

JASON DUVAN CONTRERAS CHAPARRO

**PROPUESTA PARA EL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN
PARA LA MULTINACIONAL XYZ DE LA INDUSTRIA DE BPO PARA MEJORAR EL
PROCESO DE EXCEPCIÓN DE ACCESO.**

(Maestría en Gerencia Estratégica de Tecnologías de la Información)

Bogotá, D. C. - Colombia

2021

**PROPUESTA PARA EL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN
PARA LA MULTINACIONAL XYZ DE LA INDUSTRIA DE BPO PARA MEJORAR EL
PROCESO DE EXCEPCIÓN DE ACCESO**

Jason Duvan Contreras Chaparro

Liliana López

Asesor

Universidad Externado de Colombia

Facultad de Administración de Empresas

Maestría en Gerencia Estratégica de Tecnologías de la Información

Bogotá, D. C. - Colombia

2021

UNIVERSIDAD EXTERNADO DE COLOMBIA
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
MAESTRÍA EN GERENCIA ESTRATÉGICA DE TECNOLOGÍAS DE LA
INFORMACIÓN

Rector: **Dr. Hernando Parra Nieto**

Secretaria General: **Dr. José Fernando Rubio**

Decano Facultad de Administración de Empresas: **Dr. Alejandro Beltrán Duque**

Presidente de Tesis: **Dr.**

Director de Tesis: **Dra. Liliana López**

Examinadores:

Nota del Autor

Propuesta para el Gobierno de la Seguridad de la Información para la multinacional XYZ de la industria de BPO para mejorar el proceso de excepción de acceso.

Maestría en Gerencia Estratégica de Tecnologías de la Información. Facultad de Administración de empresas. Universidad Externado de Colombia (Bogotá - Colombia).

La correspondencia con relación a este trabajo debe dirigirse al programa de Posgrado:
Jason Duvan Contreras Chaparro

Correo Electrónico: jason.contreras@est.uexternado.edu.co.

Copyright © 2021. Jason Duvan Contreras Chaparro. Todos los derechos reservados.

Dedicatoria – Agradecimientos

*El presente trabajo lo dedico a mi señora madre **Nubia**, quien me ha inculcado la disciplina como si fuese uno de sus alumnos durante esta hermosa materia que se llama vida, a mi señor padre **Pedro** quien con su personalidad, nobleza y experiencia me ha enseñado la importancia de luchar a pesar de las circunstancias que se puedan presentar en la vida, que quizás, muchas personas necesitan una oportunidad para poder brillar; a mi hermano **Diego** quien durante la vida me ha retado en volverme un mejor profesional y persona, a retarme personalmente en el día a día para ser una mejor versión de mí.*

*Muy especialmente, a mi amada hija **Sarah**, que, con tan solo sus 5 añitos a la culminación de este trabajo, me ha entregado todo su amor, paciencia, motivación y cariño para poder incentivar me en culminar este trabajo de grado.*

A Dios, que a pesar de las dificultades me ha cuidado, me orienta, me da sabiduría y no me desampara en mi día a día, ante todo, especialmente en los años 2018 (finales), 2019 a 2021, los cuales han traído muchos retos profesionales y personales, que gracias a su voluntad me ha permitido culminar diferentes ciclos y proyectos de la mejor forma en mi vida.

Un reconocimiento inmenso a la Organización a la que pertenezco, por darme la oportunidad de crecer y poder abrir las puertas para la realización de este proyecto, el cual espero pueda ser de gran beneficio para la Organización.

Agradezco a mis compañeros de Maestría por esas clases magistrales de discusión, de conocer más del sector público y salir de la burbuja del sector privado; y agradecido con todos ellos por la permanente atención y preocupación, por preguntarme por mis avances a pesar de que ellos ya habían obtenido el título de Magíster y ofrecerme su ayuda y guía para poder culminar este documento.

*De igual forma mi gratitud a la Universidad Externado, en especial a la profesora **Liliana** quien me compartió una Cátedra excepcional de Metodologías*

de Investigación, quien siempre estuvo disponible para resolver mis dudas, inclusive, después de 2 años en los que estuve alejado; guiándome para poder llegar a la culminación de este documento.

Finalmente, me agradezco por mi entereza, por permitirme seguir en una preparación continua y mantener ese espíritu de aprendizaje que despertó desde que era muy pequeño; el cual se mantiene, como también por esas ganas de culminar los proyectos, iniciando por la resiliencia que me caracteriza y poder resistir diferentes adversidades sin perder el foco a donde me dirijo.

Contenido

Introducción.....	13
1. Planteamiento del problema.....	15
1.1 La organización y su negocio.....	15
1.2 El contexto en Colombia	16
1.3 La importancia de la información	17
1.4 Introducción a seguridad de la información (crecimiento requiere integración) 17	17
1.5 Operación a seguridad de la información.....	19
1.6 Proceso de excepción de acceso.....	19
1.7 Seguridad de la información en la Organización.....	21
1.8 Problemática	22
1.9 Preguntas de investigación	23
Rectora.....	23
Secundaria	23
1.10 Objetivos.....	24
General.....	24
Específicos	24
1.11 Alcance limitaciones	25
1.12 Justificación	25
2. Revisión de literatura - Marco Conceptual.....	27
2.1 Definiciones básicas	27
2.2 Generalidad de gobierno	27
2.3 Marco de referencia para el Gobierno de Seguridad de la Información.....	28
2.4 Resultados de una efectiva gobernanza en seguridad de la información.....	33
2.5 Relación entre gobierno y riesgo	34
2.6 El papel de evaluación de riesgo	35
2.7 Riesgo en la industria de tercerización de servicios	36
2.8 Riesgo en sistemas tecnológicos de información	38
2.8.1 Definiciones básicas de Riesgo.....	38
2.8.2 Factor de Riesgo 1: Amenaza.	39
2.8.3 Factor de Riesgo 2: Vulnerabilidades.....	40

2.8.4	Factor de Riesgo 3: Condiciones de predisposición.....	42
2.9	Marcos para la evaluación del riesgo	43
2.9.1	Marcos sujetos al ciclo de Deming.	43
2.10	Determinación del Riesgo.....	53
2.10.1	Factor de Riesgo 3: Probabilidad.	53
2.10.2	Factor de Riesgo 4: Impacto.....	54
2.11	Controles del Riesgo.	57
2.11.1	PCI DSS.	58
2.11.2	ISO/IEC 27002:2005.	59
3.	Metodología de Investigación.....	62
3.1	Tipo de investigación	62
3.2	Instrumentos para la recolección de la información	62
3.2.1Observación	62
3.2.2	Análisis de documentos.....	64
3.2.3	Entrevistas.....	65
3.3	Muestra de estudio.....	67
3.3.1	Muestra de estudio para instrumento de observación.	67
3.3.2	Muestra de estudio para instrumento de análisis de documentos.	68
3.3.3	Muestra de estudio para instrumento de entrevistas.	68
3.4	Recolección de información	69
3.5	Análisis de información	69
3.6	Sesgo.....	70
3.7	Piloto	70
3.8	Consideraciones éticas	71
4.	Recolección de información y Análisis de datos.....	72
4.1	Recolección de información	72
4.1.1	Proceso de recolección de información para: Observación.....	72
4.1.2	Proceso de recolección de información para: Análisis de documentos.	73
4.1.3	Proceso de recolección de información para: Entrevistas	74
4.2	Análisis de datos	75
4.2.1	Análisis de información: Observación.....	76

