atacando infraestructuras tecnológicas importantes de naciones o empresas en todo el mundo. Raramente se trata de ataques organizados por una sola persona. Sus acciones están motivadas por creencias religiosas o políticas extremistas.

2.3 ¿Por qué las amenazas internas son particularmente peligrosas?

Según lo expresado por (Ibm, 2023) Los ataques cibernéticos a través del abuso de acceso pueden dañar a una empresa, a sus empleados y a sus clientes. De acuerdo con el "IBM X-Force Threat Intelligence Index 2020", las amenazas internas inadvertidas son la razón principal del aumento de más del 200 % en la cantidad de registros vulnerados en 2019 con respecto al 2018. Las personas internas generalmente saben dónde se encuentran los datos confidenciales de una organización y, a menudo, tienen altos niveles de acceso, independientemente de si tienen intenciones maliciosas o no.

Los ataques internos también son costosos para las empresas. En el estudio del costo de las amenazas internas 2020 de Ponemon Institute, los investigadores descubrieron que el costo anual promedio de la brecha de seguridad de datos internos era de USD 11.45 millones, y que el 63 % de los incidentes se atribuían a negligencia. Ya sea de forma accidental o deliberada, las personas con información privilegiada pueden exponer, o ayudar a exponer, información confidencial del cliente, propiedad intelectual y dinero.

2.4 Tipos de amenazas internas

Según (Ibm, 2023), Los empleados actuales, exempleados, contratistas o socios comerciales tienen información confidencial que podría ser un peligro. Sin embargo, cualquier persona con acceso adecuado a los sistemas informáticos y datos de una empresa, incluidos los proveedores o vendedores, puede dañarlos.

Como menciona (Partners, 2021), el estudio de Gartner clasifica la amenaza interna en cuatro categorías: el perro, el tonto, el colaborador y el lobo solitario.

El Peón: Los empleados que caen víctimas de spear-phishing o social engineering y son engañados para perder acceso a datos confidenciales se conocen como pawns. Es posible que sean objetivo de malware que se descarga inadvertidamente en una estación de trabajo. También pueden ser manipulados para revelar las credenciales de seguridad a alguien que se presenta como un operador de ayuda.

El tonto: es la amenaza interna más probable y la que mejor se protege mediante la creación de una cultura de seguridad sólida. Goofs no actúan con intención maliciosa, pero causan daños en el marco de seguridad debido a la falta de cuidado o tal vez porque no anticipan ser atacados. Debido a que creen que las medidas de seguridad no deberían aplicarse a ellos, los altos directivos suelen ser responsables de las locuras. Una seguridad inútil para la facilidad de acceso.

El colaborador: Un colaborador malicioso que planea crear una brecha de seguridad en colaboración con otros actores se conoce como colaborador, también conocido como turncloak. Los colaboradores utilizan su acceso como empleados para intencionalmente dañar la organización. Los colaboradores son contratados para realizar espionaje industrial, robo de propiedad intelectual o perturbar las operaciones diarias. También tienen la capacidad de actuar a nivel internacional, trabajando en nombre de una organización gubernamental o nación.

El lobo solitario: Los lobos solitarios actúan con intención maliciosa, pero en contraste con los colaboradores, actúan por sí mismos. Los lobos solitarios pueden ser motivados por el dinero, ya que

esperan vender información confidencial o acceso a posibles compradores futuros, o pueden actuar como una vendetta, compensación por una deuda o queja. Los lobos solitarios son los más peligrosos cuando tienen permisos de seguridad de alto nivel. Los exempleados que aún tienen acceso a los sistemas de la empresa representan un gran riesgo de seguridad si deciden actuar de manera maliciosa.

El incidente de Waymo es reconocido como uno de los peores casos de un ataque de lobo solitario a una organización importante. En 2018, un ingeniero de software que trabajaba para Google fue arrestado y acusado de robar más de 14,000 documentos confidenciales relacionados con el funcionamiento del sistema de inteligencia artificial de vehículos autónomos de Alphabet, Waymo. El ingeniero había robado estos datos y utilizó la información para crear una empresa rival llamada Otto, que posteriormente fue vendida a Uber. Como resultado de este delito, Uber tuvo que pagar un acuerdo a Alphabet y transferir la propiedad de la inteligencia artificial. El ingeniero fue condenado a pagar una multa considerable y cumplir una pena de prisión.

2.5 ¿Cuál es la frecuencia con la que ocurren los ciberataques?

Según menciona (Cisco, s.f.), cada día, las empresas son víctimas de ciberataques. "Existen dos tipos de empresas: las que han sido atacadas y las que no saben que lo han sido", dijo John Chambers, el anterior CEO de Cisco. De enero de 2016 a octubre de 2017, el número total de eventos casi se ha cuadruplicado, según el informe anual de seguridad cibernética de Cisco. Los ciberataques también pueden llevarse a cabo por razones adicionales. Algunos ciberdelincuentes utilizan el hacktivismo para eliminar datos y sistemas.

2.6 ¿Cuál es la razón por la cual las personas realizan ciberataques?

(cisco, s.f.) menciona que a medida que las personas intentan beneficiarse de los sistemas comerciales vulnerables, los ciberdelitos aumentan cada año. Los atacantes buscan con frecuencia rescates: el 53 % de los ciberataques causan daños por más de \$ 500 000.

2.7 Cómo los estafadores utilizan información privilegiada vulnerable

Como lo menciona (Ibm, 2023), el estafador se enfoca en obtener los privilegios de acceso de un empleado. Los estafadores aprovechan a los peones y los tontos para cometer sus delitos cibernéticos. Los correos electrónicos de estafa, los ataques de abrevadero y el malware son solo algunas de las muchas formas en que obtienen credenciales. Los estafadores pueden acceder a datos confidenciales o dinero con esas credenciales, moverse a través de un sistema y aumentar sus privilegios. Durante la comunicación de salida, el servidor de mando y control (C2) permite que los estafadores accedan a datos o información desde ubicaciones no seguras. Pueden transferir salida de volumen o cambiar los intentos de salida.

Los estafadores atacan así:

“Buscan vulnerabilidades

- Despliegan e-mails de phishing o malware.
- Identifican un usuario deshonesto.
- Obtienen credenciales comprometidas.

Explotan el acceso

- Mueven lateralmente al objetivo deseado
- Escalan privilegios según sea necesario
- Acceden a activos

Abusan del acceso

- Ofuscan la actividad de la red

- Alteran datos
- Exfiltran datos” (Ibm, 2023)

2.1 ¿A qué se dirigen los atacantes cibernéticos?

(Ibm, 2023) menciona que los ciberataques suceden debido a que las organizaciones, los actores estatales o los particulares quieren una o varias cosas, como:

- Datos financieros empresariales.
- Listas de clients.
- Datos financieros del cliente.
- Bases de datos de clientes, incluida la información de identificación personal.
- Direcciones de e-mail y credenciales de inicio de sesión.
- Propiedad intelectual, como secretos comerciales o diseños de productos.
- Acceso a la infraestructura de TI.
- Servicios de TI, para aceptar pagos financieros.
- Datos personales confidenciales.
- Departamentos y agencias gubernamentales.

Según (proofpoint, 2022), el robo de credenciales a las organizaciones aumentó un 65% en el costo total, pasando de 2,79 millones de dólares en 2020 a 4,6 millones de dólares en la actualidad.

La duración de un incidente interno aumentó de 77 a 85 días, lo que obligó a las organizaciones a aumentar los gastos de contención.

Las empresas pagaron en promedio 17,19 millones de dólares (base anualizada) por incidentes que tardaron más de 90 días en solucionarse.

2.2 ¿Cuáles son los tipos habituales de ciberataques?

Cabe mencionar que no todos los ciberataques son iguales. Estos pueden variar en función de la forma en que se ejecuta, su finalidad, su víctima, etc. A continuación, con ayuda de (iberdrola, s.f.) se pueden mencionar los delitos ciberdelictivos más comunes:

- **Phishing:** es el envío de mensajes falsos, generalmente a través de correo electrónico, que parecen provenir de fuentes confiables y seguras. El principal objetivo de este tipo de ciberataques es robar datos personales muy sensibles, como información sobre inicios de sesión o datos de tarjeta de crédito, entre otros.
- **Malware:** Se refiere al software malicioso que contiene virus y gusanos. En esencia, ataca cuando los usuarios hacen clic en un enlace o en un archivo adjunto an un correo electrónico, aprovechando las vulnerabilidades de las redes. La instalación de software dañino (ransomware) o la obtención furtiva de información (spyware) son algunos de sus efectos.
- **Instalación de SQL:** Cuando un delincuente inserta código malicioso en un servidor que utiliza SQL, lo obliga a desvelar información protegida o que normalmente no revelaría, se produce una inyección de lenguaje de consulta estructurado (SQL). El hacker solo puede hacerlo enviando un código malicioso a un cuadro de búsqueda de un sitio web vulnerable.
- **Ataque de denegación de servicio:** El objetivo de este ciberataque es agotar los recursos y el ancho de banda saturando los sistemas, los servidores e incluso las redes con tráfico. Los piratas informáticos suelen emplear una variedad de dispositivos diseñados específicamente para llevar a cabo ataques, lo que resulta en la incapacidad de completar solicitudes legítimas.
- **Fuga de información:** es “una fuga de datos es la pérdida de datos confidenciales causada por un incidente de seguridad que puede haber ocurrido a una organización o una persona. Es decir, hablamos de fuga de datos cuando una información considerada confidencial se pierde, aunque no siempre queda expuesta. La pérdida de información puede ser de cualquier tipo, desde secretos comerciales hasta datos personales o sensibles, pero siempre con ese carácter confidencial, lo que significa que perderla pone en riesgo tanto la integridad como la

disponibilidad de la información, y en el caso de una fuga de datos personales, la privacidad de las personas” (34, s.f.).

Aunque estos son solo algunos de los ciberataques más conocidos y comunes, existen otros, como los de intermediario, los de día cero y la tunelización de DNS.

6 áreas que impactan el riesgo cibernético dentro de una organización

Es imprescindible que las empresas conozcan el daño y alcance que pueden llegar a tener por causa de ciberataques a nivel interno y externo del negocio. Según (marsh, 2023) las áreas mas afectadas son las siguientes:

1. Interrupción de negocio, retrasos en los procesos de producción o entrega de servicios: Cuando los sistemas están bloqueados por el secuestro de información, pueden pasar varias horas o incluso días antes de que se recupere la información comprometida y se realice un rescate para reiniciar las operaciones. El negocio puede haber tenido un impacto financiero de lucro cesante en este punto.
2. Afectación económica: Cuando los ciberdelincuentes solicitan grandes cantidades de dinero para recuperar la información que ha sido sustraída y secuestrada. Esto tiene un impacto directo en los costos comerciales porque para resolver un siniestro se requiere asistencia y asesoramiento legal y tecnológico de expertos.
3. Afectación informática: Es necesario limpiar archivos, restaurar datos, reconfigurar sistemas y restaurar copias de datos en sitios de almacenamiento alternativos con mayor protección como resultado de un siniestro.
4. Pérdida de clientes y proveedores: Materialización de riesgos reputacionales, que pueden tener un impacto negativo en la reputación de la empresa frente al mercado, aliados, clientes y proveedores,

así como una pérdida de confianza.

5. Afectación laboral: Pérdida de horas de trabajo, horas extras después de un siniestro y pérdida de beneficios.

6. Legal: Información sobre los afectados y responsabilidad civil de terceros según la Ley de protección de datos personales.

2.3 ¿Qué pueden hacer los ciberataques?

Si el ciberataque tiene éxito, (Ibm, 2023) menciona que pueden resultar en tiempo inactivo, pérdida o manipulación de datos y pérdida de dinero por rescates. Además, la falta de actividad puede causar interrupciones significativas del servicio y pérdidas económicas. Como ejemplo:

- Los ataques DoS, DDoS y malware tienen el potencial de causar fallas en el sistema o el servidor.
- Los ataques de tunelización de DNS e inyección de SQL tienen la capacidad de modificar, eliminar, agregar o robar datos en un sistema.
- Los ataques de phishing y la explotación de día cero permiten a los atacantes infiltrarse en un sistema para causar daños o robar información importante.
- Los ataques de ransomware pueden desactivar el sistema hasta que la empresa pague un rescate al atacante.

2.4 Data los prevention

Según lo comenta (Fernández, 2020) los usuarios finales de una red no deben enviar datos sensibles o confidenciales. Esto se conoce como prevención de pérdida de datos. Se utiliza un software de administración de redes que monitorea el tipo de datos que transfieren los usuarios. Dicho concepto puede parecer bastante evidente a simple vista. Sin embargo, las amenazas que ocurren a nivel interno de la organización tienen más probabilidades de convertirse en ataques y vulnerabilidades

peligrosas. Hoy en día, es bastante necesario implementar prácticas y soluciones DLP. Cada vez que ocurre un accidente de tráfico, los datos de la organización son monitoreados de cerca. Tanto a través de la red como los intentos de hacerlos salir de la red de origen. En caso de ser descubierto, se considera como actividad sospechosa y se imponen políticas rigurosas para prohibirla.

Para (Fernández, 2020), los datos con los que se debe tener especial cuidado son:

- Propiedad Intelectual: cualquier creación original de datos realizada por la organización. Aquí también se consideran datos sensibles como listas de precios, control de inventario, facturación y documentación general.
- Los datos corporativos son el núcleo de la organización. como documentos de planificación estratégica organizacional, datos financieros y datos de colaboradores (datos personales, nóminas).
- Datos del cliente: números de tarjetas de crédito, código de seguridad, datos financieros, números de seguridad social, registros médicos y mucho más.

2.5 Desvinculación laboral

Tal como lo menciona (Team, s.f.) El proceso donde la relación laboral entre un empleador y un colaborador se rompe se conoce como desvinculación laboral. En otras palabras, es el proceso por el cual el empleado deja de prestar sus servicios al empleador, lo que significa que termina la relación contractual que había existido entre ambos. Todos los pasos necesarios para despedir al colaborador están incluidos en este proceso. Es fundamental que el proceso de salida del trabajador se realice de manera positiva y bajo un proceso claro y detallado, respetando los derechos laborales del trabajador y las leyes laborales aplicables, ya sea por razones personales del trabajador o por decisión de la empresa.

Así mismo menciona (Team, s.f.) que la rotación de empleados es inevitable y, aunque no es fácil, administrar esas transiciones es una inversión importante y valiosa para las empresas. La forma en que se lleva a cabo la desvinculación laboral tiene un impacto significativo en la confianza en la

empresa, los procedimientos, la reputación, la cultura y los clientes. La forma en que se lleva a cabo este proceso demuestra los valores bajo los cuales se rige la empresa. El empleado siempre recuerda dos momentos de su relación laboral: su llegada a la empresa y su despedida. Es importante tener en cuenta que los ex empleados siguen siendo portavoces de su marca, por lo que la impresión que dejan durante el proceso de transición es crucial. Por lo tanto, una transición fluida tanto para la empresa como para la persona que se marcha se garantiza si se realiza correctamente.

“Siempre es recomendable despedirse en buenos términos con los empleados que se van. Pero el proceso de transición puede ser difícil y hasta complicado, y los empleados a menudo se marchan sintiéndose insatisfechos, no respetados o con una mala impresión de su experiencia”.
(Team, s.f.)

2.6 Tipos de desvinculación laboral en Honduras

Existe una variedad de tipos de desvinculación laboral, que se clasifican según su lugar de origen o residencia y cómo afectan al trabajador y al empleador. El marco legal de la Ley de Contrato de Trabajo y el Código de Trabajo de Honduras regula la desvinculación laboral. A continuación, se enumeran los tipos de desvinculación más comunes en Honduras según (Zelaya, 2021):

1. Despido sin causa justa: el artículo 59 del código de trabajo establece que un empleador puede despedir un trabajador sin justa causa siempre y cuando respete el derecho a una compensación. Además de las prestaciones sociales que le corresponden al trabajador, la indemnización debe incluir un mes de salario por cada año trabajado.
2. Despido por causa justa: El artículo 61 del Código de Trabajo de Honduras establece las causas justas de despido, como el incumplimiento de las obligaciones laborales, el abuso de confianza, el incumplimiento de las normas de seguridad e higiene en el trabajo, la violación de secretos de la empresa, entre otras. El empleador debe notificar al empleado sobre la causa del despido antes de proceder con el despido y darle la oportunidad de defenderse. Además, el empleado tiene la capacidad de impugnar el despido ante la autoridad competente.
3. Renuncia voluntaria: El artículo 74 del Código de Trabajo de Honduras establece que el

trabajador tiene derecho a renunciar voluntariamente a su trabajo en cualquier momento, siempre y cuando lo comunique al empleador con una anticipación mínima de 15 días. El trabajador no tiene derecho a recibir una compensación por su renuncia voluntaria.

4. Terminación del contrato por mutuo acuerdo: El artículo 67 del Código de Trabajo de Honduras establece que el empleador y el trabajador pueden rescindir el contrato de trabajo en cualquier momento, siempre y cuando los términos y condiciones del contrato se establezcan de mutuo acuerdo. El trabajador tiene derecho a una compensación acordada entre las partes en este caso.
5. Terminación del contrato por vencimiento del plazo: Según el artículo 56 del Código de Trabajo de Honduras, si se trata de un contrato a plazo fijo, el contrato terminará automáticamente al final del plazo. En este caso, al término del contrato, el trabajador tiene derecho a recibir todas las prestaciones sociales.

2.7 Lean Six Sigma

Para (sixsigma.co.uk, s.f.) Lean Six Sigma podría definirse como la metodología Lean Six Sigma (LSS) es una estrategia de mejora de procesos comerciales que se basa en la unión de dos filosofías de gestión, Lean y Six Sigma. Six Sigma mejora la calidad y reduce la probabilidad de fallas y errores, mientras que Lean elimina desperdicio del proceso de fabricación para maximizar la satisfacción del cliente. La técnica se basa en ocho tipos de desechos:

- Defectos
- Sobreproducción
- Inventario
- Transporte
- Talentos no utilizados
- Procesamiento adicional
- Espera
- Movimiento

Uno de los enfoques de Six Sigma es DMAIC. Definir, medir, analizar, mejorar y controlar es lo que significa. A continuación, se describirá cómo implementar DMAIC, las cinco fases y otras estrategias.

Pero primero hay que describir que es DMAIC:

Para (Jonathan Trout, 2021), DMIC, pronunciado də-MAY-ick, es un acrónimo de "definir", "medir", "analizar", "mejorar" y "controlar". El objetivo de este método de mejora basado en datos es encontrar y eliminar los defectos. Es una de las dos metodologías utilizadas para implementar Six Sigma, aunque no es exclusiva de Six Sigma. Su objetivo es mejorar los procesos y proyectos existentes.

A continuación, se procede a describir las 5 fases de DMAIC:

Definir: Para (Jonathan Trout, 2021) "hay que comenzar por plantearse la siguiente pregunta ¿Qué problema le gustaría solucionar?" Para responder a esta pregunta, el equipo debe crear una declaración del problema, una declaración de objetivos y un cronograma en un documento vivo que lo abarque todo. El estatuto del proyecto es utilizado por su equipo para aclarar temas como los problemas que se están investigando, por qué los está investigando y cómo debería ser un resultado exitoso. El enunciado del problema debe incluir una medida identificable, como la calidad del producto y el tiempo de entrega. La cantidad de tiempo que le lleva al cliente hacer una solicitud hasta que se entrega el producto se conoce como tiempo de entrega. El término "calidad" puede referirse a una variedad de cosas, pero generalmente se refiere a la falta de calidad.

Medir: (Jonathan Trout, 2021) menciona que la fase de medición de DMAIC le muestra cómo se está desempeñando su proceso actual, destacando la magnitud de los problemas. Se trata de recopilar sus datos para que puedan analizarse. Antes de comenzar a hablar sobre los procedimientos de la fase de medición, repasemos algunas definiciones importantes.

Analizar: "¿Qué está causando el problema?" es para (Jonathan Trout, 2021) la pregunta que responde la fase de análisis de DMAIC. Aquí es donde su equipo descubre las causas verdaderas de los problemas haciendo un análisis de causa raíz. La fase de análisis no se enfoca en la implementación de soluciones, sino en la resolución de problemas. Para ello, haga una lluvia de ideas sobre las posibles causas raíz, cree una hipótesis de por qué existen los problemas y luego trabaje para respaldar las hipótesis. Antes de encontrar soluciones, los equipos deben examinar el proceso y el análisis de datos. El análisis de la operación incluye:

Analizar el tiempo. Esta forma de análisis se centra en el tiempo real en que se realiza el trabajo durante un proceso en comparación con el tiempo de espera.

Análisis de valor total. Analiza sus procesos desde la perspectiva del cliente. En otras palabras, descubra qué es importante para el cliente y mejore esas características.

Visualizar el flujo de valor. Aquí, los datos del proceso se combinan con los pasos de un proceso que agrega valor para ayudar a destacar dónde se pueden eliminar los desperdicios.

Controlar, una vez que el problema se ha solventado, se ha dado una solución y se están llevando a cabo mejoras. Para (Jonathan Trout, 2021) es el momento de mantener la solución y mantener los cambios positivos con el nuevo proceso. La fase de control de DMAIC es donde su equipo crea un plan de monitoreo para medir las mejoras de los nuevos procesos y un plan de respuesta en caso de que el desempeño disminuya. Registrar el nuevo procedimiento. Su equipo debe registrar los nuevos y mejorados procesos durante la fase de control. Los mapas de procesos actualizados, las listas de verificación actualizadas con nuevos procedimientos y otra documentación estandarizada son parte de esto. Todos tendrán más facilidad para adoptar la nueva manera de hacer las cosas cuanto más fácil sea digerir y comprender la documentación. Hacer visible el lugar de trabajo es la forma más efectiva de hacerlo. Para garantizar que cada espacio de trabajo esté ordenado y limpio, así como para etiquetar cada espacio de trabajo con instrucciones importantes, se utilizan herramientas como el sistema 5-S.

CAPÍTULO 3. ANALISIS DE RIESGO CIBERNETICO ASOCIADOS AL PROCESO DE DESVINCULACIÓN LABORAL

Durante esta capitulo, se analiza los riesgos cibernéticos asociados el actual proceso de desvinculación laboral. Dicho proceso presenta una importante vulnerabilidad ocasionando riesgo en termino de seguridad y privacidad de información, estas deficiencias dan la apertura para fuga y perdida de información crítica para la empresa, como datos de clientes, estrategias comerciales, lo que pone en riesgo la ventaja competitiva de la empresa, lo que podría conllevar consecuencias financieras. Además, los datos secretos de la empresa podrían ser utilizados en su contra o vendidos a competidores, lo que podría tener un impacto significativo en la reputación y la confianza de los clientes.

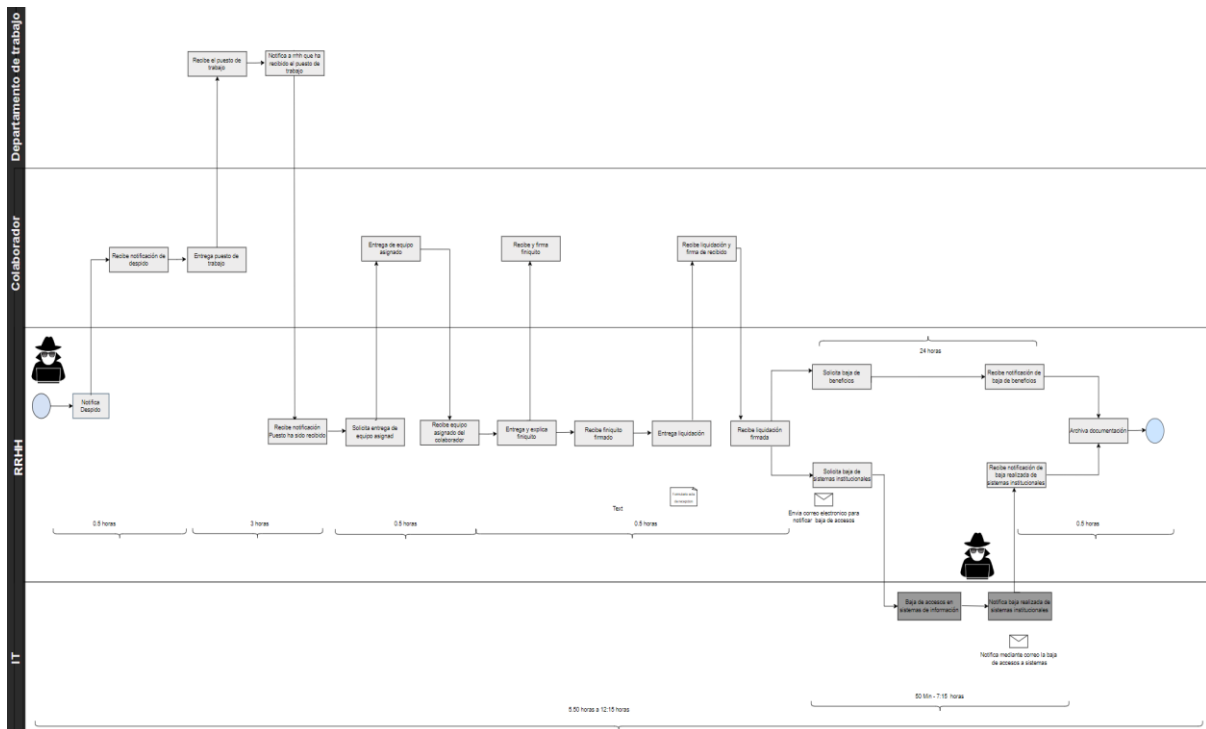
Ocurre lo mismo al tener la capacidad de poder realizar modificaciones no autorizadas en los sistemas o llevar a cabo ataques cibernéticos internos durante el proceso de desvinculación laboral, ya que representa una amenaza para la integridad y el buen funcionamiento de los sistemas de la empresa. Esto podría dar lugar a la interrupción de operaciones comerciales u operacionales críticas, pérdida de datos valiosos y daños a la infraestructura tecnológica.

Con el objetivo de identificar y abordar los riesgos asociados, se procede a analizar cada etapa del proceso de desvinculación laboral, centrándose en aquellas etapas del proceso que presentan mayor amenaza para la información. El propósito es identificar las debilidades del proceso y proponer las medidas necesarias que garanticen la protección de los datos.

3.1 Proceso actual de Despido laboral

A continuación, se muestra una representación gráfica de las actividades, las interacciones y los puntos de decisión del proceso de desvinculación laboral. Se marcó con un símbolo las dos partes del proceso en la que se están presentando vulnerabilidades de seguridad de la información. Se seleccionaron los dos procesos de desvinculación laboral más comunes, por despido y renuncia.

Ilustración 1 - Proceso actual de despido



*En anexos se muestra este mismo diagrama en mayor tamaño para visualizarlo mejor.

Como se puede observar, se identificaron vulnerabilidades que pueden ocasionar un riesgo en términos de integridad, disponibilidad, seguridad y privacidad de la información, con posibilidades de fuga y pérdida de información crítica para la empresa, daños de reputación y costos financieros.

Se puede notar que uno de los riesgos cibernéticos importantes se da desde el momento en el que el colaborador puede extraer información sensible de la empresa incluso antes de ser despedido o de presentar su renuncia, lo cual hace que la posibilidad de realizar dicha acción durante el proceso de separación laboral sea aún más alta. Esto ocasionado porque no actualmente no cuentan con ningún medio que analice la manera en que las personas utilizan los datos y que pueda prevenir

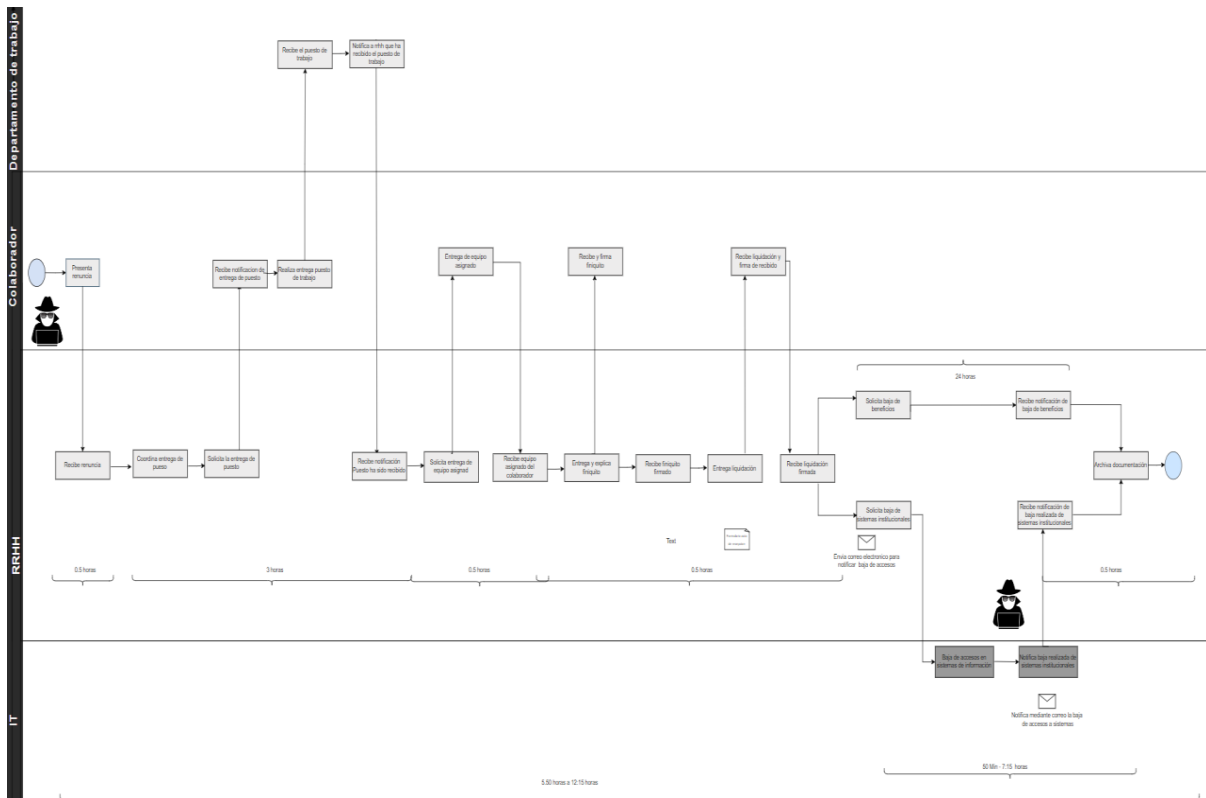
la fuga de la información.

Otro de los riesgos importantes es que el subproceso, “baja de accesos de los colaboradores” está tomando un tiempo importante, lo cual indica que los tiempos límites para la eliminación de accesos de un excolaborador actualmente está en 50 min a 7:15 horas, lo cual es tiempo suficiente para que la empresa quede vulnerable y pueda sufrir un ataque cibernético que amenazan la posición competitiva y la estabilidad financiera.

3.2 Proceso actual de renuncia laboral

Seguidamente, se muestra una representación gráfica del proceso actual de renuncia laboral. Se marcó con un símbolo las dos partes del proceso en la que se están presentando vulnerabilidades de seguridad de la información.

Ilustración 2 - Proceso actual de renuncia laboral



*En anexos se muestra este mismo diagrama en mayor tamaño para visualizarlo mejor.

Como se puede notar, el proceso de renuncia laboral también presenta los mismos riesgos de seguridad de información. Los riesgos cibernéticos cuando los colaboradores pueden extraer información de la empresa antes o posterior al presentar su renuncia. Con una alta probabilidad de que realicen acciones indebidas durante el proceso de separación laboral.

Según el análisis anterior, se ha decidido centrarse en las dos partes del proceso de desvinculación laboral que presentan mayor vulnerabilidad en términos de riesgo cibernético:

3.3 Etapas del proceso de desvinculación laboral a analizar y mejorar.

3.3.1 Riesgo cibernético previo a la desvinculación laboral.

La fuga de información previa a la desvinculación laboral no solo representa una amenaza para la empresa en términos financieros y de competitividad, ya que la divulgación de datos sensibles o confidenciales podría ser aprovechada por competidores o personas malintencionadas.

Además, puede ocasionar pérdida de confianza por parte de los clientes, proveedores y otros interesados, quienes podrían sentirse preocupados por la seguridad de sus datos, quienes al verse en este tipo de situaciones podrían optar por buscar servicios o productos en una empresa más confiable.

De este mismo punto se deriva el impacto en la reputación de la empresa. Puede dañar la imagen y credibilidad, lo cual es principalmente perjudicial en un ambiente empresarial altamente competitivo como en el que se encuentra Tecno Solutions. La pérdida de la confianza y el prestigio ganados a lo largo del tiempo puede resultar difícil de recuperar, afectando la relación con los clientes existentes y dificultando la captación de nuevos.

Además, la fuga de información previa a la desvinculación laboral puede dar lugar a violaciones de privacidad y protección de datos, lo cual podría acarrear consecuencias legales y sanciones.

3.3.2 Riesgo cibernético asociado al proceso de baja de accesos lógicos y físicos.

Como se ha visto durante el análisis del proceso de desvinculación laboral, el riesgo cibernético asociado al subproceso de baja de accesos lógicos y físicos representa una preocupación y un desafío importante para la empresa Tecno Solutions. Durante este proceso, existe la posibilidad de que se produzcan brechas de seguridad que permitan accesos no autorizados a los sistemas y las instalaciones físicas de la empresa.

Estas brechas de seguridad dar lugar a diversos problemas, como la fuga de información confidencial, el robo de datos sensibles, el sabotaje de sistemas, la interrupción de operaciones comerciales y tecnológicas, así como la pérdida de activos críticos. Además, pueden poner en riesgo la reputación de la empresa y generar consecuencias financieras negativas.

Para mitigar el riesgo cibernético asociado a este proceso, es fundamental implementar medidas de seguridad sólidas, para ello se procederá a realizar un análisis minucioso de este subproceso y poder identificar más a profundidad las posibles causas del problema y de esta forma hacer las recomendaciones respectivas para reducir este riesgo cibernético asociado al proceso

CAPÍTULO 4. REDUCCIÓN DE RIESGOS CIBERNÉTICOS EN PROCESO DE DESVINCULACIÓN LABORAL

Durante este capítulo, se abordarán los dos riesgos cibernéticos identificados como los más significativos asociados al proceso de desvinculación laboral mencionado en el capítulo anterior.

Se presentarán análisis detallados y mejoras con el objetivo de proteger la información confidencial, prevenir ataques cibernéticos y preservar la integridad de los sistemas y garantizar la continuidad del negocio.

4.1 Análisis y disminución del riesgo cibernético previo a la desvinculación laboral.

Uno de los riesgos importantes identificados en el proceso de desvinculación laboral, es la fuga de información previo a este periodo de transición. Durante este periodo existe una ventana de vulnerabilidad en la que los empleados que están a punto de dejar la empresa pueden filtrar confidencial y valiosa.

Este riesgo puede manifestarse en diversas circunstancias, por ejemplo, los empleados descontentos o resentidos pueden usar su posición privilegiada para acceder, copiar o divulgar información estratégica como planes comerciales, estrategias de marketing, datos de clientes o incluso propiedad intelectual. Además, pueden intentar borrar o alterar datos en los sistemas de la empresa, comprometiendo la integridad de la información y afectando la operatividad del negocio.

Este problema se agrava aún más debido a que actualmente no se cuenta con políticas, medidas preventivas para analizar cómo se utilizan los datos y prevenir la fuga de la información, así como tampoco hay una cultura de seguridad sólida para proteger la información valiosa.

Por lo tanto, como se ha mencionado anteriormente para controlar adecuadamente la seguridad de la información se debe tener visibilidad sobre cómo los usuarios interactúan con los datos y las aplicaciones es clave.

Es fundamental tener en cuenta estos dos aspectos cruciales, los datos y las personas, al evaluar y gestionar eficazmente la seguridad de la información.

Por dicha razón, es crucial mitigar este riesgo e implementar medidas preventivas.

Para ello se proponer lo siguiente:

1. Para poder proteger la información confidencial y los intereses comerciales se propone establecer acuerdos de confidencialidad y no competencia, así como cláusulas de no divulgación como parte de los contratos laborales.
 - Establecer un NDA (acuerdo de confidencialidad), donde se indica que la información confidencial compartida al colaborador debe mantenerse en secreto y no divulgarse con terceros sin el consentimiento de la empresa. Información confidencial como secretos comerciales, datos financieros, estrategias o cualquier otra información sensible que pueda afectar los intereses de la organización.
 - Establecer acuerdos de no competencia. Es decir, un contrato que indica que el colaborador se compromete a no participar en actividades comerciales o competir directamente con la empresa durante un periodo de tiempo. Podría establecerse para puestos de altos ejecutivos, para evitar que utilice la información confidencial para beneficiarse y perjudicarla la empresa.
2. Implementar un DLP (Data loss prevention). El factor humano, o las interacciones entre usuarios, datos y redes, debe ser parte del programa de protección de datos de una organización. **Además, se debe monitorear la transferencia de datos y enfatizar a quienes crean, tocan y mueven los datos a través de la empresa.**

Se recomienda implementar Forcepoint DLP en la nube. Es un software de prevención de fuga

y pérdida de datos que se usa para identificar, investigar y reducir los riesgos potenciales para activos e información sensibles.

Según (forcepoint, 2021), las características de esta solución son:

Cumplimiento de políticas, analíticas de comportamiento, descubrimiento y clasificación de datos según su nivel de confidencialidad, facilitando la identificación y protección de la información sensible.

Esta aplicación permite a los administradores de TI priorizar las actividades de alto riesgo según los incidentes de datos, los modelos y los eventos de recopilación de terminales, y automatizar las políticas para proteger los datos en tiempo real. El DLP puede implementar reglas y políticas para evitar la filtración de datos confidenciales, bloquear o controlar la transferencia, copia o acceso no autorizado a datos confidenciales.

Permite administrar y controlar el acceso y el uso de dispositivos de almacenamiento externos, como unidades USB o discos duros externos, para evitar la pérdida o robo de datos.

permite el seguimiento y la detección de actividades sospechosas. El DLP puede detectar brechas de seguridad supervisando y analizando el tráfico de datos en la red, el almacenamiento de archivos, el correo electrónico y otras comunicaciones.

De igual forma, puede generar informes y registros detallados sobre el uso y movimiento de datos sensibles, lo que ayuda a cumplir con regulaciones y normativas de seguridad de datos, lo que ayuda en la auditoría y cumplimiento normativo.

Para reducir la necesidad de infraestructura física, se propone que esta herramienta se encuentre en la nube, lo que a su vez reducirá el consumo de energía y la generación de residuos.

4.2 análisis y mejora del subproceso de baja de accesos mediante

metodología DMAIC

Durante esta capítulo, se analiza el actual subproceso de baja de accesos, ya que se identifico que esta presentando vulnerabilidades en términos de riesgos cibernéticos. Con el objetivo de identificar las debilidades del proceso y mejorarlo para prevenir daños a la empresa y proteger información confidencial, lo que garantiza la integridad y disponibilidad de la información. Reduciendo colateralmente los potenciales costos financieros y daños en la reputación. Se realizará mediante el uso de la metodología DMAIC Lean Six Sigma y se diseñará un nuevo proceso optimizado para mejorar la eficiencia, eficacia y calidad del proceso, sin afectar la seguridad y operatividad de la empresa.

4.2.1 DEFINE

Se definirán los objetivos del proyecto y los entregables.

4.2.1 Problem Statement

La empresa Tecno solutions actualmente se está enfrentando a un importante riesgo en termino de seguridad y privacidad de información asociado al proceso de desvinculación de empleados, específicamente en su subproceso de baja de accesos físicos y lógicos. estas deficiencias dan la apertura para fuga y perdida de información crítica para la empresa, como datos de clientes, estrategias comerciales, datos secretos de la compañía, realizar modificaciones no autorizadas en los sistemas, o incluso llevar a cabo ataques cibernéticos contra la empresa. Estas deficiencias ponen en riesgo la integridad y reputación de la empresa, lo que puede tener consecuencias financieras.

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL LAURY FERNANDA OSORIO PAGAOGA

4.2.2 Goal Statement

Fortalecer y mejorar la seguridad informática en un 70% mediante la mejora del subproceso de baja de accesos físicos y lógicos, reduciendo así la posibilidad de fugas de información y minimizando los riesgos de seguridad y privacidad de los sistemas de información. El proyecto se completará en 5 meses, con el propósito de mitigar los riesgos cibernéticos, proteger la empresa y sus sistemas de información, y evitar posibles costos financieros y daños en la reputación. Sin impactar negativamente la seguridad y operatividad de la organización.

4.2.3 Project Charter

Ilustración 3- Project Charter

PROJECT CHARTER					
Problem Statement			Business Case & Benefits		
<p>La empresa Tecno solutions actualmente se está enfrentando a un importante riesgo en termino de seguridad y privacidad de información asociado al proceso de desvinculación de empleados, específicamente en su subproceso de baja de accesos físicos y lógicos. estas deficiencias dan la apertura para fuga y perdida de información crítica para la empresa, como datos de clientes, estrategias comerciales, datos secretos de la compañía, realizar modificaciones no autorizadas en los sistemas, o incluso llevar a cabo ataques cibernéticos contra la empresa. Estas deficiencias ponen en riesgo la integridad y reputación de la empresa, lo que puede tener consecuencias financieras.</p>			<p>El proceso de baja de accesos físicos y logicos, seguro y eficiente ayuda a prevenir daños a la empresa y proteger información confidencial, tambien disminuye el riesgo de ataques cibernéticos lo que garantiza la integridad y disponibilidad continua de la información. Esto reduce costos financieros y daños en la reputación, y fortalece la posición competitiva de la empresa.</p>		
Goal Statement		Timeline			
<p>Fortalecer y mejorar la seguridad informática en un 70% mediante la mejora del subproceso de baja de accesos físicos y lógicos, reduciendo así la posibilidad de fugas de información y minimizando los riesgos de seguridad y privacidad de los sistemas de información. El proyecto se completará en 5 meses, con el propósito de mitigar los riesgos cibernéticos, proteger la empresa y sus sistemas de información, y evitar posibles costos financieros y daños en la reputación. Sin impactar negativamente la seguridad y operatividad de la organización.</p>		Phase	Planned Completion Date	Actual	
		Define:	Mes 1		
		Measure:	Mes 2		
		Analyze:	Mes 3		
		Improve:	Mes 4		
		Control:	Mes 5		
Scope In/Out		Team Members			
1st Process Step	Notificación de renuncia/Despido	Position	Person	Title	% of Time
Last Process Step	Archivar documentación				20%
					30%
					25%
In Scope:	<p>Evaluación de las vulnerabilidades actuales del subproceso de baja de accesos en términos de seguridad informática. Diseño e implementación de medidas de seguridad adecuadas para proteger la información confidencial durante el proceso de desvinculación. Implementación piloto y evaluación de la eficacia de las medidas de seguridad. Implementación completa de las medidas de seguridad. Monitoreo y revisión continua de las medidas de seguridad implementadas para garantizar su efectividad.</p>				
Out of Scope:	<p>Decisiones y políticas relacionadas con la contratación y despidos</p>				

4.2.4 SIPOC

En la siguiente imagen se muestra una perspectiva del subproceso baja de accesos físicos y lógicos, se centró en esta parte del proceso de desvinculación de empleados, ya que como se había mencionado anteriormente, es donde se encuentra un alto riesgo de ataque cibernético. Se identifican los proveedores, las entradas, el propio proceso, las salidas y los clientes relacionados con la reducción de riesgo cibernético durante la desvinculación laboral, específicamente en la baja de accesos físicos y lógicos.