4.2.2	Análisis de información: Análisis de documentos.....	78
4.2.3	Análisis de información: Entrevistas.....	80
4.2.3.1.	<i>Análisis de entrevistas Operaciones</i>	80
4.2.3.2.	<i>Análisis entrevistas tecnología</i>	83
4.2.3.3.	<i>Análisis entrevistas seguridad de la información</i>	86
4.3	Generación de proposiciones.....	88
4.3.1	Integración de las categorías.....	88
4.3.2	Agrupación de las categorías.....	89
4.3.3	Generación de variables.....	90
4.3.4	Generación de proposiciones.....	92
5.	Propuesta.....	93
5.1	Transformación digital de la excepción de acceso.....	93
5.1.1	Estandarizar la información.....	93
5.1.2	Identificación numérica.....	94
5.1.3	Acceso para consulta.....	94
5.1.4	Evaluaciones de riesgo.....	95
5.1.5	Flujo del proceso.....	95
5.2	Mejorar interrelación de los departamentos involucrados.....	96
5.2.1	Entender el departamento de operaciones.....	96
5.2.2	Entender el departamento de seguridad de la información.....	97
5.2.3	Entender el departamento de tecnología.....	97
5.3	Cultura Organizacional.....	98
5.4	Gobierno.....	99
5.4.1	Contratos.....	99
5.4.2	Patrocinador de la transformación digital.....	99
5.4.3	Estructura de aprobación.....	100
5.4.4	Excepciones concedidas en otras geografías para clientes con operaciones globales.....	100
6.	Recomendaciones y conclusiones.....	101
	Referencias.....	105
	Anexos.....	112

Lista de tablas

Tabla 1. Categoría Excepciones, autoría Organización XYZ	20
Tabla 2. Beneficios efectiva Gobernanza.....	33
Tabla 3. Ranking Razones y Riesgos en Industria de Tercerización	36
Tabla 4. Fuentes de amenaza comunes.	40
Tabla 5. Definición de Probabilidad.....	54
Tabla 6. Definición de magnitud de impacto,	55
Tabla 7. Matriz Nivel de Riesgo.	56
Tabla 8. Escala de riesgo, recomendación de acciones y sugerencias.	57
Tabla 9. Controles PCI DSS a alto nivel.....	58
Tabla 10. Cláusulas y Categorías de Seguridad de ISO/IEC 1799:2005	60
Tabla 11. Integración categorías y análisis de instrumentos de investigación	88
Tabla 12. Agrupación de categorías y análisis de instrumentos de investigación.....	90
Tabla 13. Conjunto final de variables.	91
Tabla 14. Amenazas Humanas: Fuente de amenaza. Motivación y acciones de amenaza.	112
Tabla 15. Pares de vulnerabilidad y amenaza.	114

Lista de figuras

Figura 1. Localizada la Organización XYZ dentro del cuadrante de líderes.....	16
Figura 2. Fases que componen el Gobierno de Seguridad de la Información.....	29
Figura 3. Marco de Gobierno para Seguridad de la Información.....	31
Figura 4. Modelo de Gobierno de Tecnologías de la Información.....	32
Figura 5. Ciclos de Propuesto Dr. Edwards Deming	44
Figura 6. Estructura base	45
Figura 7. Integración del Ciclo Deming	47
Figura 8. Procesos fundamentales para la evaluación del riesgo	48
Figura 9. Modelo de relación estructurada.....	50
Figura 10. Modelo en estrategias de seguridad, políticas, estructuras de sistemas y características funcionales.....	51
Figura 11. Recolección de información básica.....	131
Figura 12. Justificación.....	132
Figura 13. Interfaz para actualizar notas.....	133
Figura 14. Grupo de aprobadores.....	134
Figura 15 Lista de requerimientos.....	135

Lista de anexos

Anexo 1. Amenazas Humanas: Fuente de amenaza. Motivación y acciones de amenaza	112
Anexo 2. Pares de vulnerabilidad y amenaza.	114
Anexo 3. Documento PCI DSS.	114
Anexo 4. Instrumento de observación	115
Anexo 5. Herramienta de análisis documental.	118
Anexo 5.1. Herramienta para análisis de documentos de excepción de acceso	118
Anexo 5.2. Categoría de excepciones	119
Anexo 6. Ejemplo excepción de acceso.....	120
Anexo 7. Instrumento de entrevistas	124
Anexo 7.1. Entrevista para el departamento de operaciones.	124
Anexo 7.2. Entrevista para el departamento de seguridad de la información.	125
Anexo 7.3. Entrevista para el departamento de Tecnología.	127
Anexo 8. Integración y asociación de categorías	128
Anexo 9. Interfaz de ServiceNow.	131

Introducción

Este documento propone una solución al proceso de excepción de acceso, el cual es ejecutado por el departamento de Seguridad de la Información dentro de una multinacional del sector BPO. Dicho proceso ha acarreado varios problemas dentro de la Organización XYZ, hasta el punto de generar una mala perspectiva de algunos clientes corporativos por diferentes desconexiones a nivel interno, no solo del departamento de Seguridad de la Información sino de varios de los departamentos involucrados en dicho proceso.

Inicialmente el documento guía al lector para ponerlo en contexto referente a la problemática que tiene la Organización XYZ, en segunda instancia se desarrolla un marco teórico enfocado en proveer la definición sobre el gobierno de seguridad de la información, dicha definición abarca varios conceptos, los cuales se desarrollan para que el lector tenga claridad del marco de referencia que se propone para el gobierno de seguridad de la información, qué según el autor, se ajusta de mejor forma a la problemática objeto del desarrollo de este trabajo. Adicionalmente se guía al lector sobre marcos de evaluación de riesgo y el papel vital de la gestión riesgo, dentro del gobierno de seguridad de la información.

Como tercera etapa, se expone la metodología de investigación a usar en este caso de estudio, se mencionan los diferentes instrumentos de investigación que hicieron parte de la elaboración de este documento, se informa sobre la muestra de estudio por cada instrumento de investigación usado dentro de la organización XYZ.

En la cuarta etapa se da a conocer los procesos usados para la recolección de la información, de qué forma se analizó dicha información, la misma con el fin de explicar cómo se generaron las proposiciones. Dichas proposiciones son los insumos base para elaborar la propuesta a implementar.

En quinto lugar, se hace mención de propuestas a nivel del gobierno de seguridad de la información, las cuales apalancarían de una forma positiva y eficiente las mejoras en el proceso de excepción de acceso con el fin de obtener beneficios para el negocio y

departamentos involucrados dentro del proceso. Las propuestas mencionadas involucran una transformación digital al proceso de excepción de acceso mediante el uso de ServiceNow, esta herramienta ya es usada por otros departamentos de la Organización XYZ, pero no por el departamento de seguridad de la información, se menciona el poder intervenir un poco la cultura organizacional para que el proceso pueda ser ejecutado de una manera más eficiente. Cabe resaltar que el papel del gobierno de seguridad de la información es vital, ya que son los mayores patrocinadores en que se puedan implementar las propuestas expuestas en este documento.