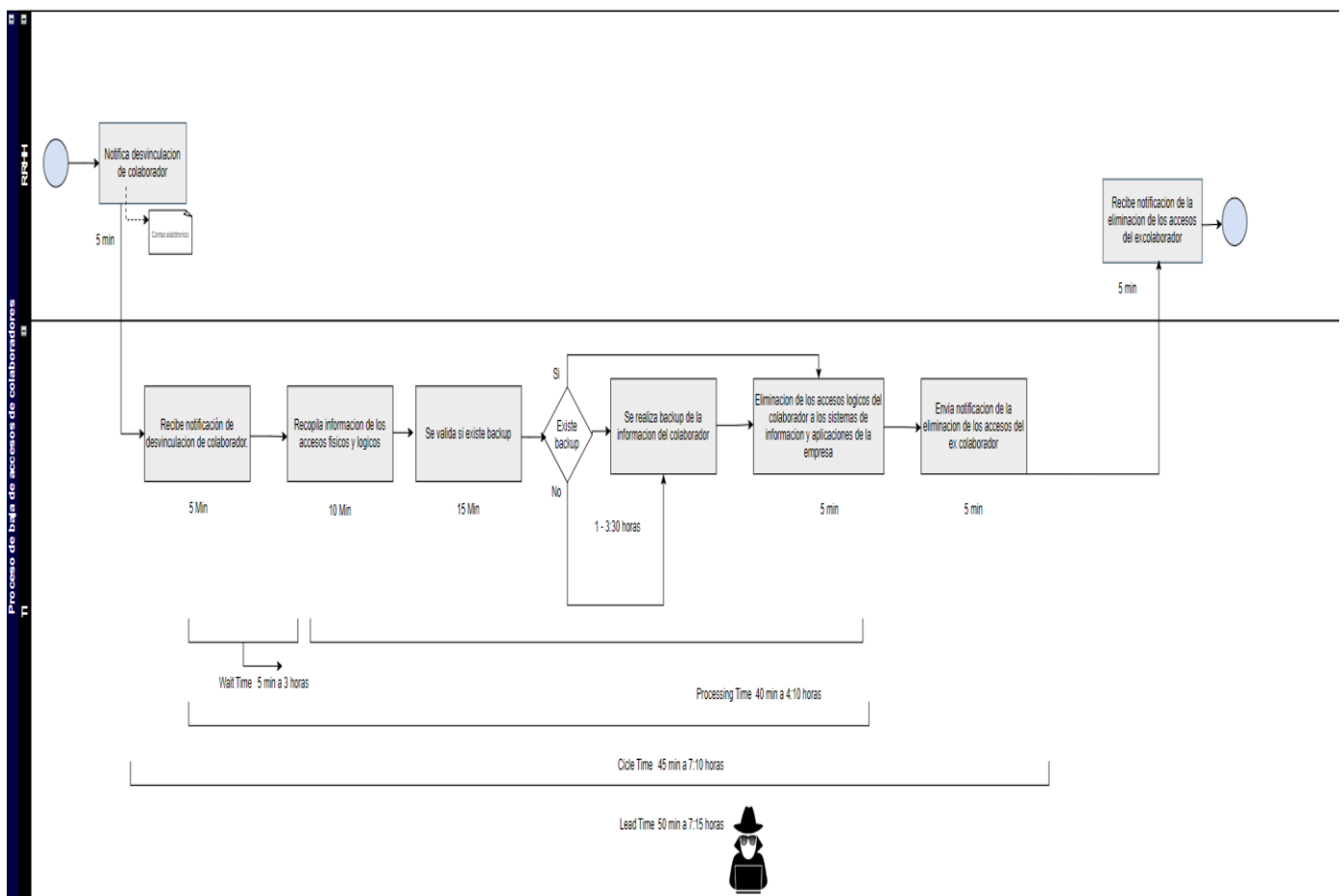
Ilustración 4 - SIPOC



4.2.5 Process Map

En este punto muestra una representación gráfica de las actividades, las interacciones y los puntos de decisión del proceso de baja de accesos físicos y lógicos del colaborador.

Ilustración 5 - Process Map



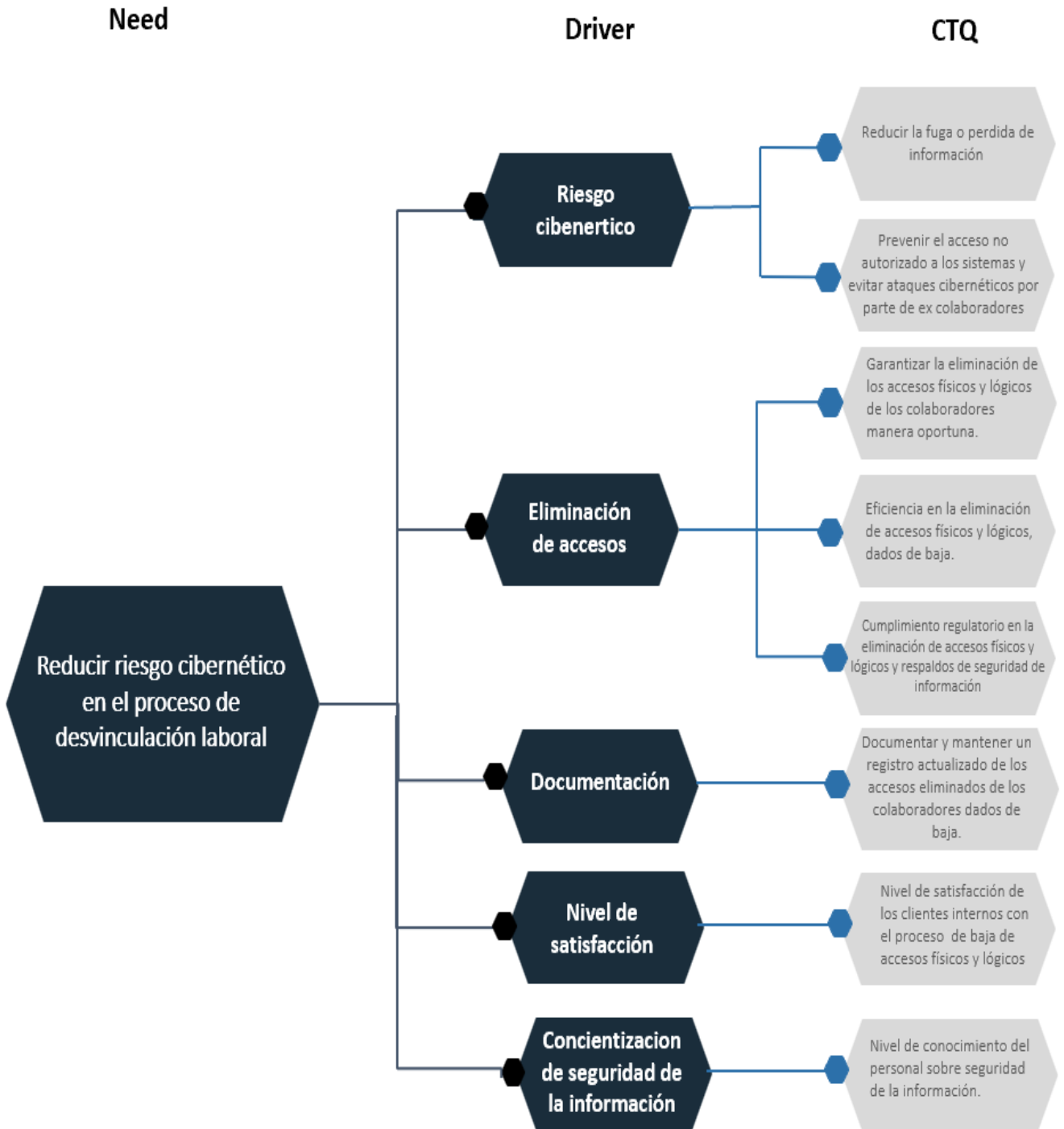
*En anexos se muestra este mismo diagrama en mayor tamaño para visualizarlo mejor.

El proceso de baja de accesos, ilustrado en la imagen, inicia cuando el departamento de Recursos Humanos notifica la desvinculación de un colaborador y culmina cuando el departamento de Tecnologías de la Información (TI) envía una notificación por correo electrónico confirmando la eliminación exitosa de los accesos del usuario correspondiente. Sin embargo, se destaca que el símbolo utilizado en la imagen indica que, debido al tiempo prolongado necesario para eliminar los accesos, existe un alto riesgo de que la empresa sea vulnerable a posibles ataques cibernéticos. Estos ataques pueden generar un impacto negativo en la organización en términos de seguridad, reputación y operaciones. Es necesario abordar esta vulnerabilidad y tomar medidas adecuadas para minimizar los riesgos asociados.

4.2.6 Critical to Quality

A continuación, se priorizan las necesidades que el proyecto debe cubrir, se identifican los factores critical to quality (CTQ)

Ilustración 6- Critical To Quality

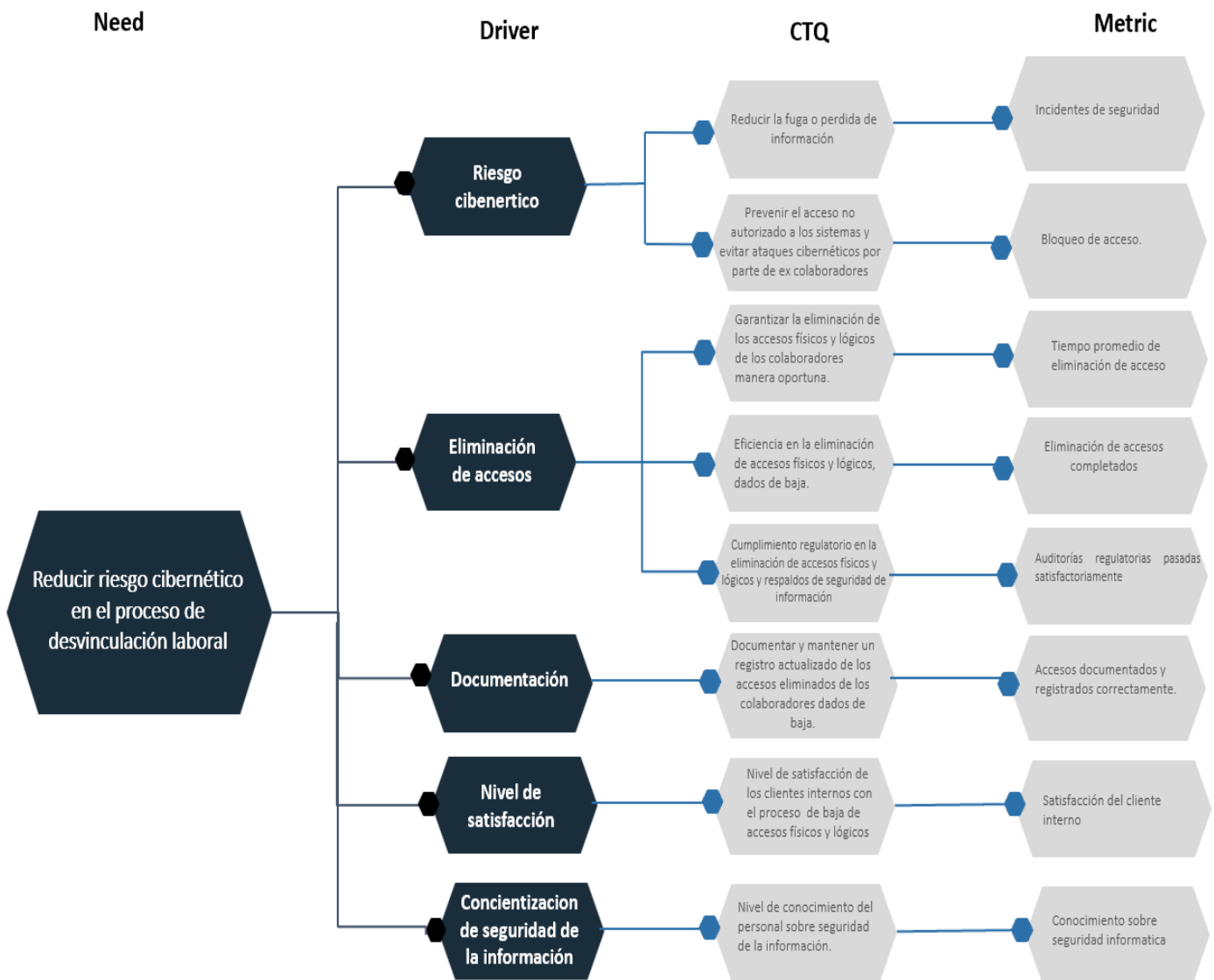


4.3 MEASURE

A continuación, se llevará a cabo el análisis del proceso con el objetivo de obtener una comprensión completa de su estado actual y cuantificar el problema que se está abordando. Mediante este proceso de medición, se recopilarán datos relevantes y se realizarán evaluaciones para identificar las áreas de mejora necesarias e implementar las acciones correctivas adecuadas.

4.3.1 KPI's (Key Performance Indicators)

Ilustración 7 - KPI Key Performance Indicators



4.3.2 Data Collection

La recolección de los datos se hizo mediante los correos electrónicos que son enviados por talento humano notificando la desvinculación laboral, y los correos electrónicos enviados por el departamento de TI notificando que los accesos físicos y lógicos se han eliminado. Se tomaron como muestra las bajas de los colaboradores de los últimos 4 meses.

Tipo de dato: Variables, continuos.

4.3.3 Medidas Lean

En el siguiente apartado, se hará un análisis con las medidas lean, centrándose en el subproceso de baja de accesos, debido a que es la parte del proceso de desvinculación de empleados que está mostrando vulnerabilidades para la disponibilidad e integridad de la información. Se analizará para identificar los tiempos de ejecución del subproceso y posibles fallas en el mismo, que colateralmente este afectando los tiempos del proceso general de desvinculación laboral, generando así un potencial riesgo cibernético.

Lead time: Es el tiempo que transcurre desde que recursos humanos notifica que el colaborador ha dejado de laborar para la empresa para proceder a la baja de accesos físicos y lógicos del usuario, hasta el momento en que el departamento de TI notifica a recursos humanos de excolaboradores es de 50 min a 7:15 horas, dependiendo de 2 escenarios.

Escenario 1: Existe la copia de seguridad de la información del excolaborador: 50 minutos

Escenario 2: No existe la copia de seguridad de la información del excolaborador: de 50 min a 7:15 horas, dependiendo de la cantidad de información existente en el ordenador.

El Cycle Time (CT) o tiempo de ciclo es la métrica que muestra el tiempo que le toma al departamento de TI dar de baja a los accesos físicos y lógicos de los excolaboradores, desde que recibe la notificación de desvinculación laboral, hasta que envía la notificación de que los accesos se han

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL LAURY FERNANDA OSORIO PAGAOGA

eliminado.

En este caso, el cycle time se ha dividido en dos componentes:

Wait time: Tiempo que transcurre desde que el departamento de TI recibe la notificación para la baja de los accesos del excolaborador hasta que comienza a trabajar en la acción.

Processing time: Tiempo que transcurre desde que el departamento de TI comienza a realizar el proceso para la baja de accesos hasta que envía la notificación a talento humano de que los accesos han sido eliminados.

Tabla 1 - Medidas Lean

Fecha y hora de notificación de desvinculación laboral	Nombre del colaborador	Cargo laboral	Fecha de comienzo de baja de accesos TI	Fecha y hora notificación de accesos eliminados	Cycle Time		
					Wait time (hr)	Processing time (hr)	LEADTIME (hr)
27/1/2023 16:05	Persona 1	SOPORTE DE DATA CENTER S.P.S	27/1/2023 16:17	30/1/2023 08:28	0	64:11	64.11
27/1/2023 17:41	Persona 2	RECEPCIÓN	30/1/2023 08:54	30/1/2023 09:15	63	00:21	63.21
27/1/2023 17:41	Persona 3	INGENIERO DE PREVENTA Y DISEÑO S.P.S	30/1/2023 09:05	30/1/2023 11:30	63	02:25	65.25
1/2/2023 18:27	Persona 4	ASISTENTE ADMINISTRATIVO	2/2/2023 08:22	2/2/2023 08:35	13	00:13	13.13
6/2/2023 07:54	Persona 5	TÉCNICO OPERADOR DE CENTRO DE SERVICIO	6/2/2023 09:03	6/2/2023 10:31	1	01:28	2.28
21/2/2023 18:55	Persona 6	GERENTE DE VENTAS PREMIUM	22/2/2023 09:49	22/2/2023 10:11	14	00:22	14.22
23/2/2023 08:14	Persona 7	ANALISTA PROGRAMADOR SR	23/2/2023 08:28	23/2/2023 12:20	0	03:52	3.52
23/3/2023 17:49	Persona 8	TÉCNICO OPERADOR DE CENTRO DE SERVICIO	24/3/2023 08:36	24/2/2023 09:36	14	01:00	15.00
20/3/2023 12:54	Persona 9	INGENIERO DE RED HFC, NIVEL 1	20/3/2023 12:54	20/3/2023 14:16	0	01:22	1.22
29/3/2023 17:22	Persona 10	SOPORTE DE DATA CENTER S.P.S	29/3/2023 17:29	30/3/2023 08:10	0	14:41	14.41
29/3/2023 17:51	Persona 11	TÉCNICO SPS	30/3/2023 09:17	30/3/2023 11:41	15	02:24	0.19
21/4/2023 17:55	Persona 12	INGENIERO DE RED CORE	25/4/2023 08:10	25/4/2023 11:10	62	03:00	65.00
10/4/2023 16:19	Persona 13	ANALISTA PROGRAMADOR MID - LEVEL	10/4/2023 16:32	10/4/2023 18:38	0	02:06	2.06

Medidas Lean

Lead time: FNE-FNB

Cycle Time

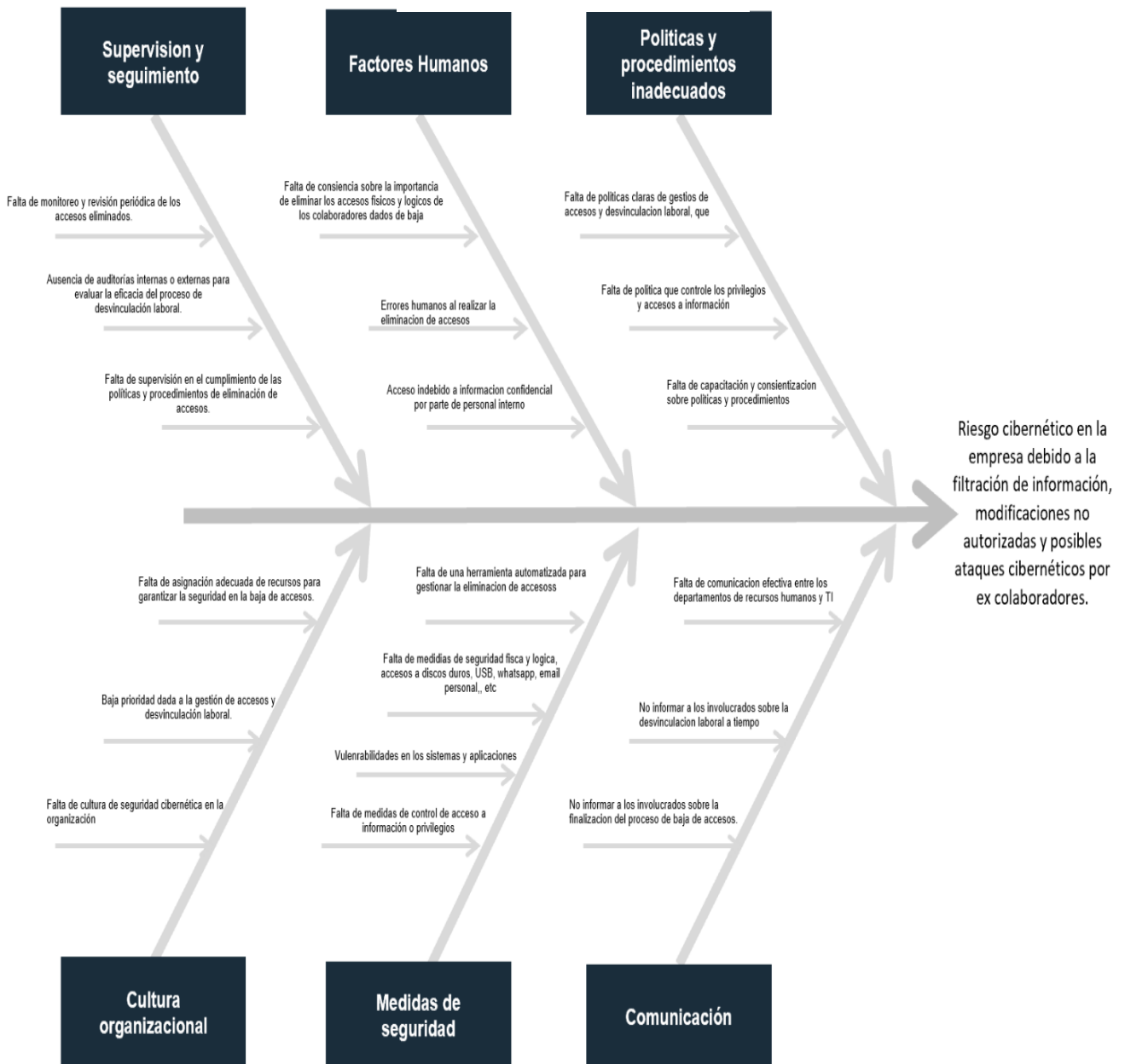
- **Wait time: FCB-FNB**
- **Processing time: FCB-FNE**

En la tabla 1, se puede notar que en el wait time, el 53% de las solicitudes de baja de accesos, son atendidas por el departamento de TI en tiempos superiores a 12 horas de haber recibido la notificación por el departamento de talento humano. Cuanto no debería ser mayor a 3 horas según el proceso de baja de accesos actual.

4.3.4 Matriz de Causa y Efecto (Fishbone Diagram)

En el siguiente diagrama se identifican y comparan las posibles causas del riesgo cibernético como la fuga de información, modificaciones no autorizadas o ataques que ponen en amenaza la seguridad, disponibilidad e integridad de la información.

Ilustración 8 - Matriz de Causa y Efecto



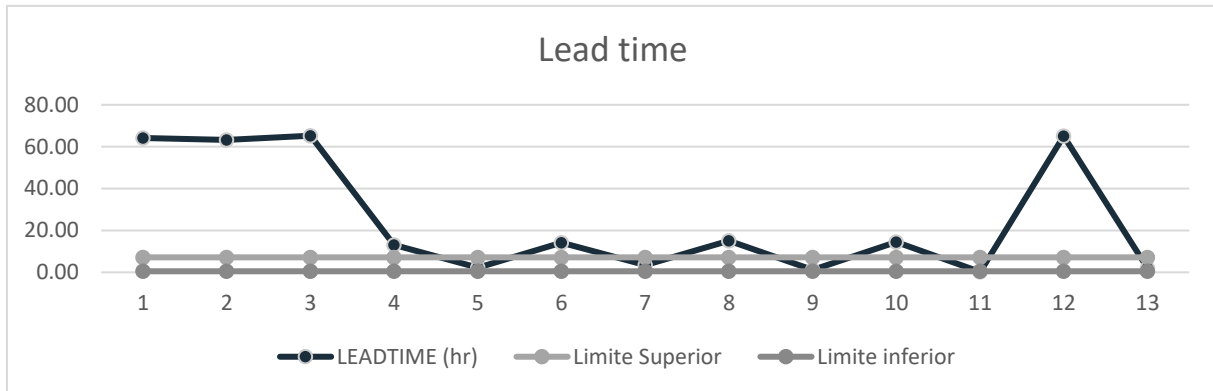


4.4 ANALIZE

En el siguiente apartado se hará un análisis del subproceso de baja de accesos, como se ha explicado anteriormente, hay un enfoque en esta parte del proceso general, ya que está presentando una fuerte amenaza a la disponibilidad e integridad de la información.

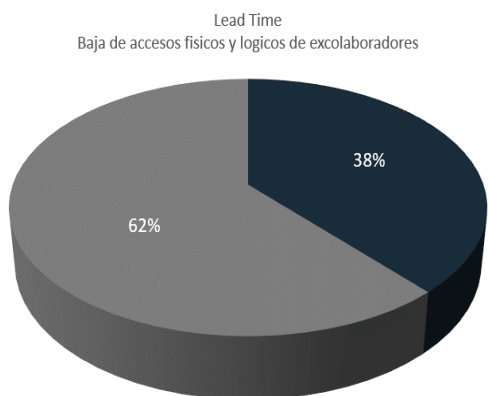
4.4.1 Lead Time

Ilustración 9 - Lead Time



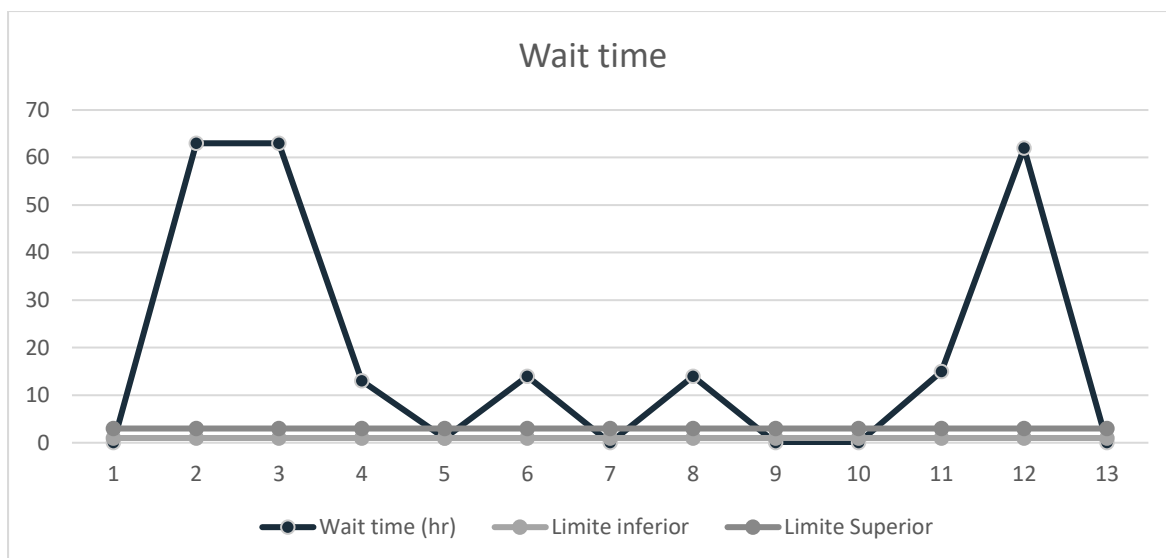
En el gráfico anterior, se presenta el lead time, que representa el tiempo de ejecución del proceso de baja de accesos físicos y lógicos de excolaboradores. Los límites aceptables establecidos son un mínimo de 50 minutos y un máximo de 7:15 horas. Al observar el gráfico, podemos notar que 8 de los 13 puntos se encuentran fuera de estos límites, con un rango de 14 horas hasta 65 horas. Esta situación indica que existe una variabilidad significativa en el tiempo de entrega y que el proceso no está bajo control. Las consecuencias de estos tiempos tan elevados, es el retraso existente para poder dar de baja a los accesos físicos y lógicos de los excolaboradores, tiempo durante el cual el excolaborador aún tiene acceso a los sistemas y datos de la empresa, pueden utilizar esta oportunidad para acceder de manera no autorizada a información confidencial o estratégica. Pueden robar, filtrar o utilizar dicha información de manera malintencionada, lo que representa un riesgo para la seguridad y la privacidad de la empresa.

Ilustración 10 - Diagrama pastel Lead Time



En el gráfico de la izquierda, se puede ver claramente que el 62% de las solicitudes de baja de accesos esta fuera de lead time y solamente un 28% de las solicitudes se están realizando dentro de los tiempos establecidos.

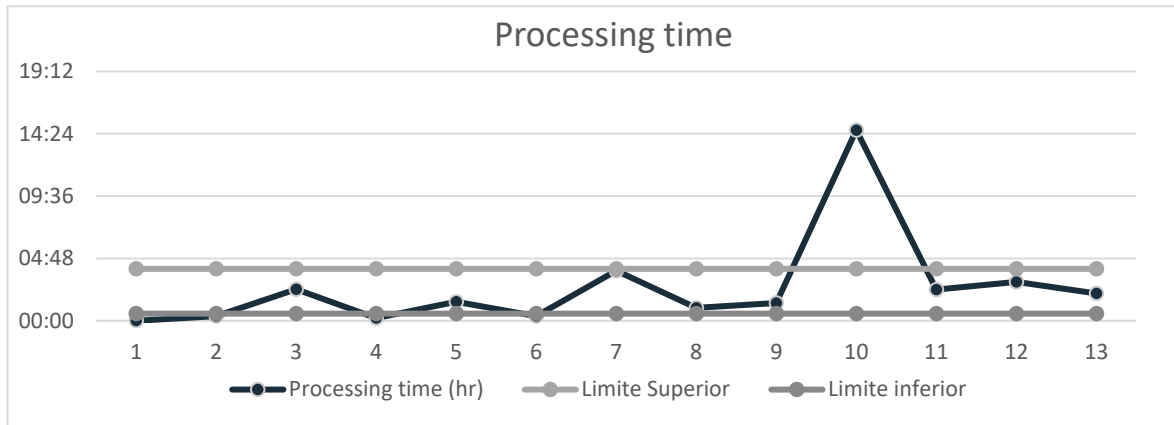
Ilustración 11 - Wait Time



Para analizar más a profundidad donde están los tiempos más elevados de todo el proceso de baja de accesos, se procede a representar el wait time. Tiempo transcurrido desde que recursos humanos realiza la solicitud de baja de accesos del excolaborador hasta el momento en que el departamento de TI comienza a realizar la tarea de eliminación de accesos. Los límites aceptables establecidos son un mínimo de 5 minutos y un máximo de 3 horas. Se observa que 7 de los 13 puntos se encuentran fuera de estos límites, en un rango entre 14 a 63 horas. Tiempo durante el cual, los excolaboradores con acceso no revocado pueden representar una amenaza interna para la empresa. Pueden intentar dañar los sistemas, filtrar información, introducir malware o realizar actividades maliciosas que afecten la infraestructura tecnológica de la organización, pudiendo afectar las operaciones de la empresa.

4.4.3 Processing Time

Ilustración 12 - Processing Time

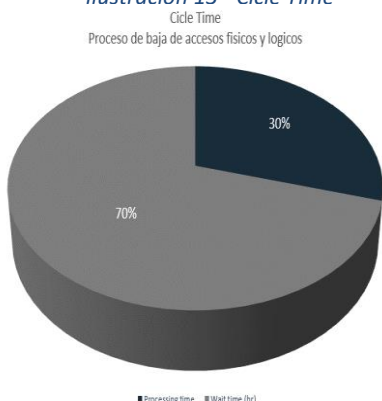


En el grafico anterior se representa el processing time, es decir, el tiempo necesario para completar el proceso de dar de baja los accesos físicos y lógicos de los excolaboradores. Este proceso comienza cuando el administrador de TI inicia la tarea y finaliza cuando se notifica a Recursos Humanos que la baja se ha realizado correctamente. Los límites aceptables establecidos actualmente por la empresa son un mínimo de 40 minutos y un máximo de 4:10 horas. Es importante mencionar que el 92% de los datos se encuentra dentro de estos límites aceptados.

Tras analizar las causas de un dato fuera de límite (14:41 horas), se identificó que la solicitud de baja de accesos se envió en el último momento de la tarde, lo que generó una demora en la ejecución del proceso. Adicionalmente, el excolaborador no contaba con un respaldo de seguridad de la información, lo cual requirió que la ejecución y eliminación del usuario se pospusiera para la noche y se completara al día siguiente.

Se resume, que los datos están dentro de los límites establecidos, sin embargo, por la criticidad del tipo de proceso, se sugiere que puedan reducirse los tiempos para dicho proceso y sus respectivos límites, así se disminuiría la posibilidad de filtración de datos confidenciales o de cualquier acción dañina que pueda perjudicar a la organización.

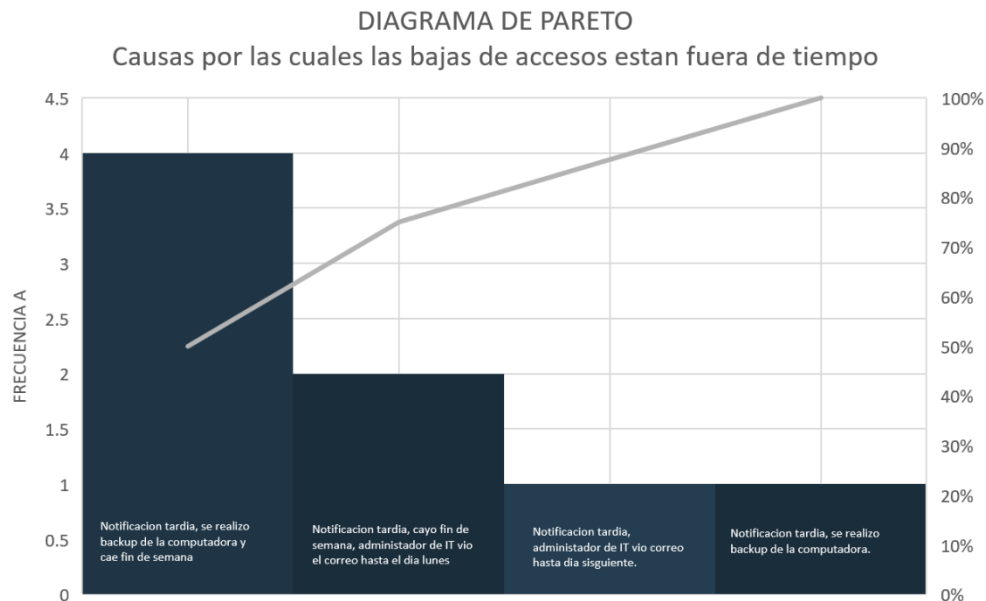
Ilustración 13 - Cycle Time



En el gráfico de la izquierda, se puede observar que el 70% del tiempo del proceso está en el wait time, tiempo que tarda en ser atendida la solicitud y solo un 30% del tiempo lo tiene la ejecución de la baja de los accesos físicos y lógicos.

4.4.4 Diagrama de Pareto

Ilustración 14 - Diagrama de Pareto



Para obtener una comprensión más clara del problema, se realizó un análisis del proceso de baja de accesos, utilizando el diagrama de Pareto, para identificar las causas más comunes de los tiempos prolongados en el proceso de baja de accesos de excolaboradores. Se observó que el mayor problema se encuentra en el momento en que se envían las notificaciones de baja de accesos de excolaboradores desde el departamento de recursos humanos hacia el departamento de TI, las cuales llegan de forma tardía.

La mayoría de las solicitudes que se atendieron fuera de tiempo se debieron a notificaciones enviadas los días viernes por la tarde. En estos casos, los excolaboradores no contaban con un respaldo de seguridad de la información, lo que requería que el proceso se ejecutara durante el fin de semana y que los accesos se eliminaran hasta el próximo lunes. Otra causa común, es que la notificación de baja de accesos llegó al final del día laboral y el administrador de TI pudo verla y atenderla hasta el día siguiente. Convirtiéndose en una brecha importante, ya que los excolaboradores aun pueden acceder a información confidencial, realizar cambios no autorizados, filtrar información sensible como datos confidenciales de la empresa, datos de clientes, secretos comerciales u otra información estratégica que pueda ser utilizada en perjuicio de la organización.

Tras el análisis del proceso de baja de accesos de colaboradores, se identificó que existen diferentes problemas que están afectando los tiempos para poder realizar el proceso de manera eficiente y eficaz. Los cuales se enumeran a continuación:

1. Protocolo de comunicación deficiente. Recursos humanos envía la notificación de baja de colaboradores mediante correo electrónico en horas muy tardías, por lo que el departamento de TI recibe la notificación en algunos casos el mismo día, sin embargo, en ciertos casos se debe realizar respaldo de la información del usuario y por lo tanto, la baja de accesos se realiza el siguiente día laboral. Así como también, existen casos donde la notificación de baja de colaborador es enviada los días viernes en horas de la tarde, y las bajas son recibidas por el departamento de TI hasta el día lunes de la siguiente semana. Por lo que existe tiempo suficiente para que un excolaborador, pueda comprometer las cuentas, lo que aumenta considerablemente las vulnerabilidades de seguridad y hace que la empresa sea susceptible a posibles ataques cibernéticos.
2. No se realizan respaldos periódicos y frecuentes de la información de los excolaboradores, lo cual resulta en un proceso más lento al momento de llevar a cabo su desvinculación.
3. No existe una concientización en la empresa sobre la seguridad y protección de la información, por lo que actualmente estos procesos son realizados en cualquier momento, sin considerar el posible riesgo que podría causar no dar de baja a los accesos de los usuarios en el momento oportuno.
4. No existe evidencia de que se ha dado de baja a los accesos del excolaborador, actualmente TI solo se envía una notificación mediante correo electrónico al departamento de RRHH indicando que se ha dado de baja a los accesos del usuario.
5. No se realizan auditorías periódicas para validar y confirmar que los accesos de los excolaboradores se han eliminado correctamente.

4.4 IMPROVE

En el siguiente capítulo se propondrá la implementación de soluciones efectivas que reduzcan y mitiguen los riesgos cibernéticos asociados con el proceso de baja de accesos de colaboradores que colateralmente reducirán los riesgos del proceso general de desvinculación de empleados. Es fundamental implementar un proceso eficiente y oportuno.

Por lo que se proponen las siguientes medidas:

Acciones inmediatas:

1. Establecer un protocolo para la comunicación oportuna de las solicitudes de baja de accesos.

Es importante que se realicen con suficiente anticipación para permitir un procesamiento adecuado sin afectar los plazos, para asegurarse que este proceso se realice de manera más efectiva y reduciendo riesgos de seguridad.

- El protocolo debe establecer el plazo de tiempo requerido para que el departamento de recursos humano informe al departamento de TI sobre la baja de accesos del excolaborador. Esto permitirá que el departamento de TI pueda tener tiempo suficiente para ejecutar la baja sin demoras innecesarias. Se recomienda que dicha notificación pueda realizarse en horas tempranas de la tarde.
- Dicho protocolo debe establecer los canales de comunicación adecuados para hacer la solicitud de baja de accesos. Se propone que el primer medio sea mediante llamada telefónica para notificar la hora en que se efectuara la baja del colaborador, posteriormente formalizarlo mediante la apertura de un ticket al departamento de TI.
- Se debe brindar detalle del usuario al que se dará de baja, como el nombre del empleado, número de ID, departamento al que pertenece, fecha de salida y sistemas o aplicaciones a los que se le debe dar de baja.
- Una vez que se envía la solicitud de baja de accesos, y la baja de accesos se ha realizado, el departamento de TI notificará mediante el cierre del ticket con sus respectivas evidencias.

2. Dado que actualmente el departamento de recursos humanos no cuenta con acceso a la herramienta de tickets, se deberá brindar acceso al sistema de tickets de la empresa, para que pueda realizar la solicitud de baja de accesos al departamento de TI. Esto permitirá registrar, realizar seguimiento y comunicarse de manera efectiva con el departamento de TI.
3. Revocar los accesos de manera inmediata cuando un empleado deja la organización. Esto implica que TI debe desactivar los permisos a la hora notificada por el departamento de Recursos humanos, deberá desactivar contraseñas, tarjetas biométricas y cualquier otro medio de acceso que el empleado tenga para ingresar a oficinas, sistemas, aplicaciones, redes, etc. Posteriormente a las validaciones correspondientes se procedería a realizar la eliminación del usuario.
4. Realizar los respaldos de seguridad de la información de los colaboradores de manera frecuente o periódica. Actualmente la empresa cuenta con una bitácora de respaldo, pero no existe la cultura de parte de los empleados para realizar sus backups. Por lo que se sugiere automatizar los backups, esto garantizará que la información crítica está protegida y disponible, lo que permitirá que el proceso de eliminación de accesos se pueda llevar a cabo de manera más eficiente y sin retrasos innecesarios.
 - Establecer una frecuencia de respaldos periódica, así la información estará actualizada en el servidor de backups.
 - Debe incluir todos los datos relevantes que pueda tener el colaborador en su ordenador. Para esto, primero se debe culturizar a los colaboradores sobre la clasificación de la información. Se debe indicar al colaborador bajo que dominio se deben guardar los documentos.
 - Realizar revisiones periódicas sobre los backups realizados. Con el objetivo de confirmar

- la correcta ejecución o algún error y tomar acciones.
- Realizar auditorías a los colaboradores sobre la correcta clasificación de la información.
 - Contar con un proceso claro de recuperación, esto implica tener un plan claro y documentado para restaurar en caso de pérdida o necesidad de acceso a la información que tenía el colaborador en su ordenador.
 - Establecer políticas y procedimientos claros para garantizar un manejo seguro y adecuado de los accesos a los sistemas y datos de la empresa.
 - Fomentar la importancia de contar con respaldos de seguridad de la información para todos los excolaboradores.
5. Documentar y mantener un registro actualizado de los accesos que se han eliminado, esto garantizara la gestión eficiente y a la vez cumplir con las regulaciones y auditorias.
- Es necesario tener un registro detallado de los accesos que han sido eliminados. Debe contener la fecha y hora que se llevó a cabo dicha acción, nombre del empleado, departamento al que pertenecía, sistemas asociados, responsable de la eliminación de los accesos, cualquier observación o comentario relevante. Dicha información debe proporcionar un historial completo.
 - Estos registros deben mantenerse actualizados de manera regular. Esta información será importante ante la auditoria o cualquier consulta o investigación relacionada con el manejo de accesos de la organización.
6. Realizar auditoria de cumplimiento del proceso de baja de accesos, donde se pueda validar que los accesos han sido eliminados completamente, si se ha realizado en tiempo y dentro de un SLA establecido.
- Realizar una revisión minuciosa de todos los accesos del empleado que ha dejado la organización. Revisar accesos físicos y lógicos, se deberá confirmar que todos los

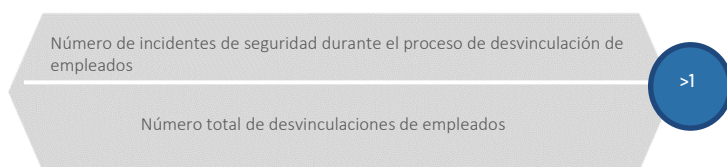
- accesos se han eliminad de manera completa y efectiva.
- Durante la auditoria se deberá documentar y registrar todas las acciones realizadas para eliminar los accesos de los colaboradores, incluyendo datos como fechas y horarios en que realizaron las bajas de los accesos, esto será importante para futuras referencias y seguimiento.
 - Verificación del cumplimiento del SLA establecido para la baja de los accesos físicos y lógicos, donde se pueda comprobar que ha cumplido con los tiempos y requisitos establecidos. Es decir, que se ha cumplido con los tiempos y procesos establecidos.
 - Realizar pruebas de verificación para confirmar que los accesos han sido eliminados correctamente, esto implica acceder a los sistemas utilizando las credenciales del excolaborador. Con el objetivo de comprobar que los accesos han sido recabados exitosamente.
 - Al finalizar la auditoria, se debe generar un informa de los detalles obtenidos- Debe incluir detalle de las acciones realizadas, hallazgos, incumplimiento del sla si existiera y sus respectivas recomendaciones.
7. Capacitación y concientización acerca de los riesgos cibernéticos y las mejores prácticas de seguridad a todos los colaboradores, independientemente de su nivel o rol en la organización, para garantizar que todos tengan acceso a la información y herramientas necesarias para protegerse. La Concientización desempeña un papel importante en la reducción del riesgo. Se necesita un firewall humano fuerte como última línea de defensa, por ello se propone la implementación de knowBe4. Es la plataforma de phishing simulada y capacitación en concienciación sobre seguridad, la plataforma ayuda a manejar el problema actual de la ingeniería social.

4.5 CONTROL

Se establecerán los siguientes KPI para analizar las mejoras implementadas. Brindará información relevante y precisa sobre la eficacia y el logro de los objetivos establecidos. Esto permitirá tomar decisiones informadas y estratégicas sobre la reducción del riesgo cibernético.

4.5.1 Incidentes de seguridad

Esta métrica cuantifica la tasa de incidentes de seguridad asociados al proceso de desvinculación de empleados es el PKI - Potencial de Incidentes de Seguridad.