En la parte final del documento, se dan a conocer al lector las conclusiones y recomendaciones donde se resalta los hallazgos, haciendo énfasis a la propuesta y resaltando que se pretende por cada uno de los puntos discutidos, dejando ver la importancia que juega el gobierno de la seguridad de la información como el principal patrocinador de las propuestas expuestas.

1. Planteamiento del problema

1.1 La organización y su negocio

La multinacional XYZ¹, tiene operaciones en más de 15 países, dichos países cuentan con una ubicación geográfica estratégica, con el fin de poder converger en los diferentes husos horarios de las regiones AMER², APAC³, EUR⁴, regiones donde la multinacional presta servicios a billones de clientes naturales⁵.

Históricamente la organización pertenecía a la industria BPO⁶, sin embargo, actualmente se ha autodenominado como organización transformadora de procesos. El negocio de este tipo de organización se enfoca en el ayudar a los clientes corporativos⁷ en repensar y reconstruir procesos para la era digital. Dicha transformación se da a partir de la aplicación de design thinking a una escala y precisión en analítica de datos, con el objetivo de ayudar a los clientes en lograr una alta agilidad, a través de un servicio al cliente automático y transformado digitalmente, traduciéndose en beneficios económicos para los clientes, esta estrategia de negocio ha hecho que Gartner la catalogue como una de las organizaciones líderes en la industria de BPO; en la figura 1, se encuentra localizada la Organización XYZ dentro del cuadrante de líderes.

La multinacional presta servicios a más de 120 clientes corporativos pertenecientes a Fortune 100⁸. Los clientes corporativos pertenecen a diferentes industrias, segmentados como se menciona a continuación: banca y servicios financieros, cuidado de la salud (healthcare), seguros, telcos, retail, tecnología, viaje,

¹ Se hace mención en este documento a la organización de estudio como Multinacional XYZ, compañía XYZ u Organización XYZ, debido a políticas de privacidad y seguridad con el fin de proteger el nombre de la compañía.

² AMER, referencia para denotar los países comprendidos en el continente americano.

³ APAC, referencia para denotar los países ubicados dentro de la región Asia y Pacífico.

⁴ EUR, hace referencia a los países ubicados en el continente europeo.

⁵ Clientes Naturales, hace referencia a las personas que toman servicios con grandes empresas, como por ejemplo usted o quien escribe, toma servicios por ejemplo con Claro.

⁶ BPO, del inglés *Business Process Outsourcing*, tercerización de procesos de negocio.

⁷ Clientes Corporativos, hace referencia a las organizaciones que tercerizan sus servicios y son entregados a una compañía de outsourcing.

hospitalidad y gobierno. Cada segmento representa para la multinacional XYZ una línea de negocio, es decir, que actualmente cuentan con 8 líneas de negocio.

La relación de negocio se da entre el cliente corporativo y la Organización XYZ, donde se definen diferentes métricas tanto para la prestación de servicio a los clientes naturales, como métricas de la infraestructura tecnológica dispuesta por la Organización XYZ para prestar los servicios tercerizados.



Figura 1. Localizada la Organización XYZ dentro del cuadrante de líderes.

Fuente: Recuperado de Singh & Manusama (2016).

1.2 El contexto en Colombia

En Colombia la industria BPO juega un papel muy importante, ya que es una industria muy atractiva para diferentes inversionistas por factores como: estructura de costos, mano de obra, flexibilidad laboral, ubicación geográfica estratégica, conectividad tecnológica (Dinero, 2013). 350.000 puestos de trabajo generó la industria de BPO en el

año 2017, aportando 1,2% del PIB, con transacciones superiores a los 6 billones de pesos (Dinero, 2017).

La multinacional XYZ, actualmente emplea alrededor de 7.000 personas en Colombia, que están distribuidos entre Bogotá y Barranquilla, concentrando la mayoría de los empleados en Bogotá. En cuanto a Latinoamérica es la operación más grande, por ende, es la operación insignia de la región.

1.3 La importancia de la información

Por la naturaleza de los servicios que ofrece la multinacional XYZ, es común que los empleados asignados a la operación tengan contacto con información sensible de los diferentes clientes naturales, quienes están ubicados en diferentes regiones del planeta, entendiendo como información sensible los datos financieros, médicos, personales, gubernamentales; entre otros, siendo estos necesarios para poder dar continuidad a los procesos y/o requerimientos propios de la operación de cada cliente corporativo.

Entendiendo, el concepto de información como uno de los elementos más importantes de cualquier organización hoy en día y catalogado como uno de los tres recursos más valorados por las organizaciones actualmente (Kovacich & Haliobazek, 2016). La información está expuesta a múltiples riesgos informáticos, ya que las organizaciones deben hacer un gran esfuerzo en poder transmitirle al cliente el estado de seguridad *“implementando mecanismos de encriptación, protección, autenticación y verificación”* (Chellappa & Pavlou, 2002). Es por esto que, el futuro de las transacciones de este tipo depende en cómo se controlan riesgos de seguridad de la información, mejorando la percepción del cliente (Friedman, Khan & Howe, 2000) y a su vez, generando y transmitiendo confianza (Hoffman et al., 1999).

1.4 Introducción a seguridad de la información (crecimiento requiere integración)

En los últimos años el negocio de la multinacional XYZ se ha expandido de una manera muy acelerada, debido a que las operaciones han crecido y se han transformado

de una forma muy dinámica, haciendo que el gerenciamiento tome un contexto más complejo, parte de este crecimiento se ve reflejado también en las áreas de soporte como lo son: finanzas, recursos humanos, calidad, tecnología, seguridad de la información; entre otros. Sin embargo, al crecer la operación de la organización, se debe tener en cuenta que para poder entregar servicios efectivos tanto para los clientes naturales como para los clientes corporativos, se deben integrar los procesos de negocio y funciones de soporte para tener un alineamiento perfecto en la entrega del servicio y a su vez tener una mejor gestión del negocio (Brotby, 2009). Lo cual, en ciertas áreas no se cumple debido a que el objetivo de la organización es crecer lo que más pueda y poder cumplir con los rendimientos financieros pactados, dejando atrás la integración sugerida por Brotby (2019).

Dicha integración se ve afectada en la relación de negocio que sostienen los departamentos de seguridad de la información y tecnología con el área de operaciones. Vale aclarar en este punto que las diferentes áreas de soporte se reportan en una estructura organizacional separada de operaciones, conocida como verticales. El departamento de Seguridad de la Información tiene la responsabilidad junto con el departamento de Tecnología en establecer e implementar controles alineados con las políticas de seguridad establecidos por la gerencia estratégica de Seguridad de la Información y Tecnología de la Organización XYZ, garantizando el uso adecuado de los datos que entregan los clientes naturales a la multinacional XYZ. Ya que los clientes corporativos exigen el cumplimiento y la certificación de estándares internacionales como son PCI⁹, ISO 27001¹⁰, entre otros estándares importantes relacionados con seguridad de la información.

⁹ PCI, Payment Card Industry, conjunto de estándares de seguridad diseñados para garantizar que todas las compañías que procesan almacenan o transmiten información de tarjetas de crédito mantienen un entorno seguro.