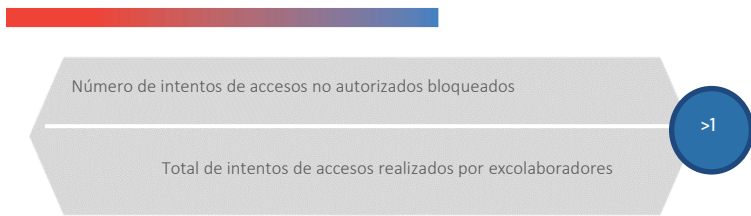
Esta KPI compara el número de incidentes de seguridad ocurridos durante el proceso de desvinculación con el número total de desvinculaciones de empleados. Proporciona una medida relativa del nivel de incidentes de seguridad asociados con la desvinculación laboral en la Tecno Solutions. Es importante mencionar que la medición precisa de la fuga de información puede ser un poco compleja, debido a que algunos incidentes pueden pasar desapercibidos o no ser detectados. Por esta razón, se ha recomendado la implantación de un sistema de monitoreo y detección adecuados, así como con la revisión y análisis de incidentes reportados o descubiertos.

4.5.2 Tasa de bloqueo de accesos. (como se puede medir este KPI)

Esta métrica evalúa la eficacia de los controles implementados para prevenir el acceso no autorizado. Esto nos demostrara la capacidad del sistema de control y monitoreo para detectar y bloquear los intentos de accesos no autorizados por parte de exempleados. Deberá ser evaluado mensualmente.

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL

LAURY FERNANDA OSORIO PAGAOGA

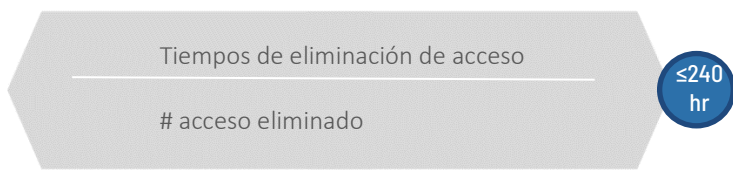


Un mayor porcentaje de bloqueo indica una mayor efectividad en la prevención de ataques cibernéticos y garantiza que los sistemas estén protegidos contra accesos no autorizados.

4.5.3 Tiempo promedio de eliminación de accesos

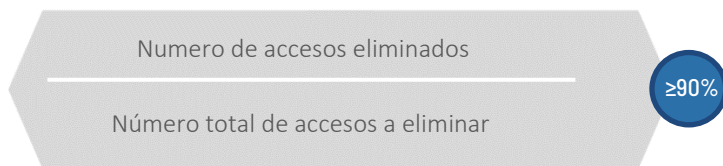
Esta métrica indica el tiempo promedio que se tarda en eliminar los accesos físicos y lógicos de un colaborador después de la desvinculación laboral

Para este KPI se establecido un SLA de 2.40 horas para la eliminación de cada acceso. Para la evaluación de este KPI, su periodicidad deberá ser mensual.



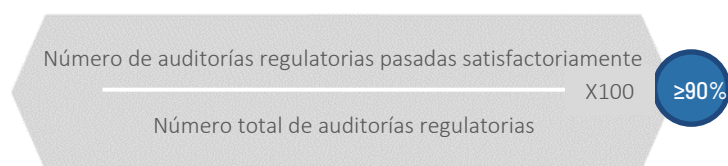
4.5.4 Tasa de eliminación de accesos completados

Esta métrica hace referencia al porcentaje de accesos que se han logrado eliminar correctamente, dentro de un periodo de tiempo, en este caso será mensual.



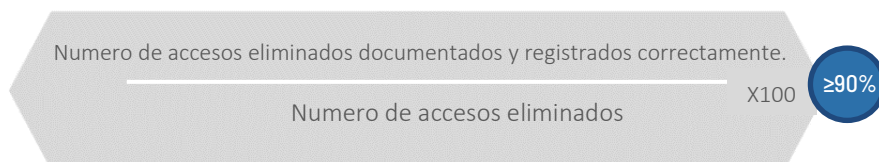
4.5.5 Tasa de auditorías regulatorias pasadas satisfactoriamente,

Este KPI nos proporciona una medida clara del número de auditorías regulatorias que han sido superadas de manera satisfactoria, específicamente para el proceso de eliminación de accesos físicos y lógicos y el de respaldos de seguridad de la información. El valor establecido para pasar satisfactoriamente es de $\geq 90\%$ e indica un buen nivel de cumplimiento regulatorio y demuestra que el departamento de TI ha cumplido con los requisitos establecidos. Deberá ser mensual.



4.5.6 Porcentaje de accesos documentados y registrados correctamente

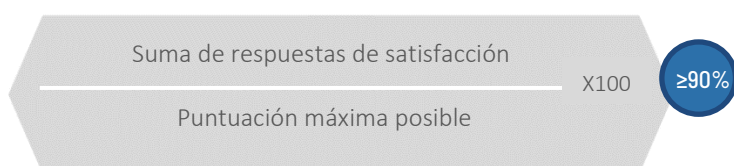
Esta métrica proporciona una medida del grado de precisión y exactitud en la documentación y registro de la eliminación de los accesos físicos y lógicos de los excolaboradores. Es muy importante que ayude a mantener una gestión correcta de la seguridad de los sistemas y protección de la información. Para ello se propone una periodicidad mensual.



4.5.7 Porcentaje de satisfacción interna

Esta métrica evalúa el nivel de bienestar, satisfacción del departamento de recursos humanos respecto al departamento de TI.

Para calcular esta métrica se propone utilizar una encuesta de satisfacción interna con preguntas relacionadas con diferentes sobre el proceso de eliminación de accesos, luego, se asigna una escala de evaluación (por ejemplo, de 1 a 5 o de 1 a 10) a cada respuesta.

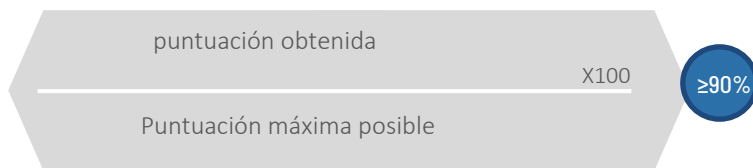


Es importante llevar a cabo encuestas de satisfacción interna de manera periódica, por lo que se propone que deben tener una periodicidad mensual, así se tomaran las acciones respectivas para mejorar continuamente.

4.5.8 Nivel de conocimiento sobre seguridad informática

Esta métrica evaluará el grado de conocimiento y comprensión que tienen los colaboradores sobre las mejores prácticas y medidas de seguridad informática. Esta métrica es importante para evaluar la capacidad de los colaboradores para proteger la información y los sistemas de la organización.

Para poder medirlo, se propone realizar una prueba, tipo test sobre el contenido impartido, que cubra diferentes aspectos de seguridad, como la gestión de contraseñas, el manejo de datos sensibles, la identificación de riesgos y amenazas, etc. Cada respuesta correcta se puntúa y se obtiene una puntuación total.



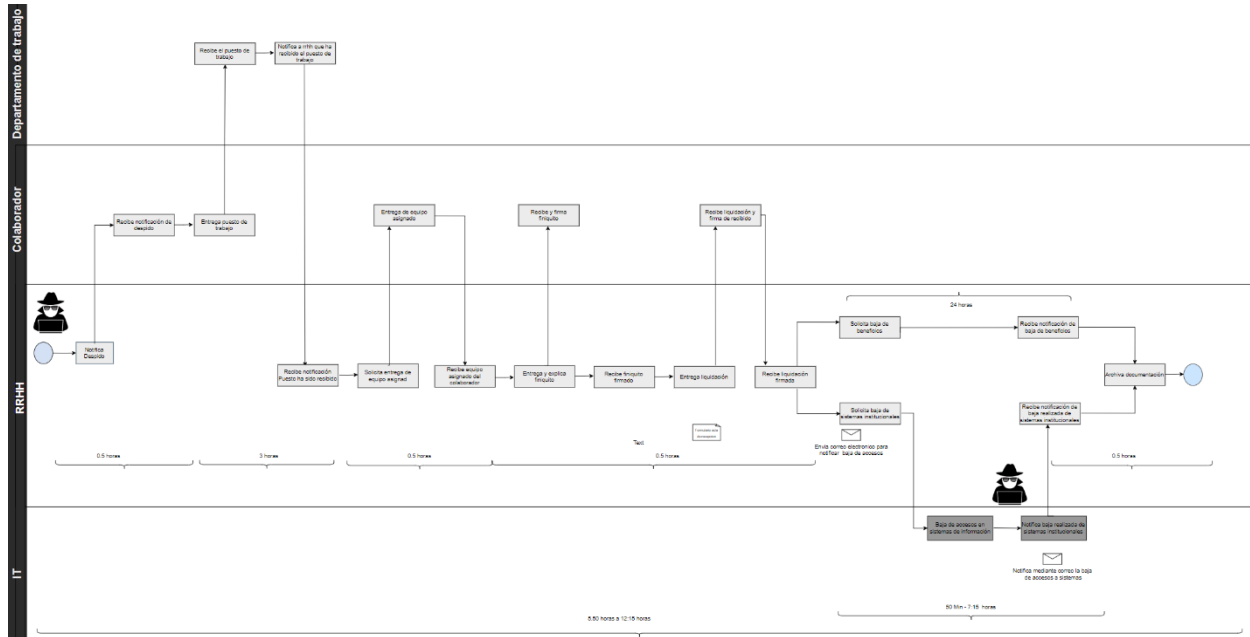
Es importante realizar hacer este tipo de evaluaciones para identificar áreas de mejora y proporcionar oportunidades de capacitación y concienciación para garantizar un nivel adecuado de conocimiento y competencia en seguridad informática en toda la organización.

CAPÍTULO 5. IMPLANTACIÓN

Durante este capítulo, se presenta una visión sobre los procesos de desvinculación laboral y subproceso de baja de accesos y como se transformarán con la implementación de las mejoras propuestas. Permitiendo una evaluación exhaustiva del impacto de las mejoras en la empresa.

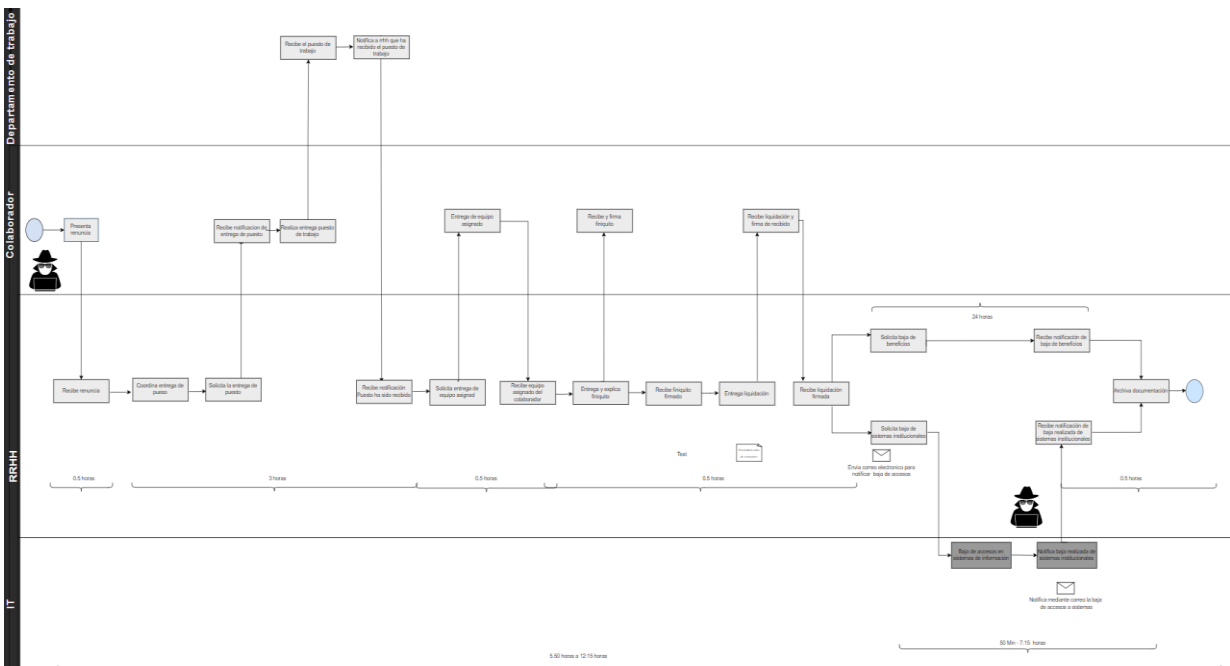
Proceso actual de desvinculación laboral, por despido.

Ilustración 15 - Proceso actual de desvinculación laboral, por despido.



Proceso actual de desvinculación labora, por renuncia

Ilustración 16 - Proceso actual de desvinculación labora, por renuncia



*En anexos se muestra este mismo diagrama en mayor tamaño para visualizarlo mejor.

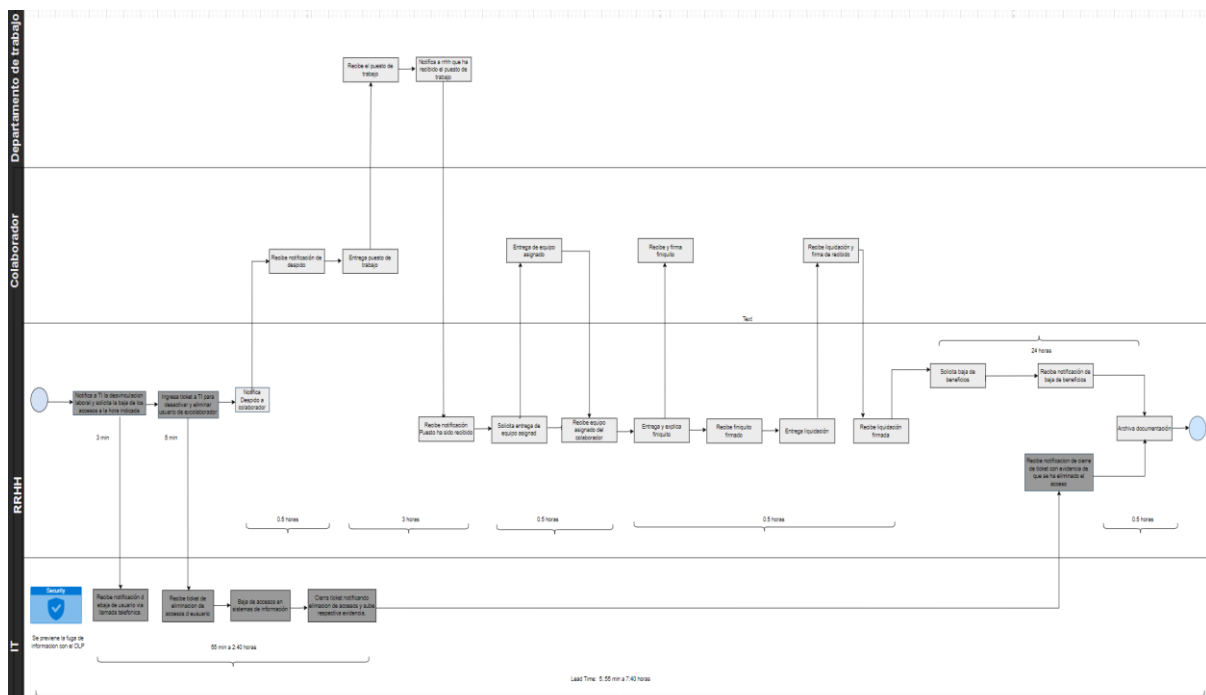
REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL
LAURY FERNANDA OSORIO PAGAOGA

Como se puede observar en ambos procesos, se identificaron vulnerabilidades que pueden ocasionar un riesgo cibernético con posibilidades de fuga y pérdida de información crítica para la empresa, daños de reputación y costos financieros.

1. Riesgo cibernético desde el momento en que el colaborador puede extraer información de la empresa previo o durante la separación laboral.
2. Riesgo ocasionado en el proceso de desvinculación de colaboradores está tomando en promedio 5:50 horas a 12:15, esto principalmente porque el subproceso de baja de accesos está tomando un tiempo importante, lo que causa que los excolaboradores pudieran tener acceso a la información sin autorización.

Propuesta de proceso de desvinculación laboral por despido

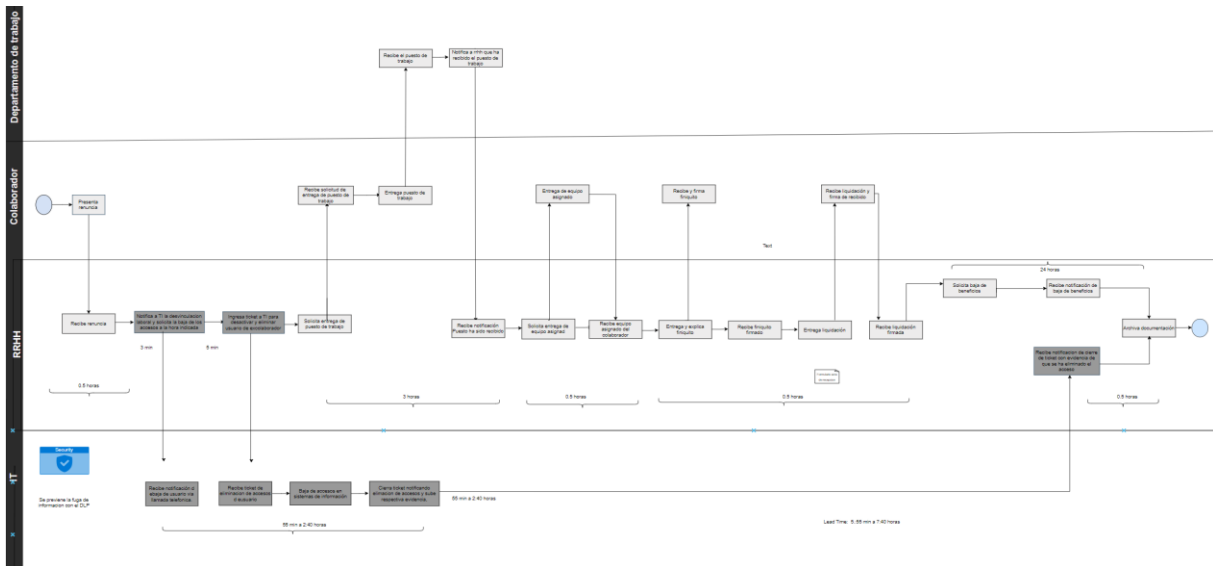
Ilustración 17 - Propuesta de proceso de desvinculación laboral por despido



*En anexos se muestra este mismo diagrama en mayor tamaño para visualizarlo mejor.

Propuesta de proceso de desvinculación laboral, por renuncia

Ilustración 18 - Propuesta de proceso de desvinculación laboral, por renuncia



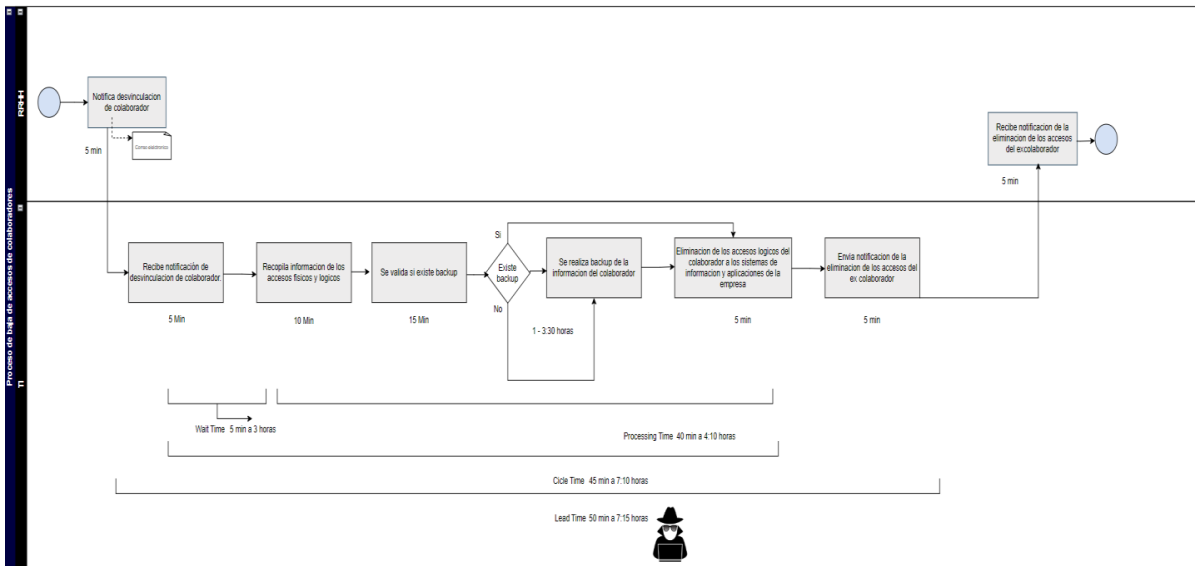
*En anexos se muestra este mismo diagrama en mayor tamaño para visualizarlo mejor.

Como se puede notar, en ambos procesos de desvinculación laboral, se han mejorado los siguientes aspectos importantes, con el objetivo de tener una postura de seguridad sólida y así mitigar los riesgos asociados a las amenazas cibernéticas.

1. Para reducir riesgo cibernético. Se propuso la implementación de un DPL (data loss prevention), así como también se propuso la concientización a los colaboradores sobre seguridad informática, reduciendo notablemente las posibilidades de fuga y pérdida de información crítica para la empresa, daños de reputación y costos financieros.
2. Se eficientiza y se reduce notablemente el tiempo que está tomando dicho proceso actualmente. El lead time ahora es de 5.50 horas a 12:15 horas, con las mejoras sugeridas, el lead time pasaría a ser de 5:55 min a 7:40 horas, reduciendo el tiempo máximo de este proceso en un 39%.
3. Con la implementación de acuerdos de confidencialidad y competencia se reducen considerablemente los riesgos legales que podrían existir en el proceso de desvinculación laboral.
4. Con la concientización de los colaboradores y formación sobre seguridad informática propuesta, se obtendrán beneficios como, reducir los incidentes de seguridad, promover la cultura de seguridad, cumplir con los requisitos establecidos, mejorar la respuesta ante incidentes y proteger la reputación y confianza de la empresa.

Proceso actual de baja de accesos de colaboradores

Ilustración 19 - Proceso actual de baja de accesos



*En anexos se muestra este mismo diagrama en mayor tamaño para visualizarlo mejor.

Como se puede percibir, en el subproceso de baja de accesos, se identificaron vulnerabilidades que abren puertas para una posible fuga de información un ataque cibernético. Que podrían causar daños grandes a la operación de la empresa, afectando fuertemente la reputación y generando grandes costos financieros.

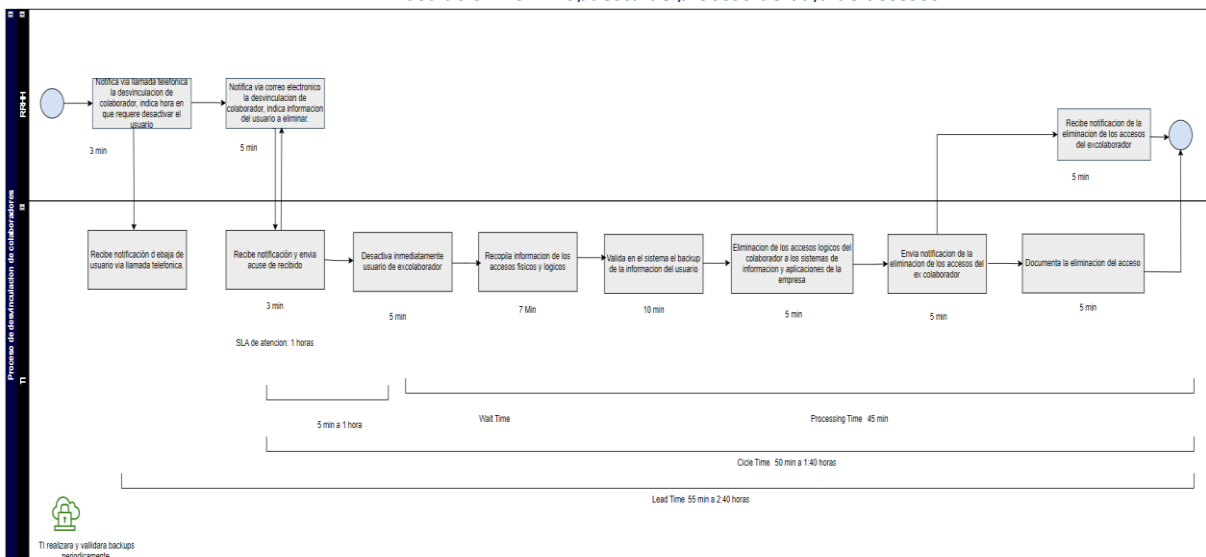
1. Riesgo cibernético debido a que la baja de los accesos físicos o lógicos está tomando un tiempo importante, según el proceso actual debería demorar entre 5.50 horas a 7:15 horas, sin embargo, en la realidad se han tenido tiempos de 65.25 horas., lo cual permite que el excolaborador pueda tener sus accesos físicos y lógicos activos aun terminada la desvinculación laboral. Lo cual permite acceso no autorizado a sistemas y otros datos sensibles y pueda hacer mal usos de sus privilegios para llevar a cabo acciones maliciosas o dañinas dentro de los sistemas de la empresa, esto puede incluir, alteración de datos, manipulación de configuraciones de los sistemas, realizar ataques de phishing dirigidos o comprometer la seguridad en general.
2. Se identificó que el 62% de las solicitudes de baja de accesos esta fuera de lead time y solamente un 28% de las solicitudes se están realizando dentro de los tiempos establecidos.

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL LAURY FERNANDA OSORIO PAGAOGA

3. De igual forma, se idéntico que el 70% del tiempo del proceso está en el wait time, tiempo que tarda en ser atendida la solicitud y solo un 30% del tiempo lo tiene la ejecución de la baja de los accesos físicos y lógicos, esto debido principalmente a que las solicitudes de baja de accesos realizadas por recursos humanos están llegando en los tiempos incorrectos causando que el departamento de TI no pueda gestionarlas en el momento oportuno, extendiendo así los tiempos para el subproceso de eliminación de accesos.

Propuesta de proceso de baja de accesos de colaboradores

Ilustración 20 - Propuesta de proceso de baja de accesos



*En anexos se muestra este mismo diagrama en mayor tamaño para visualizarlo mejor.

Como se puede apreciar, se han realizado mejoras significativas en el proceso de baja de accesos, con el fin de hacer el proceso más eficiente y con el propósito de fortalecer la postura de seguridad, mitigando los riesgos inherentes a las amenazas cibernéticas.

1. Se estableció un protocolo para la comunicación oportuna de las solicitudes de baja de accesos. Realizando primeramente una llamada telefónica, notificando al departamento de TI la hora en que habrá una baja de colaborador, y posteriormente el ingreso de un ticket con los datos requeridos. Reduciendo así el wait time en un 66%.
2. Revocar los accesos de manera inmediata, ayudara a proteger la información confidencial, mitigara los riesgos de posibles actividades maliciosas o acciones no autorizadas por parte de excolaboradores, protegiendo así la reputación y confianza de los empleados, clientes o socios

- comerciales, ya que demuestra una postura de responsabilidad hacia los datos de la organización.
3. Al realizar respaldos de seguridad de información de colaboradores de manera periódica, ayudará que el proceso de baja de accesos sea más rápido y por ende, eficiente, dado a que no se tendrá que realizar esta actividad en el momento exacto de la eliminación de los accesos.

Actualmente el proceso debería durar un máximo de 4:10, sin embargo, se podría reducir hasta un límite máximo a 45 minutos, mejorando los tiempos del procesing time en un 82%.
 4. Actualmente su leadtime tiene como límite máximo 7:15 horas, sin embargo la realidad es que 61% de los casos analizados están por fuera de ese límite, en un rango de 14 hasta 65 horas, con un promedio de 24 horas con 8 minutos. Con todas las mejoras propuestas el leadtime del subproceso de baja de accesos físicos y lógicos se establezca dentro de del límite máximo de 2:40 horas. Mejorando considerablemente este valor en un porcentaje de 63% y por ente reduciendo de una manera importante los riesgos cibernéticos asociados a dicho proceso.
 5. Para el cumplimiento normativo de auditorías, se ha sugerido mantener una documentación correcta y registro actualizado de los accesos que se han eliminado y de los backups realizados. Las auditorías para el control de baja de accesos de empleados y la realización de backups auditorías son una herramienta fundamental para garantizar una gestión adecuada de los accesos y los respaldos, y para mantener la seguridad de la información en la organización. Ayudaran para el cumplimiento normativo, la identificación de riesgos, la mejora de los procesos, la protección de la información, la generación de confianza y una mejor toma de decisiones.
 6. Otra de las mejoras propuestas es la capacitación y concienciación de los empleados sobre seguridad de la información, mediante la plataforma KnowBe4. Ayudará a fortalecer la seguridad de los datos, reducir los incidentes de seguridad, promover una cultura de seguridad, mejorar la respuesta ante incidentes y cuidar la reputación y la confianza de la organización.

CAPÍTULO 6. PLAN FINANCIERO

6.1 Valoración del riesgo financiero sin herramientas y conocimiento de protección de seguridad informática.

Para poder realizar una valoración del riesgo cibernético sin la implementación de medidas y herramientas, se tomaron 3 posibles escenarios y el impacto financiero, reputacional, afectación de imagen que la empresa podría tener nivel de imagen frente al mercado, aliados, clientes y proveedores, además de la pérdida de confianza.

Puesto estratégico

Se ha dado una desvinculación laboral con alto ejecutivo, quien tenía acceso a información estratégica confidencial, obtuvo datos privilegiados sobre un proyecto en curso para proporcionar servicios de cable e internet en una urbanización residencial exclusiva, ubicada en una zona prestigiosa de la ciudad. Este proyecto tenía como objetivo brindar servicios a 300 casas, con un precio establecido de \$80 por paquete de cable e internet.

Lamentablemente, el ejecutivo tomo de forma desfavorable la desvinculación laboral con Tecno Solutions y decidió unirse a una empresa competidora. Sin escrúpulos, reveló el secreto comercial que había obtenido durante su empleo en Tecno Solutions. Este acto de traición y competencia desleal ha causado un daño significativo a Tecno Solutions, ya que su competidor ahora tiene acceso a información privilegiada y puede utilizarla para ganar una ventaja injusta en el mercado.

Como consecuencia directa de esta revelación de información confidencial, Tecno Solutions enfrenta pérdidas sustanciales. Su competidor puede aprovechar la información sobre el proyecto en la urbanización residencial en crecimiento, dirigirse directamente a los clientes y ofrecer servicios similares a precios más competitivos. Además, el competidor puede personalizar sus ofertas y utilizar el conocimiento adquirido para socavar la posición de Tecno Solutions en el mercado, atrayendo a los

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL
LAURY FERNANDA OSORIO PAGAOGA

clientes y perjudicando su crecimiento y rentabilidad.

La traición del ejecutivo y su transferencia de conocimientos a la competencia han causado un daño significativo a Tecno Solutions, erosionando su ventaja competitiva y generando pérdidas económicas:

Tabla 2 - Riesgo financiero de un Puesto estratégico

Casas	Precio por paquete x mes	Precio de maquete anual	Pérdida Anual
300	\$40	\$480	\$144,000.00

Puesto comercial

Un empleado de ventas labora para Tecno Solutions. Durante su tiempo en la empresa, tiene acceso a una base de datos confidencial que contiene información detallada de los clientes, como nombres, direcciones, números de teléfono y hábitos de consumo.

El colaborador ha terminado la relación laboral con Tecno Solutions y decide llevar a cabo una acción deshonesta y roba la base de datos de clientes de la empresa antes de dejar su puesto. Aprovechando su nuevo empleo en la empresa competidora del mismo sector, el utiliza la información de la base de datos robada para su beneficio personal y el de su nueva empresa.

Con esta información privilegiada, el colaborador y su nueva empresa pueden dirigirse directamente a los clientes de la empresa anterior, ofreciéndoles servicios similares a precios más competitivos o promociones exclusivas. Al tener acceso a los datos de contacto y los hábitos de consumo de los clientes, el excolaborador y su nueva empresa pueden personalizar sus ofertas para atraer a estos clientes y ganar su negocio.

Este comportamiento desleal por parte del excolaborador representa una violación de la confianza y la ética empresarial. Además, perjudica a la empresa original al perder clientes y enfrentar una competencia desleal, causando así una pérdida financiera.

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL
LAURY FERNANDA OSORIO PAGAOGA

- Los ingresos aproximados de la empresa están en \$5,000,000.00 anuales.
- Se considero una perdida financiera por perdida de clientes de un 10% sobre el total de la facturación.

Tabla 3 - Riesgo financiero de un Puesto Comercial

Ingresos anuales aproximados de la empresa	Pérdida de clientes y facturación por fuga de información	Perdida financiera
\$5,000,000	10%	\$500,000.00

Puesto operacional

1. HFC Support, 1st line.

Un colaborador ocupa el puesto de HFC Support en la ciudad de Tegucigalpa, donde tiene acceso limitado a los CMTS (Cable Modem Termination Systems) de dicha localidad. Este acceso implica ciertos privilegios, siendo el más crítico la capacidad de apagar los nodos.

En concreto, el colaborador cuenta con acceso a 4 CMTS de la ciudad, los cuales son responsables de gestionar hasta 30 nodos cada uno en Tegucigalpa. Cada nodo proporciona servicio a un promedio de 300 usuarios.

Sin embargo, debido a su desvinculación laboral reciente y su estado emocional alterado, el colaborador toma una decisión inapropiada. Aunque ha terminado su relación laboral, sus accesos no han sido eliminados y aun puede ingresar a los equipos de red. Decide acceder a los CMTS a los que tenía acceso y apagarlos, lo que resulta en la interrupción del servicio de 2 horas para todos los usuarios que dependían de estos nodos para recibir su conexión de Internet.

Es importante destacar que este comportamiento es altamente perjudicial, ya que afecta a un gran

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL
LAURY FERNANDA OSORIO PAGAOGA

número de usuarios que dependen de la conexión a Internet para sus actividades diarias. Además, compromete la integridad, imagen y la reputación de la empresa Tecno Solutions, así como una afectación financiera por compensación de 12% por cada hora de indisponibilidad de servicio.

Disponibilidad del servicio ofrecido por debajo del 99.9% Mensual
Con base al cálculo descrito en el apartado del mismo nombre, Tecno Solutions se obliga a pagar al cliente (x) como pena convencional una compensación financiera equivalente al 12% sobre el monto de la facturación total mensual de los servicios contratados por cada hora de indisponibilidad excedida con base a la disponibilidad mensual ofrecida.

Tabla 4 - Riesgo financiero de un puesto de HFC Support, 1st line.

CMTS/Nodos	Usuarios afectados	Precio del servicio mensual	Penalización	Valor de la penalización	Perdida financiera por afectación de servicio al mes
4/30	36,000	\$40	12%	\$4.8 por hora \$9.6 por 2 horas	\$ 345,600.00

2. Ingeniero de red Core

Un colaborador, con el cargo de Ingeniero de red Core, tiene acceso a todos los equipos core de la red instalada en el país. Sus privilegios incluyen la capacidad de crear, modificar y eliminar configuraciones en dichos equipos.

Recientemente, el colaborador ha sido despedido de la empresa, pero sus accesos no han sido eliminados. Como resultado, se encuentra molesto y decide tomar acciones inapropiadas. Accede al router core principal y su respaldo, donde se conectan los CMTS de todo el país y decide apagarlos.

Es importante destacar que el departamento de redes tenía una política establecida para realizar respaldos de seguridad de las configuraciones de los equipos de red. Este respaldo es crucial para garantizar una rápida recuperación en caso de incidentes.

En este caso, el colaborador tiene acceso a un total de 7 CMTS en todo el país. Cada CMTS

puede gestionar hasta 30 nodos, los cuales brindan servicio a un promedio de 300 usuarios por nodo.

Es importante resaltar que, en caso de interrupción del servicio, el tiempo máximo de recuperación es de 3 horas, y tiene una compensación de 12% por cada hora de indisponibilidad de servicio.

La situación planteada es sumamente grave, ya que el acceso no autorizado y las acciones del colaborador ponen en riesgo la integridad de la red y afectan a los usuarios que dependen de los servicios. Afectando la integridad y la reputación de la empresa Tecno Solutions. Supone una penalización que se convierte en una pérdida financiera para la empresa de:

Tabla 5 - Riesgo financiero de un puesto de Ingeniero de red core

CMTS/Nodos	Usuarios afectados	Precio del servicio mensual	Penalización	Valor de la penalización	Perdida financiera por afectación de servicio al mes
7/30	63,000	\$40	12%	\$4.8 por hora \$14.4 por 3 horas	\$ 907,200.00

6.2 Inversión Inicial para la implementación de mejoras para reducción de riesgo cibernético en el proceso de desvinculación laboral.

Es necesario implementar medidas sólidas de seguridad y salvaguardar la información confidencial para evitar situaciones similares en el futuro. Por lo que se proponen las siguientes herramientas:

1. Generar accesos al departamento de recursos humanos para la plataforma de tickets.

Esta solicitud implica solicitar al proveedor de la solución que pueda ingresar los nuevos parámetros del proceso. El tiempo estimado para completar esta tarea es de 7 horas, con una tarifa de lempiras por hora.

REDUCCIÓN DEL RIESGO CIBERNÉTICO EXISTENTE EN UN PROCESO DE DESVINCULACIÓN LABORAL
LAURY FERNANDA OSORIO PAGAOGA

Tabla 6 - Inversión - Generación de accesos a herramienta de tickets

Descripción	Horas	Precio	Total
Desarrollo de proceso dentro de herramienta de tickets	7 horas	\$90	\$630

2. La plataforma phishing simulada y capacitación en concienciación sobre seguridad, KnowBe4, es necesaria para proteger a los empleados de posibles ataques de phishing y concientización sobre la protección de los datos. Se requieren 190 licencias para los colaboradores, el costo de cada licencia es de \$0.90 por mes, lo que resulta en un total de \$10.8 por año.

Tabla 7 - Inversión en plataforma Knowbe4

Descripción	Licenciamiento	Precio	Total
Plataforma Knowbe4	190	\$10.8	\$2,052.00





3. Implementación de Forcepoint DLP. Forcepoint DLP es un software DLP repleto de funciones que ofrece una detección de precisión del 100% a través de huellas dactilares. Ofrece características útiles como la gestión de incidentes / amenazas web y la identificación y prevención de fuga de datos confidenciales.

Se requieren 190 licencias, a un precio de \$12 por licencia por mes, haciendo una inversión total de \$2900 mensuales.

Tabla 8 - Inversión en Forcepoint DLP

Descripción	Licenciamiento	Precio	Total
Forcepoint DLP	190	\$144	\$27,360

CUANTIFICACIÓN DE LOS RIESGOS CIBERNÉTICOS ASOCIADOS AL PROCESO DE DESVINCULACIÓN LABORAL

Puesto estrategico		\$144,000
Puesto Comercial		\$500,000
Ingeniero soporte 1ra linea		\$345,600
Ingeniero red core		\$907,200

6.3 Impacto financiero por riesgo cibernético VS inversión en herramientas

para reducir el riesgo cibernético

6.3.1 Impacto financiero por un riesgo cibernético

Tabla 9 - Impacto financiero por un posible riesgo cibernético asociado a un puesto laboral

Escenarios de riesgo cibernético	Perdida financiera
Puesto comercial	\$500,000.00
Soporte primera linea	\$345,600.00
Ingeniero red core	\$907,200.00
Puesto estrategico	\$144,000.00

6.3.2 Inversión para prevenir el riesgo cibernético

Tabla 10 - Inversión para reducción del riesgo cibernético

Herramienta o solución para disminuir el riesgo cibernético	Total, anual
Desarrollo de proceso en herramienta de tickets	\$ 630.00
Plataforma Knowbe4	\$ 2,052.00
Forcepoint DLP	\$ 27,360.00
Inversion total	\$ 30,042.00

*No se incluyen costos por automatización de backups, realización de protocolos y documentación, se consideran como parte de las labores o funciones de cada departamento.

6.3.3 Grafico de Inversión en seguridad VS Impacto financiero por riesgo cibernético

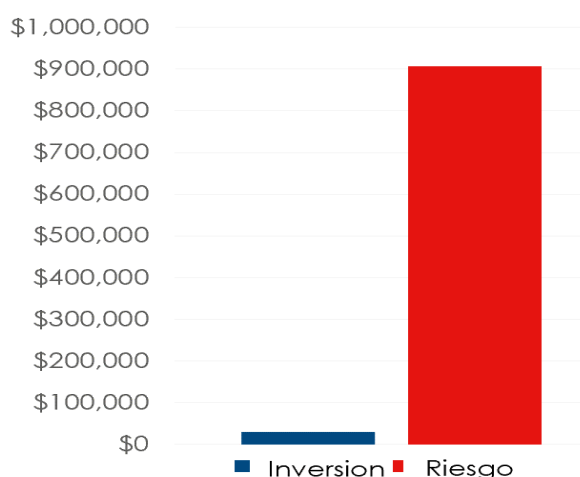
Resumen

Inversion en Ciberseguridad

\$30,042

Riesgo financiero por falta de ciberseguridad

\$907,200



*Se tomo el riesgo con mayor impacto financiero para poder hacer la comparativa, con el fin de mostrar la mayor pérdida económica que sufriría la empresa comparada con la poca inversión anual necesaria.

*La inversión para el desarrollo del proceso de tickets solo será el primer año.

*Calculos realizados en moneda dólar, segunda moneda mas utilizadas en honduras.

CAPÍTULO 7. LEGAL

7.1 La Protección de Datos en Honduras.

Según (Zelaya, 2021) En el artículo 76 de la Constitución de la República se establece el derecho al honor, la intimidad personal, familiar y la propia imagen, mientras que en el artículo 100 se establece que "toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones... salvo resolución judicial... los documentos personales solo estarán sujetos a inspección o fiscalización de la autoridad competente". De esta manera, establecen una base desde la cual parten los derechos de protección de datos.

El mismo cuerpo legal en su artículo 182 numeral 2, (Zelaya, 2021) destaca que existe la Garantía Constitucional del Habeas Data, que no solo es el reconocimiento de un derecho establecido en nuestra Carta Magna, sino también una medida para hacer efectivo este derecho de manera inmediata en caso de que se transgreda, estableciendo un mecanismo que permite la acción inmediata sin formalidades ni obstáculos.

Como lo menciona (Zelaya, 2021) Es notable que Honduras enfrenta una gran cantidad de desafíos prácticos y técnicos para proteger sus derechos de protección de datos. Aunque son reconocidos, la finalidad absoluta del derecho es hacerlos efectivos y eficaces, pero no se cuenta con los instrumentos, mecanismos y cultura social para lograrlo.

Proyecto de Ley de Protección de Datos

Según (Zelaya, 2021), Durante el mes de abril de 2018, el Congreso Nacional de Honduras ha estado posponiendo el tercer y último debate para aprobar el proyecto de Ley de Protección de Datos Personales. El hecho de que Honduras no tenga una ley que proteja los datos personales hace que este proyecto tenga ventajas, ya que las definiciones y métodos son novedosos. Sin embargo, algunos

conceptos son propensos a malinterpretaciones o carecen de un buen desarrollo conceptual, lo que puede llevar a la posibilidad de cometer actos arbitrarios.

Definiciones y Principios

Conforme a (Zelaya, 2021) Las definiciones y principios de este proyecto son abiertos y se enfocan en no limitar lo que se considera como datos personales para evitar que cualquier acción sea imposible de llevar a cabo porque no está definido como el bien jurídico a proteger. Principios tales como:

1. Principio de Finalidad de Propósitos
2. Principio de Acceso a la Información
3. Principio de Seguridad
4. Principio de Confidencialidad
5. Buscan que haya transparencia, garantía y propósito cuando un ente de carácter público o privado solicite información de un particular.

Derechos ARCOS y sus Mecanismos de Acción

De acuerdo con (Zelaya, 2021)El propósito de los Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) en este proyecto es garantizar que el titular pueda acceder a la información que conste sobre su origen, cómo se trata, si ha sido cedida previamente o si tiene la intención de cederla a terceros. Los derechos enumerados a continuación son:

1. Derecho de Acceso
2. Derecho de Rectificación
3. Derecho de Cancelación
4. Derecho de Oposición

Asimismo, (Zelaya, 2021) menciona que el titular de la información tiene la capacidad de ejercer su derecho constitucional de protección de sus datos personales mediante la implementación de mecanismos como los siguientes:

Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Entrega de información sobre datos personales.