¹⁰ ISO 27001, es el estándar más conocido en la familia que proporciona los requisitos para un Sistema de Gestión de Seguridad de la Información.

1.5 Operación a seguridad de la información

Las políticas de seguridad son emitidas a nivel de la alta gerencia de la organización y se replica a niveles tácticos y operacionales. Dichas políticas son definidas por un proceso de direccionamiento en función del cumplimiento de estándares de seguridad de la información y legislación de Estados Unidos, en suma, se valida mediante un proceso de control si se han cumplido dichas políticas, estableciendo de esta forma un modelo de Gobierno en Seguridad de la Información (Von Solms, Thomson & Maninjwa, 2011).

Sin embargo, el desarrollo del negocio de los diferentes clientes corporativos es muy dinámico y surgen requerimientos que no se ajustan a las políticas y/o estándares de seguridad de la información requeridos, es por esto, que constantemente la operación del departamento de seguridad de la información otorga excepciones a las políticas de seguridad de la información previamente definidas, el proceso internamente se denomina excepción de acceso. Dichas excepciones deben asegurar que el riesgo de otorgar la excepción sea mitigado de forma apropiada, con el objetivo de reducir el impacto de una manera que la organización pueda transmitir el estado de tranquilidad y confianza (estado seguro) a los clientes corporativos, dichas excepciones sugieren soluciones de carácter técnico que garantizan el cumplimiento de los estándares de seguridad de la información con el fin de poder certificar la operación de los clientes corporativos y poder cumplir con las políticas de seguridad.

1.6 Proceso de excepción de acceso

La excepción de acceso se acoge a una política previamente definida por la organización, dicha política establece un procedimiento el cual es:

- a. Enviar el formato de “excepción de acceso” a la persona que requirió la excepción, solicitando a la persona completar dicho formato, con una apropiada justificación de negocio y aprobación por parte del interesado de la operación (generalmente es un director).

- b. El departamento de Seguridad de la Información identifica y asigna una categoría para el tipo de excepción, en base a la matriz de excepción de acceso (tabla 1), donde se valida que grupo de interesados debe aprobar la excepción de áreas de soporte o del mismo equipo de operaciones.
- c. El equipo de Seguridad de la Información recibe de vuelta el formato con las aprobaciones y justificación acertadas, e inicia la verificación de los detalles de la excepción a estudiar, analizando los riesgos asociados con el fin de proveer y habilitar el acceso solicitado.
- d. El gerente de Seguridad de la Información asignado a la geografía o el señor vicepresidente de Seguridad de la Información, tomando como base la justificación del negocio y el riesgo asociado a la excepción, podrán aprobar o denegar el acceso.
- e. Basado en la criticidad de la excepción de acceso, el departamento de Seguridad de la Información se reserva el derecho de negar o aprobar el acceso solicitado.

Tabla 1. Categoría Excepciones, autorización Organización XYZ

Categoría Excepciones	Nivel de aprobación de cabeza del negocio
Usuario NT para contratistas / proveedores	Nivel 6 o arriba
Usuario de correo para contratistas / proveedores	Nivel 6 o arriba
Acceso web correo para contratistas / proveedores	Nivel 6 o arriba
Acceso a escritorio remoto	Nivel 6 o arriba
Privilegios de administrador local	Nivel 6 o arriba
Acceso a puerto USB, unidad de CD/DVD	Nivel 6 o arriba
Usuario NT concurrente	Nivel 6 o arriba
Uso de USB / permiso de administrador para portátiles	Nivel 6 o arriba
Recuperación de datos	Nivel 6 o arriba
Solicitud de cámara WEB	Nivel 6 o arriba
Respaldo de información en disco duro externo	Nivel 6 o arriba

Categoría Excepciones	Nivel de aprobación de cabeza del negocio
Instalación de clientes de mensajería no corporativos (Yahoo, Messenger, Skype)	Nivel 6 o arriba
Instalación de herramientas para compartir pantalla	Nivel 6 o arriba
Escritura de CD / DVD	Nivel 6 o arriba
Conectividad DSL, instalación de laboratorio	Nivel 6 o arriba
Acceso a un nuevo sitio web	Nivel 6 o arriba
Software que no es estándar dentro de la organización	Nivel 6 o arriba
Excepción a dispositivos electrónicos	Nivel 6 o arriba
Excepción a uso de teléfonos móviles	Nivel 6 o arriba

Fuente: Elaboración propia.

El riesgo se puede categorizar en 3 niveles: bajo, medio y alto. Dicha categorización es otorgada por el gerente de seguridad de la información de acuerdo a la experiencia, pericia, formación académica y análisis del entorno a la cual se debe afrontar la excepción de acceso.

1.7 Seguridad de la información en la Organización

El departamento de seguridad de la información de la Organización XYZ, es percibido en general como un departamento obstaculizador el cual no contribuye en el desarrollo del negocio por parte del departamento de operaciones, a su vez debido a que el área de tecnología es la encargada de implementar los controles de seguridad de la información, también termina involucrado en una mala relación ante el área de operaciones, de forma que la relaciones entre los departamentos mencionados sea un poco tosca, esto a consecuencia de que cada cabeza de área quiere proteger los intereses que son fundamentales del área a la cual representa. Sin embargo, el área de seguridad de la información y tecnología, se acogen a las políticas discutidas por la alta gerencia, la cual buscan mantener en alto el buen nombre de la multinacional XYZ, la reputación, manteniendo un alto cumplimiento de métricas de la seguridad de la información para la infraestructura tecnológica, la cual es compartida por varios clientes

corporativos. El cumplimiento contribuye a transmitir el estado seguro dentro y fuera de la organización, con el fin de poder proveer servicios con altos estándares de calidad como lo ha venido haciendo hasta este momento.

El área de operaciones es la encargada de entregar el servicio a los clientes naturales, es la cara frontal de la Organización XYZ al cliente corporativo, atendiendo todos los requerimientos hechos por ellos, la presión que manejan es elevada debido a que son los que están siendo medidos directamente por el cliente corporativo, así mismo, son los que generan la utilidad para la Organización XYZ. Es por esto que, en varias ocasiones, perciben a ciertas áreas de soporte como departamentos que retrasan procesos, ya que el cliente espera respuesta inmediata.

1.8 Problemática

Como se ha mencionado previamente la Organización XYZ tiene operaciones en diferentes regiones geográficas, las cuales sirven a los clientes corporativos en poder ofrecer servicios a sus clientes naturales en las regiones de AMER, APAC, EUR. Las áreas de seguridad de la información y tecnología tienen representación local en el país donde opera la Organización XYZ, las áreas hacen parte de las verticales globales que están establecidas en el marco de Gobierno Corporativo de la Organización XYZ, y pueden ser consultadas en el anexo 1.

De acuerdo con el contexto descrito en el anterior capítulo, el hecho empresarial de estudio se dirige al departamento de seguridad de la información, concretamente a la forma de gobernanza que se le está dando al proceso de excepción de acceso. En el momento de que el gerente de seguridad de la información está asignando el nivel de riesgo entre bajo, medio o alto; se evidencia una falencia en el Gobierno de Seguridad de la Información para dicho proceso.

La falencia previamente expuesta, ha traído varios desacuerdos entre las áreas internas de la organización, especialmente del departamento de operaciones con los departamentos de Seguridad de la Información y Tecnología. Además, la mala gestión de este proceso ha traído una serie de consecuencias perjudiciales para el negocio, ya

que los clientes corporativos han evidenciado falta de comunicación dentro de la Organización XYZ sin importar si es el área de operaciones, tecnología o seguridad de la información; ya que, por naturaleza el cliente corporativo debe observar a la Organización XYZ como una unidad, la cual le provee servicios de tercerización.

Los clientes corporativos evidencian esta falta de comunicación, ya que al tener operaciones en los diferentes países donde opera la Organización XYZ, han experimentado con tener la excepción de acceso aprobada en el país que presta servicios a la región de APAC, pero una negación de la misma excepción de acceso en el país donde se prestan servicios para la región AMER. Esto afecta la operación de tercerización en su día a día para poder entregar un servicio de calidad al cliente natural.

Esta problemática ha traído como consecuencia la terminación de contratos con clientes corporativos, cerrando sus operaciones en todos los países donde está desplegada la operación de dicho cliente corporativo, generando una mala imagen para la Organización XYZ y un malestar interno entre los diferentes colaboradores pertenecientes a las diferentes áreas encargadas de proveer el servicio al cliente corporativo.

1.9 Preguntas de investigación

Rectora

¿Qué elementos garantizan una mejor gobernabilidad para el proceso de excepción de acceso a las políticas de seguridad de la información?

Secundaria

- ¿Cómo puede la Organización XYZ garantizar que los gerentes de Seguridad de la Información manejen los mismos datos excepciones aprobadas o rechazadas en los diferentes países donde opera la Organización XYZ?

- ¿Qué marco de aprobación se debería implementar para la excepción de acceso solicitada por clientes que tienen operaciones globales?
- ¿Cómo se puede mejorar el análisis de riesgo desarrollado por los gerentes de seguridad?
- ¿Qué metodología se puede sugerir a la Organización XYZ, para documentar las excepciones existentes y las que existirán, con el objetivo de que sean de fácil acceso para los Gerentes de Seguridad de la Información?

1.10 Objetivos

General

Plantear a la Organización un modelo de gobernabilidad dentro del departamento de seguridad de la información, que contribuya a mejorar el proceso de excepción de acceso.

Específicos

- Contribuir a la madurez del actual modelo de gobernabilidad del departamento de seguridad de la información.
- Asegurar una inclusión total del grupo de interesados, que influye en la justificación y aprobación de la excepción de acceso.
- Proponer un marco de gobierno para la categorización del riesgo por parte de los Gerentes de Seguridad de la Información.
- Documentar de una manera más apropiada las necesidades del cliente corporativo, al momento de solicitar una excepción de acceso, con el fin de facilitar el análisis de riesgo por parte del departamento de seguridad de la información.

1.11 Alcance limitaciones

Con el desarrollo de este artículo académico, se pretende alcanzar la madurez del modelo de gobierno para la Seguridad de la Información que actualmente tiene la Organización XYZ, estableciendo una línea base, de donde se dará inicio a la propuesta de valor que será la más apropiada para el hecho empresarial que está bajo discusión. Esto con el fin de poder contribuir en mejorar la gobernabilidad del proceso de excepción de acceso.

Igualmente, se pretende lograr una mejor relación entre los departamentos de operaciones, seguridad de la información y tecnología, mediante la propuesta a exponer en este documento. Ya que como prioridad se debe hacer notar a los clientes corporativos la integración de áreas de soporte y operaciones, a través la unidad y alineamiento empresarial dentro de las diferentes áreas que conforman la Organización XYZ.

Como gran limitante para el desarrollo de este artículo, la Organización XYZ no autoriza el uso de su nombre y el de sus clientes corporativos para poder ofrecer un mejor contexto y análisis al lector, el autor se esforzará en proveer ejemplos que se asemeje a un contexto que sea de fácil entendimiento para el lector. El modelo o propuesta resultante será expuesto internamente a la gerencia estratégica de seguridad de la información de la Organización XYZ, ellos tendrán la libertad de decidir si acogen o no la propuesta sugerida, a su vez si es implementado el modelo sugerido, la Organización XYZ se reserva el derecho de compartir los resultados tras la implementación del marco o modelo sugerido.

1.12 Justificación

Tomando como primicia las consecuencias que ha traído la problemática expuesta previamente, tanto a nivel externo e interno para la Organización XYZ, es necesario la

intervención, a la forma de gobernabilidad dada hasta este momento para el proceso de excepción de acceso, esta intervención ayudará a que el departamento de seguridad de la información logre una mayor madurez en el actual marco de gobierno, el cual esta acogida.

El poder transmitir un estado de seguridad tanto al cliente corporativo, como al cliente natural es primordial, es por esto que, la información que maneja la Organización XYZ es el recurso más importante con el que cuenta, ya que el trato que se le dé a esta información depende que tan bien el cliente corporativo decida continuar requiriendo los servicios de la Organización XYZ.

También, se quiere hacer notar a la compañía el valor agregado que puede brindar seguridad de la información al gestionarlo de forma correcta, reduciendo la complejidad y aumentando la simplicidad en este caso para el proceso de excepción de acceso, con el fin de mejorar relaciones con los clientes externos y a su vez con los equipos internos como lo son operaciones, tecnología, entre otros.

Debido a que la operación en Colombia es una de las más importantes para la Organización XYZ, se desea demostrar la capacidad de resolución de este tipo de conflictos a las gerencias estratégicas que están ubicadas en EEUU e India, con el fin de afianzar más la confianza, posicionando a Colombia como una geografía de alto valor e importancia para la Organización XYZ, se desea demostrar que cuenta con colaboradores preparados para soportar todas las necesidades de la industria siendo la primera opción en las múltiples geografías donde pueden establecer un negocio, de esta forma contribuir al desarrollo de esta industria localmente en Colombia.

2. Revisión de literatura - Marco Conceptual

2.1 Definiciones básicas

En el desarrollo de este documento, se mencionan diferentes términos relacionados sobre gobierno, siendo prudente definirlos para que el lector tenga un buen contexto del uso de estos términos:

Gobierno: “Principal pilar del Estado, la autoridad que dirige, controla y administra sus instituciones, la cual consiste en la conducción política general o ejercicio del poder ejecutivo del Estado” (Cascajo Castro & García Álvarez, 1994; Ekmekdjian, 1999; López Guerra, 2001).

Gobernanza: “Arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado y la economía” (Real Academia Española, 2017).

2.2 Generalidad de gobierno

En este apartado, se orienta al lector en entregarle la definición de gobierno corporativo, seguido de la definición de gobierno para tecnologías de la información, la cual, se concluye con la definición de Gobierno para Seguridad de la Información.

Gobierno Corporativo es la estructura definida por la organización, dicha estructura prepara los objetivos que la organización debe alcanzar, a su vez la estructura define los medios para poder alcanzar los objetivos, los medios permiten a la organización monitorear el rendimiento para el cumplimiento de los objetivos (Oecd, 2015).