Mecanismos de Comunicación

Consentimiento en la Cesión de datos a terceros.

Contraposiciones del Proyecto de Ley

De acuerdo con (Zelaya, 2021), el artículo 5 establece excepciones a las definiciones y principios mencionadas anteriormente, que buscan asegurar la transparencia, las garantías y el propósito en el manejo de datos de los titulares. Lo que consideramos que causa agravios no es la existencia de las excepciones en sí, sino la amplitud de su definición y la falta de un fundamento legal que determine que existe un derecho superior que lo sustenta por sobre el derecho particular y por el cual debe respetarse. Esto se presta a la malinterpretación y puede ser utilizado de forma arbitraria sin ninguna regulación.

Asimismo, según (Zelaya, 2021), Honduras ha tenido experiencias desfavorables con el abuso justificado de legislaciones que buscan "la protección del Estado" o "la seguridad nacional". La Ley de Intervención de las Comunicaciones es un ejemplo de esto, ya que el artículo 46 literal a del Proyecto de Ley de Protección de Datos establece que "La cesión debe ser autorizada por una ley", lo que respalda esta afirmación. En este caso, no consideramos que el problema sea la existencia de la excepción en sí, sino que carece de una redacción más precisa o mecanismo que apoye su función de protección contra el cumplimiento de otras legislaciones. La ley establece una fecha límite para que el sector privado implemente políticas de protección de datos efectivas, con un enfoque particular en el sector bancario. No obstante, es crucial en el sector público promover una cultura interinstitucional

de protección de datos, capacitando y buscando la transparencia en el actuar de cada una, más que establecer una Institución Garante de estos Derechos con capacidades reales de ejercitar las acciones pertinentes, si es que el Instituto an Acceso de la Información Publica puede serlo.

En palabras de (Zelaya, 2021), cuando las tecnologías superan la capacidad técnica, práctica y de conocimiento para crear políticas y legislación efectivas en este tema, hay mucho más por desglosar en este proyecto de protección de datos. Es innegable que el resto del mundo reconoce la relevancia de la protección de datos, ya que nos encontramos en la era de la información y el conocimiento. Es fundamental comenzar a discutir los temas cruciales de protección de datos y mejorar en función de nuestras circunstancias en Honduras.

CAPÍTULO 8. CONCLUSIONES Y FUTURAS LINEAS DE TRABAJO

8.1 Conclusiones:

Después de analizar el proceso de desvinculación laboral, con el objetivo de reducir los riesgos cibernéticos asociados, se concluye lo siguiente:

1. Actualmente Tecno Solutions se encuentra muy vulnerable ante fuga de información y ataques cibernéticos, causado por tener un proceso de desvinculación laboral con brechas de seguridad. Se identifico que estas brechas vienen de dos puntos importantes:

- Proceso de desvinculación ineficiente, con una gestión y comunicación deficientes entre las áreas involucradas al momento de dar de baja los accesos físicos y lógicos de los excolaboradores.
- Falta de herramientas para monitorear y proteger el activo más valioso: la información.

Con la implementación de medidas y herramientas propuestas, el proceso de desvinculación se vuelve eficiente y seguro, logrando reducir el lead time en un 39%.

Ocurriendo lo mismo con el subproceso de baja de accesos, donde se logro reducir el lead time en un 60%

2. La propuesta de protocolos y documentación del proceso ayudara a la empresa a tener un proceso de desvinculación laboral con mayor consistencia y estandarización, además ayudara a Tecno Solutions en su preparación para la certificación ISO.
3. Para evaluar y gestionar eficazmente la seguridad informática en Tecno Solutions, es fundamental tener en cuenta dos aspectos, las personas y los datos. Por lo tanto, respecto a las personas, es indispensable que Tecno Solutions invierta en educación y concientización

sobre seguridad de la información. Con ello se podrá prevenir amenazas internas y externas y fortalecer la postura de ciberseguridad, asegurar la confidencialidad, integridad y disponibilidad de los datos, prevenir accesos no autorizados, mitigar riesgos legales, reputacionales y financieros.

4. Es crucial que Tecno Solutions invierta en soluciones de ciberseguridad para reducir el riesgo cibernético asociado al proceso de desvinculación laboral. La inversión necesaria en seguridad informática es menor, en comparación con los altos beneficios como la seguridad de la empresa y sus activos digitales y sobre todo con la reducción del alto riesgo cibernético y el impacto financiero que podría sufrir al no contar con medidas adecuadas.

5. Los costos de implementar medidas de seguridad cibernética fueron evaluados en relación con los posibles beneficios y ahorros que se obtendrán a largo plazo. Esto ayuda a asegurar que las inversiones realizadas en seguridad sean sostenibles desde el punto de vista económico.

Como conclusión, el proyecto ha logrado abordar satisfactoriamente las preguntas de investigación y alcanzar los objetivos establecidos al inicio del documento.

8.2 Futuras Líneas:

Este estudio tiene como objetivo servir de punto de partida para analizar los riesgos cibernéticos en diferentes áreas de la empresa y proporcionar una guía para implementar soluciones que aseguren las operaciones. Además, se recomienda evaluar el impacto en la imagen y reputación de la empresa debido a los riesgos cibernéticos. También se sugiere explorar la viabilidad de utilizar herramientas de machine learning para detectar amenazas en tiempo real en redes internas y externas, centros de datos, sistemas virtuales y web, con el fin de mejorar la protección y la eficiencia del sistema de ciberseguridad.

CAPÍTULO 9. ANEXOS

Anexo 1 – Correo electrónico para solicitar baja de accesos.

Correo enviado por Talento Humano, notificando la desvinculación laboral. Dicha notificación sirve a la vez como solicitud de eliminación de accesos físicos y lógicos del excolaborador. Donde se puede notar que es enviado fuera de horario laboral, por lo que el departamento de TI procederá a realizar la baja de accesos al día siguiente.

DESVINCULACIÓN LABORAL



Talento Humano

Para [redacted]

Si hay problemas con el modo en que se muestra este mensaje, haz clic aquí para verlo en un explorador web.



miércoles 1/2/2023 18:27

Buenas tardes estimados colaboradores:

Por este medio se notifica que dejo de laborar para [redacted] la ex colaboradora:

- [redacted] - SOPORTE DE DATA CENTER S.P.S

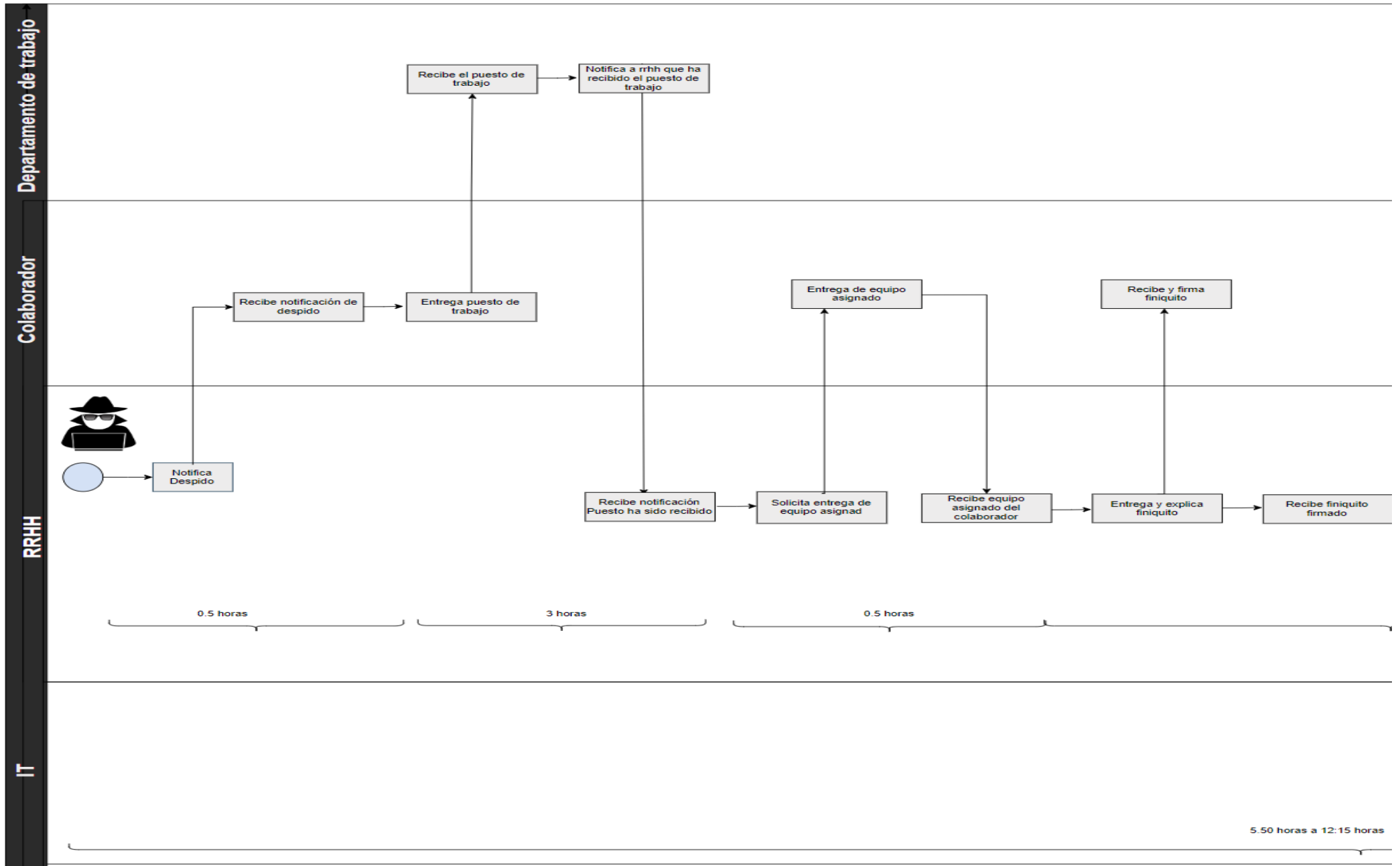
Le agradecemos el tiempo que laboró para la empresa, deseándole éxitos en sus nuevos emprendimientos personales y profesionales.

Favor tomar nota...

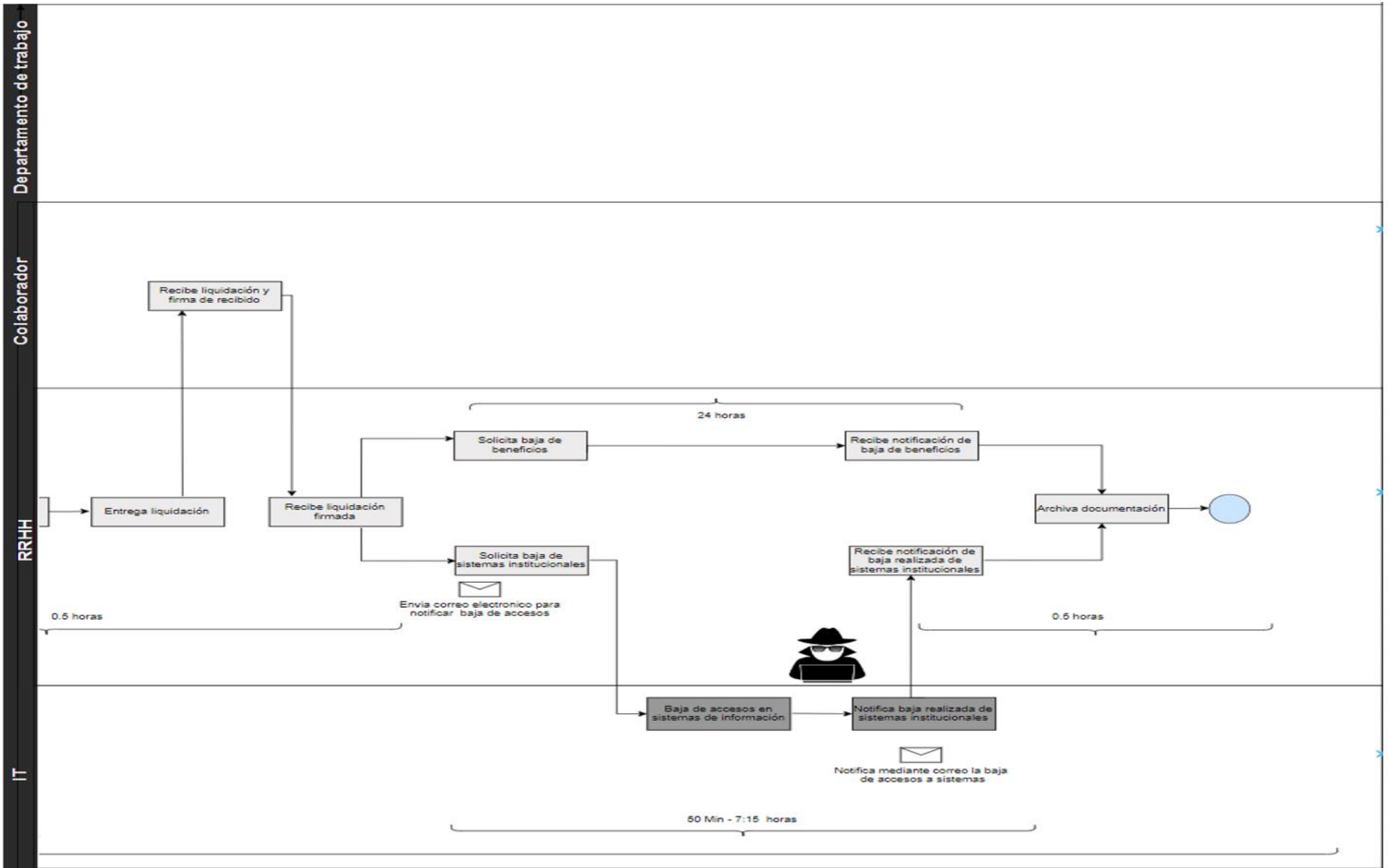
¡Saludos!

Fuera de horario laboral

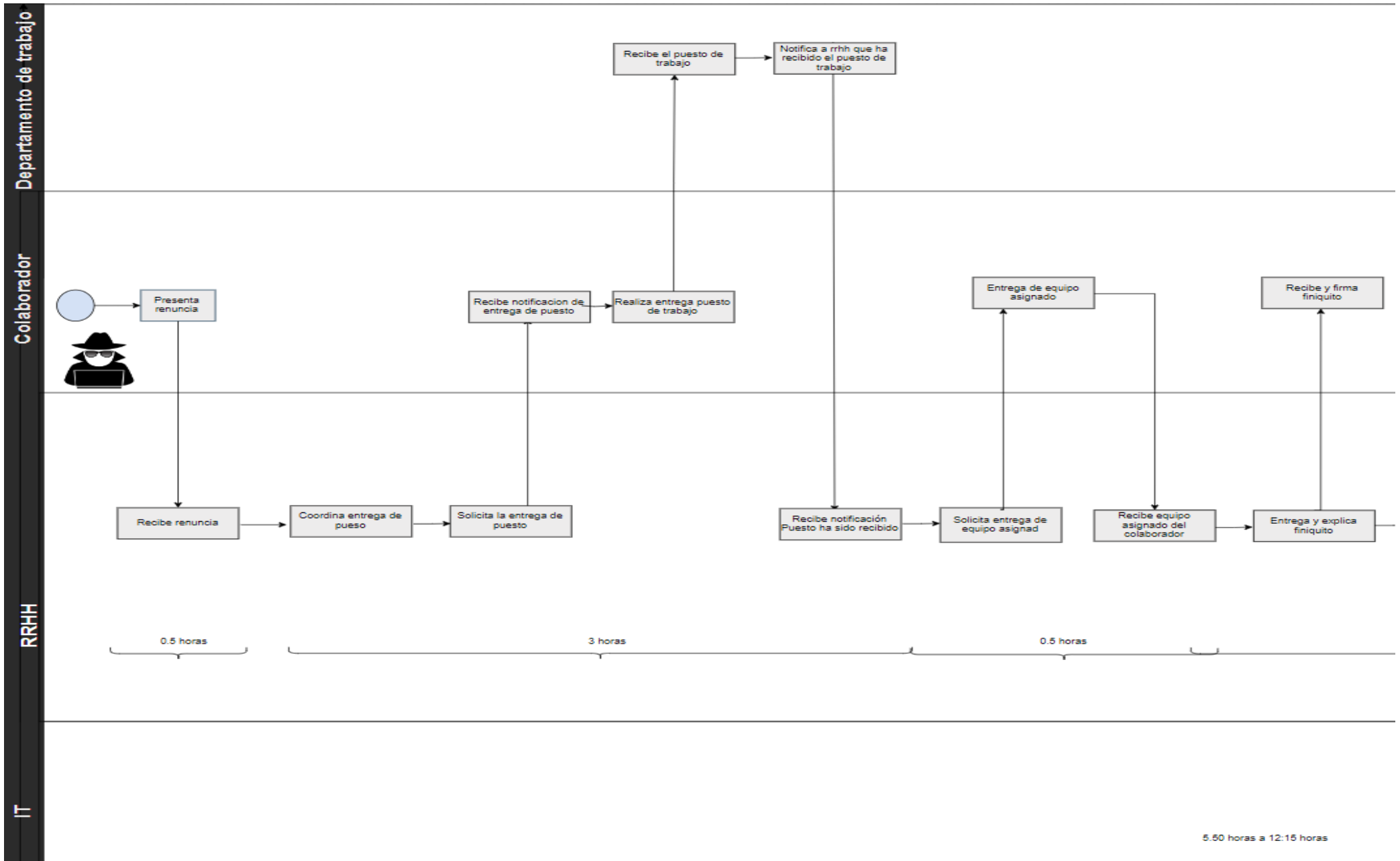
Anexo 2 - Proceso actual de despido parte 1.



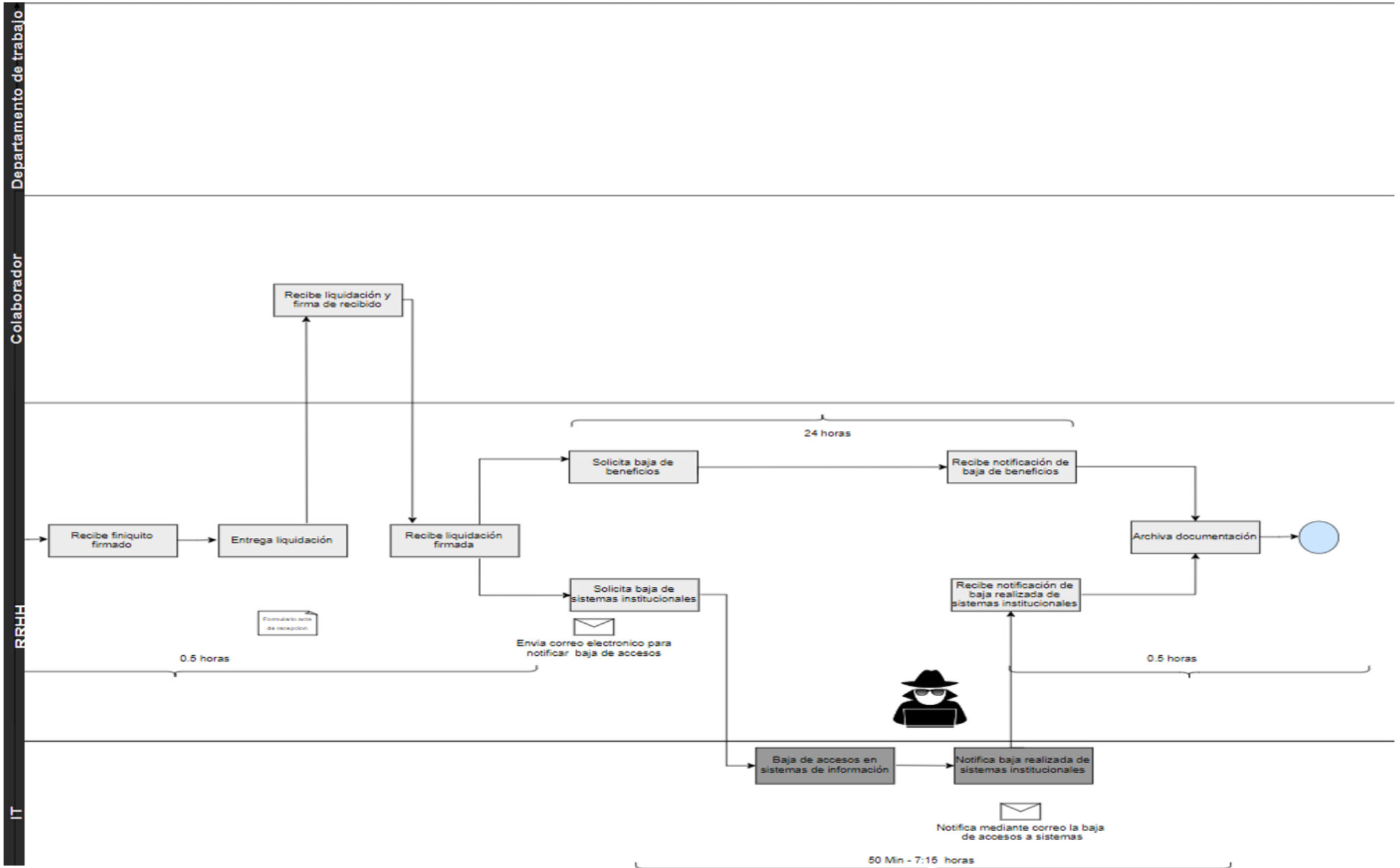
Anexo 3 - Proceso actual de despido parte 2