Gobierno de Tecnologías de la Información es el conjunto de responsabilidades y prácticas desarrolladas por la junta directiva y la alta gerencia con el objetivo de proveer dirección estratégica, asegurándose que los objetivos de la organización son alcanzados

y que los riesgos tecnológicos son manejados de forma apropiada, ratificando el uso apropiado de los recursos tecnológicos de la organización (IT Governance Institute, 2006).

La Organización Internacional para la Estandarización ISO, en el estándar 27001 hace referencia a que los sistemas de gestión de seguridad de la información deben preservar la confidencialidad, integridad y disponibilidad de la información aplicando procesos de gestión de riesgos generando confianza a los grupos de interesados (ISO, 2008).

Teniendo en cuenta que la confidencialidad, integridad y disponibilidad son las metas corporativas a las cuales debe estar enfocado la seguridad de la información, damos paso a definir el Gobierno en Seguridad de la Información, entiéndase como la estructura organizacional que refuerza la seguridad de la información; generando una cultura de total entendimiento por parte de los usuarios sobre seguridad de la información. Comprometiendo al grupo de interesados en el desarrollo de buenas prácticas de seguridad de la información, siguiendo las políticas, procedimientos, procesos, uso de tecnologías y mecanismos de cumplimiento necesarios. Mecanismo integrador que asegura la confidencialidad, integridad y disponibilidad de los recursos tecnológicos o la información con la que la organización desarrolla sus objetivos organizacionales (Coertze & von Solms, 2012).

2.3 Marco de referencia para el Gobierno de Seguridad de la Información

Seguido de la definición de gobierno, es necesario proveer un marco que indique al lector, los ámbitos que debe cubrir el Gobierno de Seguridad de la Información. La literatura especializada provee un gran número de métodos sugeridos a seguir, sin embargo, el más relevante que se ajusta a las necesidades de la Organización XYZ es el propuesto por Veiga y Eloff, a continuación, se proveerá información sobre el marco a estudiar.

El Gobierno de Seguridad de la Información hace parte de cuatro fases que componen la seguridad de la información (Veiga & Eloff, 2007), como se ilustra en la figura 2.

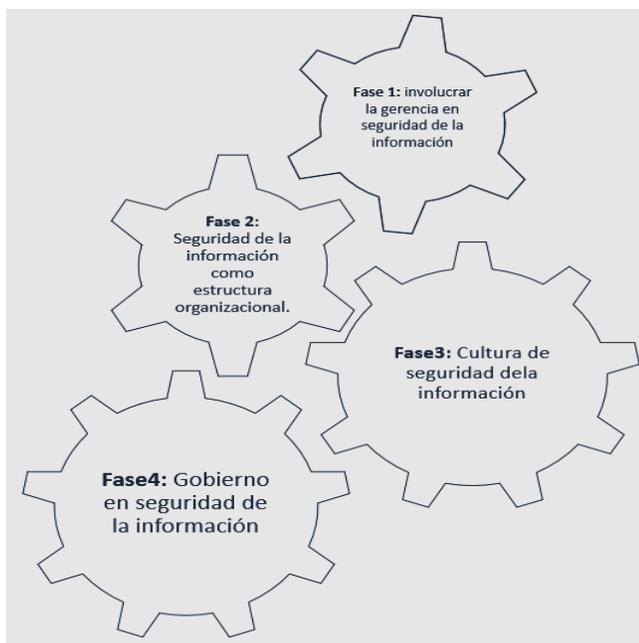


Figura 2. Fases que componen el Gobierno de Seguridad de la Información.

Fuente: Recuperado de Veiga & Eloff (2007).

La primera fase hace referencia en identificar el papel tan importante que juega la gerencia estratégica de la organización, sobre la seguridad de la información (Von Solms, 2000). La incorporación de seguridad de la información, como una estructura organizacional dentro de la organización, es la segunda fase que se ha de considerar (Veiga & Eloff 2007), garantizando que seguridad de la información tenga un papel más vital dentro de la organización. Como tercera fase se considera, cultivar una cultura efectiva de seguridad de información en los colaboradores de la organización, quienes deben adoptarla en el desarrollo de sus actividades diarias (Veiga & Eloff, 2007), esta fase comprende el ámbito humano, el cual es el eslabón más débil de los riesgos a controlar por parte de seguridad de la información. La cuarta fase hace referencia al Gobierno de Seguridad de la Información, los ejecutivos de las organizaciones son los responsables de comunicar la apropiada cultura y marcos de controles para seguridad

de la información, delegando responsabilidades de administración del riesgo en todos los niveles de la organización (IT Governance Institute, 2007).

De manera general la gobernanza de seguridad de la información se puede comprender como la forma en que está dispuesta la seguridad de la información con el fin de mitigar los riesgos (Veiga & Eloff, 2007).

La implementación de un marco de Gobierno de Seguridad de la Información, garantizará a la organización el manejar, controlar y mitigar los riesgos de forma controlada (Veiga & Eloff, 2007).

El marco propuesto por Veiga y Eloff es el resultado de la investigación hecha a cuatro enfoques de seguridad de la información, dichos enfoques son ISO17799¹¹, PROTECT¹², CMM¹³ e ISA¹⁴, la investigación arrojó como resultado el marco expuesto en la figura 3. El marco lista una serie de componentes los cuales son necesarios para el Gobierno de Seguridad de la Información.

¹¹ ISO 17799, Estándar que establece lineamientos y principios generales para iniciar, implementar, mantener y mejorar gestión de la seguridad de la información en una organización.

¹² PROTECT. Policies, risk, objectives, technology, execute, compliance and team. políticas, riesgos, objetivos, tecnología, ejecución, cumplimiento, equipo. Marco de referencia que guía y conduce la evaluación del riesgo para buenas prácticas en la toma de decisiones.

¹³ CMM, Capability Maturity Model.

¹⁴ ISA, Information Security Architecture.

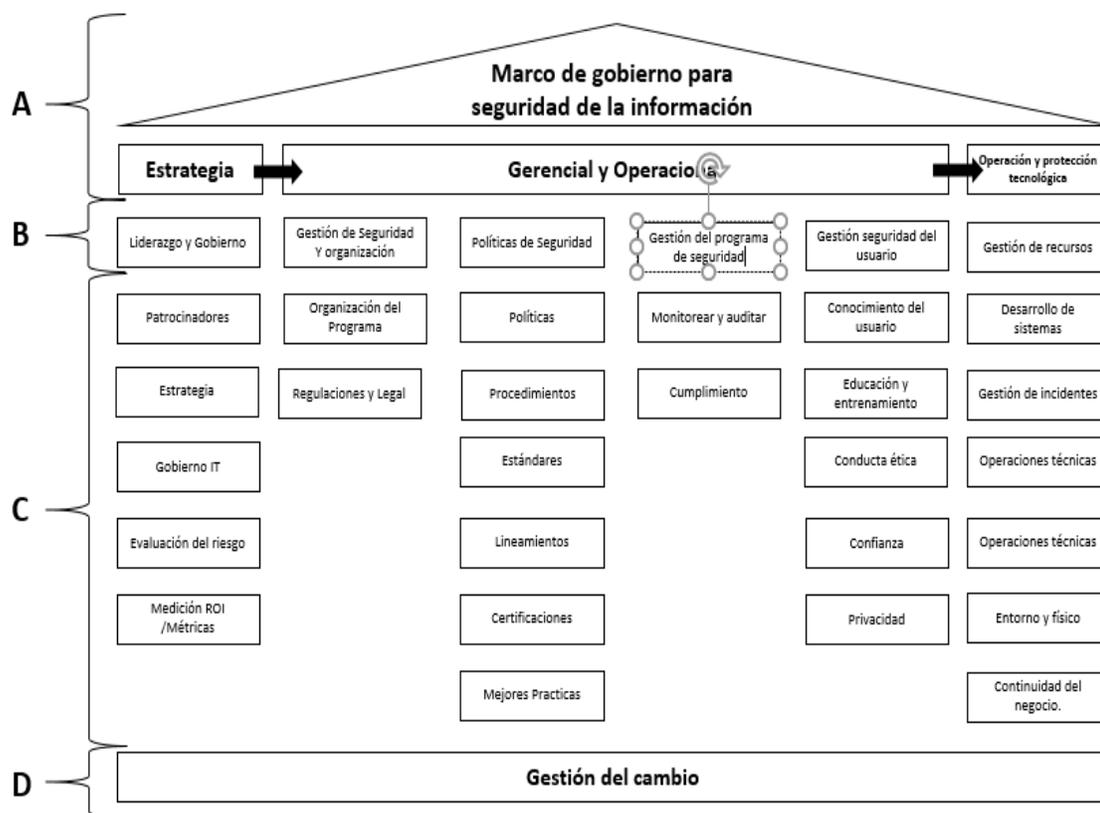


Figura 3. Marco de Gobierno para Seguridad de la Información

Fuente: Recuperado de Veiga & Eloff (2007)

El marco expuesto podría ser usado como punto de partida para gestionar el riesgo identificado por la organización, ya que permite el poder desarrollar lineamientos e implementar controles a diferentes niveles (Veiga & Eloff, 2007).

La figura 3, ilustra 4 niveles. El nivel A, hace referencia al factor estratégico del Gobierno de Seguridad de la Información, donde se definen 3 grandes grupos. El nivel B, agrupa los principales componentes de seguridad de la información en 6 grupos. El nivel C, relaciona los componentes asociados a los grupos definidos en el nivel B. En resumen, todos los componentes están sujetos a la gestión del cambio tal cual lo representa el nivel D. (Veiga & Eloff, 2007).

Si analizamos el modelo expuesto por Veiga y Eloff de forma horizontal para el nivel A, es de evidenciar que dicho marco concuerda con el expuesto por Weill, Ross y Robertson para el Gobierno de Tecnologías de la Información.

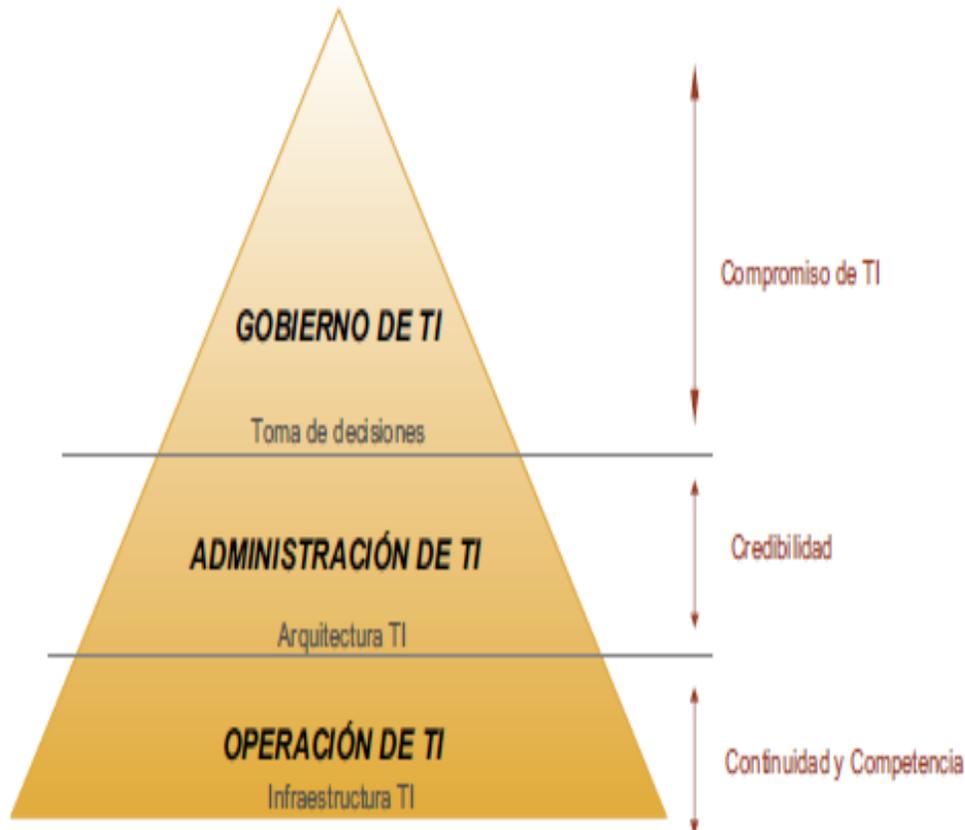


Figura 4. Modelo de Gobierno de Tecnologías de la Información

Fuente: Recuperado de Ross, Weill & Robertson (2006) (3)

La categoría de liderazgo y gobierno, enunciado en la figura 3, contempla el factor de análisis de riesgos, el cual está orientado a la implementación de controles gestionados por el liderazgo y gobierno de la organización (Veiga & Eloff, 2007).

Es de evidenciar que Gobierno de Seguridad de la Información tiene un extenso contenido, no obstante, uno de los factores determinantes para una efectiva gobernanza es la debida gestión del riesgo por parte de la organización, el cual se debe gestionar desde un nivel estratégico de la organización, tal cual lo representa Veiga y Eloff en el marco que desarrollaron.

Cabe resaltar que estudios recientes sobre gobierno de la seguridad de la información citan diversidad de autores y marcos, los cuales toman como eje

fundamental las fases expuestas en la figura 2, ya que, son el punto de partida para gestionar de una manera efectiva el gobierno de seguridad de la información, debido a que tiene un control holístico de los diferentes grupos de involucrados dentro de la organización, esto con base en los estudios realizados por AlGhamdi et al., (2020) y Schinagl & Shahim (2020).

2.4 Resultados de una efectiva gobernanza en seguridad de la información

ISACA y el Instituto de Gobierno TI concuerdan en definir los beneficios esperados de una buena gestión en el Gobierno de Seguridad de la Información, dichos beneficios son descritos en la tabla a continuación.

Tabla 2. Beneficios efectiva Gobernanza

Beneficio	Descripción
Alineamiento estratégico	Alinear actividades de seguridad con estrategia del negocio para soportar objetivos organizacionales.
Gestión del riesgo	Ejecutar medidas apropiadas para gestionar el riesgo y potenciales impactos a un nivel aceptable.
Valor agregado	Optimizar inversiones en soporte de objetivos del negocio.
Gestión de recursos	Usar recursos organizacionales eficiente y efectivamente.
Medición de rendimiento	Monitorear y reportar los procesos de seguridad para asegurar que los objetivos del negocio son logrados.