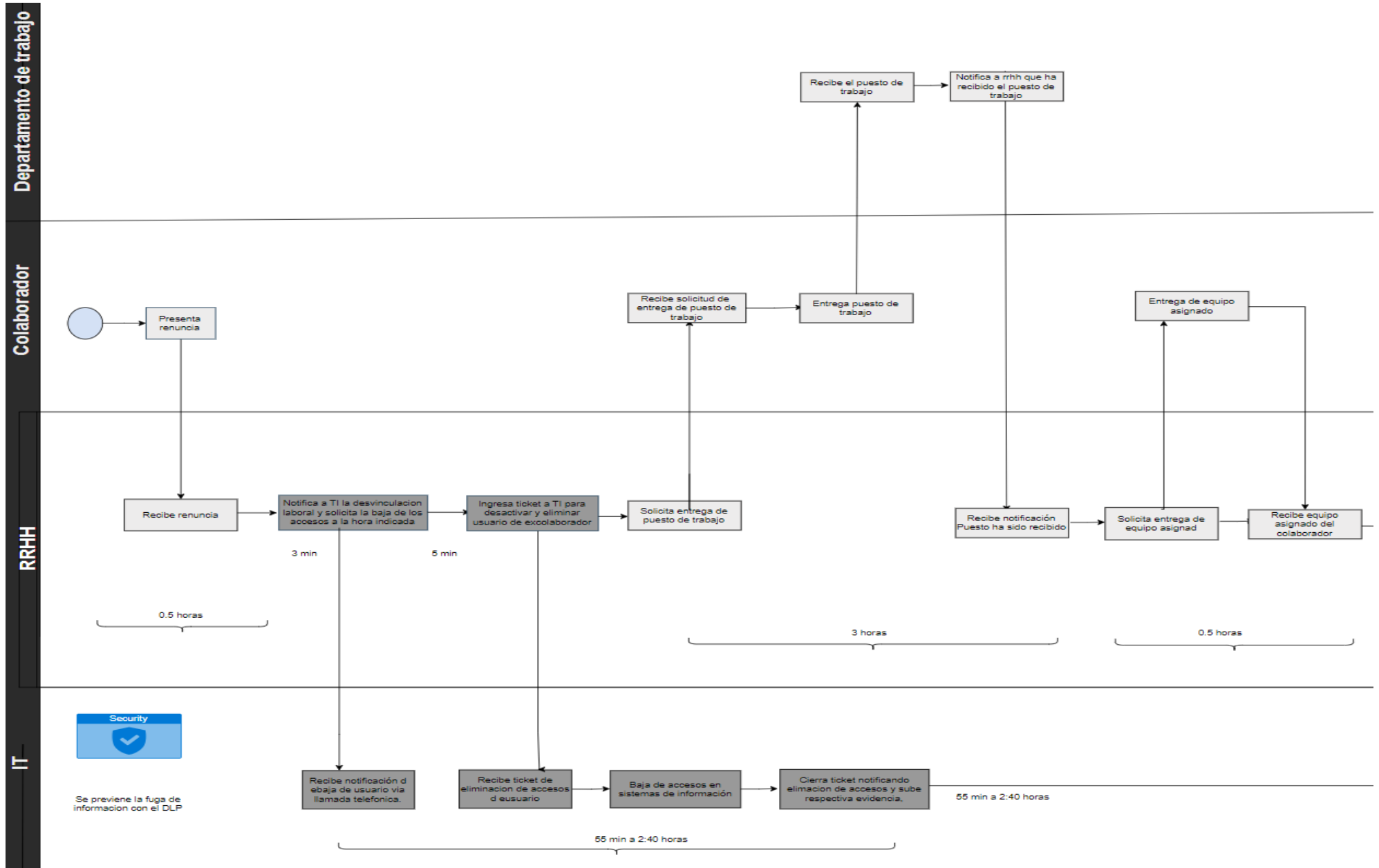
Anexo 4- Proceso actual de renuncia parte 1



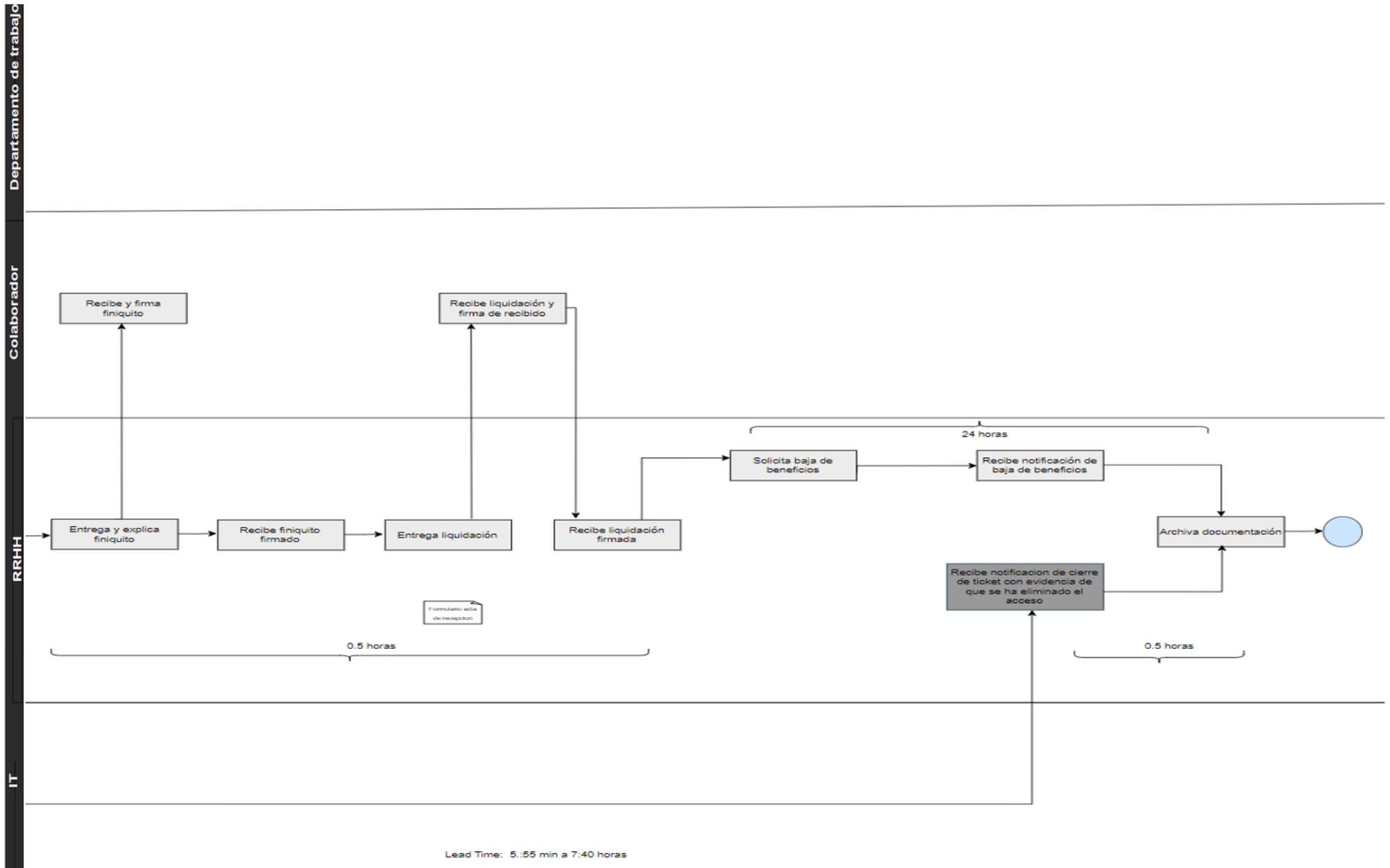
Anexo 5 -Proceso actual de renuncia parte 2



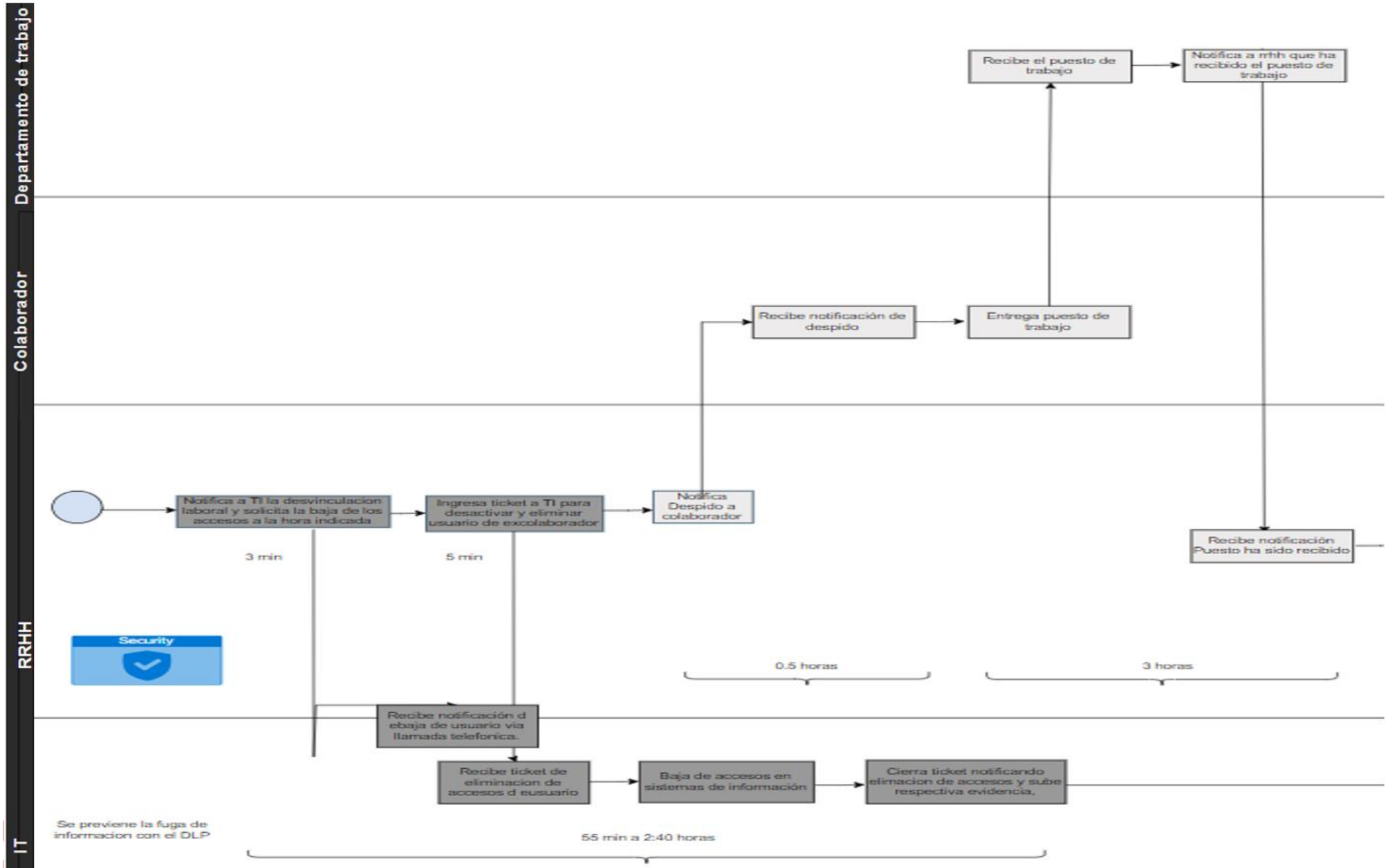
Anexo 6 -Propuesta de nuevo proceso de renuncia parte 1



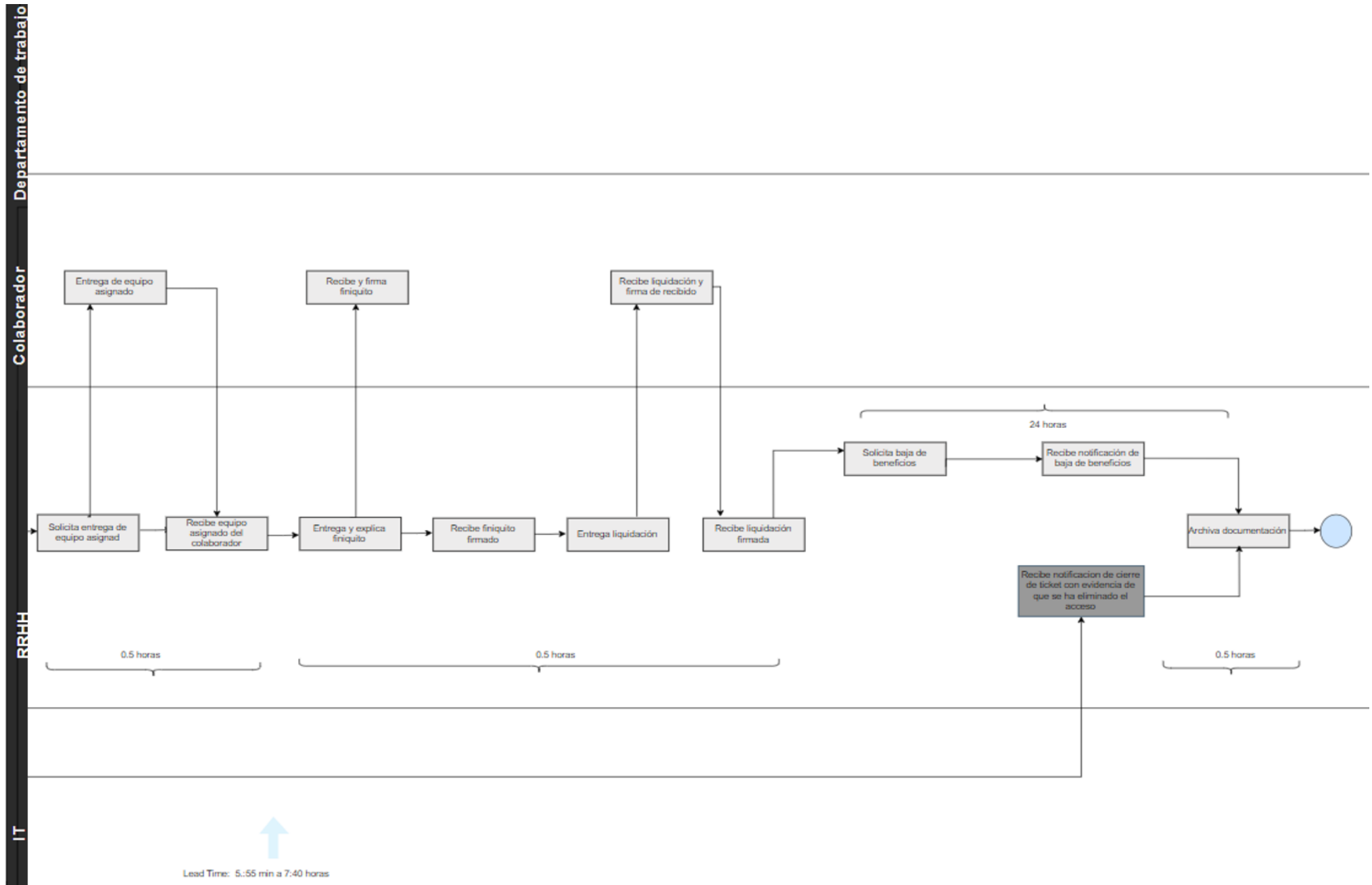
Anexo 7 -Propuesta de nuevo proceso de renuncia parte 2



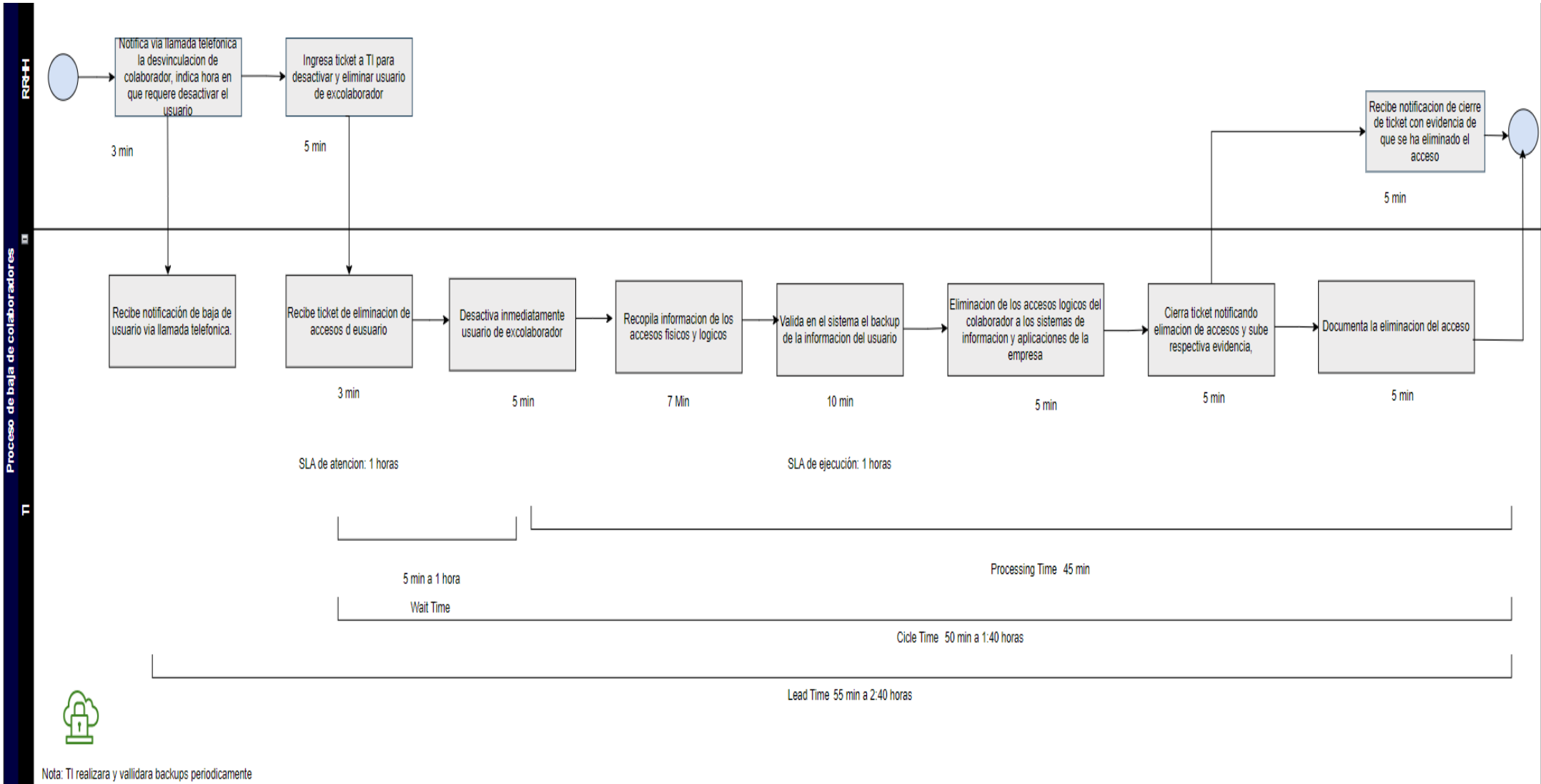
Anexo 8 -Propuesta de nuevo proceso de despido parte 1



Anexo 9 -Propuesta de nuevo proceso de despido parte 2



Anexo 10 -Propuesta de nuevo proceso de baja de accesos



Nota: TI realizara y validara backups periodicamente

CAPÍTULO 9. BIBLIOGRAFIA

- 34, G. A. (s.f.). fuga-datos. Obtenido de <https://protecciondatos-lopd.com/>: <https://protecciondatos-lopd.com/empresas/fuga-datos/>
- cisco. (s.f.). common-cyberattacks.html#~how-cyber-attacks-work. Obtenido de www.cisco.com: https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html#~how-cyber-attacks-work
- Fernández, L. (23 de 02 de 2020). <https://www.redeszone.net/tutoriales/seguridad/data-loss-prevention-que-es>. Obtenido de www.redeszone.net: <https://www.redeszone.net/tutoriales/seguridad/data-loss-prevention-que-es/>
- forcepoint. (2021). brochure-dlp-es_0. Obtenido de www.forcepoint.com: https://www.forcepoint.com/sites/default/files/resources/files/brochure-dlp-es_0.pdf
- <https://www.mundoseguros.net>. (1 de 09 de 2018). quien-esta-detras-de-los-ciberataques. Obtenido de <https://www.mundoseguros.net>: <https://www.mundoseguros.net/quien-esta-detras-de-los-ciberataques/>
- iberdrola. (s.f.). ciberataques. Obtenido de www.iberdrola.com: <https://www.iberdrola.com/innovacion/ciberataques>
- lbn. (04 de Marzo de 2023). Obtenido de lbn.com: lbn.com
- Jonathan Trout, N. C. (21 de 07 de 2021). dmaic-una-guia-completa. Obtenido de <https://cmc-latam.com>: <https://cmc-latam.com/2021/07/21/dmaic-una-guia-completa/>
- marsh. (09 de 03 de 2023). cyber-risk-impact. Obtenido de www.marsh.com: <https://www.marsh.com/co/services/cyber-risk/insights/cyber-risk-impact.html>
- paloaltonetworks. (26 de julio de 2022). paloaltonetworks. Obtenido de [paloaltonetworks](http://paloaltonetworks.com): <https://investors.paloaltonetworks.com/news-releases/news-release-details/palo-altonetworks-unit-42-incident-response-report-reveals>
- Partners, P. T. (21 de 04 de 2021). insider-threats. Obtenido de www.ptechpartners.com: <https://www.ptechpartners.com/2021/04/21/insider-threats/>
- proofpoint. (2022). cost-of-insider-threats. Obtenido de www.proofpoint.com: <https://www.proofpoint.com/es/resources/threat-reports/cost-of-insider-threats>
- sixsigma.co.uk. (s.f.). Lean Six sigma. Obtenido de www.sixsigma.co.uk: https://www.sixsigma.co.uk/es/top-selling-lean-six-sigma-certification-training-courses?hsa_acc=1898131095&hsa_cam=11873943029&hsa_grp=1337006780582502&hsa_ad=&hsa_src=o&hsa_tgt=kwd-83563332454053:loc-170&hsa_kw=lean%20six%20sigma%20certification&hsa_mt=p
- Team, L. C. (s.f.). que-es-la-desvinculacion-en-recursos-humanos. Obtenido de <https://www.lucidchart.com>: <https://www.lucidchart.com/blog/es/que-es-la-desvinculacion-en-recursos-humanos>
- Zelaya, O. (23 de 04 de 2021). honduras-la-proteccion-de-datos-en-honduras. Obtenido de <https://central-law.com>: <https://central-law.com/honduras-la-proteccion-de-datos-en-honduras/>