Fuente: Recuperado de ISACA, 2012; IT Governance Institute (2006)

ISACA hace referencia a un beneficio adicional de la efectiva gobernanza de la seguridad de la información, dicho beneficio es llamado aseguramiento y convergencia de proceso de negocios, que consiste en integrar los procesos más importantes de seguridad de la información para maximizar la efectividad y eficiencia de las actividades desarrolladas por seguridad de la información (ISACA, 2012).

2.5 Relación entre gobierno y riesgo

Gobierno y riesgo son temas de alta discusión hoy en día, siendo los determinantes en la implementación de controles en búsqueda de los objetivos para la organización. El término gobierno denota diferentes puntos de vista epistemológicos, no obstante, el enfoque abrumador hace referencia a dominios organizacionales y de gestión (Bhimani, 2009).

El riesgo se define como la combinación entre la probabilidad de ocurrencia y las consecuencias de un evento no deseado, el riesgo corporativo es definido como la amenaza que se impone en alcanzar los objetivos organizacionales (Di Serio, De Oliveira & Schuch, 2011). Una organización enfrenta diferentes clases de riesgos como lo son riesgos de cumplimiento, riesgos operacionales, riesgos de crédito, riesgos de mercado, riesgos ambientales, riesgos estratégicos y riesgos de las tecnologías de la información (ISACA, 2009). Las tecnologías de la información de una organización están expuestas a serias amenazas que pueden traer efectos adversos en los recursos de estas, impactando las operaciones de dicha organización, dichas amenazas atacan vulnerabilidades que pueden ser conocidas o desconocidas; las cuales exponen la confidencialidad, integridad y disponibilidad de la información procesada por la Organización (National Institute of Standards and Technology Gaithersburg, 2012).

Gobierno y riesgo son construcciones sociales definidas de acuerdo con el contexto en el que habitan. Como dimensión del reino de las organizaciones, gobierno y riesgo se convierten en ámbitos operacionales y procesables ya que se pueden formalizar y moldear en un contexto técnico. Aunque, convertir el concepto de riesgo y gobierno en procedimientos analíticos, aumentará la capacidad de gestión en el riesgo y gobierno dentro de la organización (Bhimani, 2009).

La evaluación del riesgo es una dimensión de gobierno, tienen una interdependencia muy cercana. Las políticas de gobierno, tecnologías de la información y el tamaño de la organización son constituyentes de las variables para moldear el sistema de control para la evaluación del riesgo. No importa el tipo o tamaño de la organización, es de evidenciar que la estructura de la evaluación de riesgo contempla una taxonomía básica, la cual es similar entre todas las organizaciones. Es infructuoso

considerar que gobierno y evaluación del riesgo son estructuras organizacionales diferentes, ya que estas dos están manejando las mismas preocupaciones en cómo alcanzar los objetivos de una organización (Bhimani, 2009).

2.6 El papel de evaluación de riesgo

Las organizaciones hoy en día están sujetas a introducir tecnologías de la información en cualquiera de los procesos con los que prestan servicios a sus clientes, es por esto que, la evaluación del riesgo juega un papel muy importante como parte del gobierno en seguridad de la información (Tohidi, 2011). La evaluación del riesgo permite al gobierno de una organización identificar sus riesgos, con el fin de desarrollar medidas y análisis de seguridad, los cuales deben ser viables económicamente en los controles a implementar a los recursos que manejan información crítica de la organización (Shamala, Ahmad & Yusoff, 2013).

El objetivo de la evaluación del riesgo es identificar, cuantificar y administrar la información relacionada al riesgo, para alcanzar los objetivos del negocio. (Brotby, 2009). Una función esencial del Gobierno de Seguridad de la Información es la evaluación del riesgo, el cual tiene como objetivo proveer un ambiente seguro para negocio electrónico y comercio electrónico (Saleh & Alfantookh, 2011).

Dicho proceso de evaluación del riesgo ofrece caminar de una forma analítica y estructurada a través del estado de seguridad de la organización (Shamala et al., 2013). La definición expuesta por Shamala, Ahmad y Yusoff, referente a la evaluación del riesgo, se asemeja a la entregada por Bhimani, en la relación de gobierno y evaluación de riesgo a su vez se alinea con la definición de Gobierno de Seguridad de la Información mencionada por Coertze y Von Solms, es de evidenciar que la evaluación del riesgo en seguridad de la información juega un papel importante a un nivel estratégico para la organización buscando como beneficio común el alcanzar los objetivos organizaciones (Coertze & von Solms, 2012).

2.7 Riesgo en la industria de tercerización de servicios

Como efecto de la globalización, muchas compañías se ven en la necesidad de reducir el costo de la operación de sus departamentos de tecnología y atención al cliente, debido a los costos operacionales que estos acarrearán para el presupuesto de las organizaciones (Magnu & Chou, 2010). Por otro lado, la mejora del servicio, la alta eficiencia en la prestación de servicios, las alianzas estratégicas o la delegación de riesgo operacional son las responsabilidades de las organizaciones que tercerizan servicios; permitiéndole a los clientes corporativos enfocarse en el núcleo de sus negocios en vez de hacer esfuerzos en la entrega de servicios (Bhatti, Murbak & Nagalingam, 2017), adicionalmente, esta industria permite de forma muy potente, a sus clientes corporativos, el poder reducir costos operacionales alcanzando una alta eficiencia y permitiendo a dichos clientes corporativos concentrarse en su negocio (Innovature Consulting, 2021). Las razones de tercerizar se pueden resumir en razones estratégicas tecnológicas y económicas (González, Gascó & Llopis, 2016), de acuerdo a la investigación hecha por González, Gascó y Llopis (2016) evidencian en su investigación que la razón estratégica es la de más relevancia y es por el cual la mayoría de las organizaciones en su estudio hacen la tercerización de servicios.

González, Gascó y Llopis (2016), en la investigación realizada hacen referencia a los riesgos de más alta importancia que se pueden observar en las organizaciones de tercerización, a su vez hacen un listado de las razones del porqué las organizaciones contratan con un proveedor la tercerización de sus servicios.

Tabla 3. *Ranking Razones y Riesgos en Industria de Tercerización*

Ranking Razones	Ranking Riesgos
Foco en problemas estratégicos	Cualificación del personal
Incrementar flexibilidad del departamento	Dependencia excesiva
Mejora de calidad	Falta de cumplimiento
Remover las tareas rutinarias	Pérdida de conocimiento

Ranking Razones	Ranking Riesgos
Facilitar acceso a tecnología	Inhabilidad del proveedor para adaptarse
Reducir riesgo de obsolescencia	Costos Ocultos
Ahorrar en costos de colaboradores	Problemas de seguridad
Ahorrar en costos de tecnología	Relación incierta
Tener alternativa para sistemas de información internos	Decisión irreversible
Estar a la moda	Posible oposición de los colaboradores
	Problemas con colaboradores

Fuente: Recuperado de (González et al., 2016).

Dichos servicios de tercerización presentan un elevado grado de riesgo debido a que servicios esenciales son tercerizados, dándole oportunidad al proveedor de servicio acceder información crítica, este aspecto de tercerización hace difícil mantener los aspectos esenciales de seguridad de la información confidencialidad, integridad y disponibilidad (Zhang et al., 2010), sobre todo en estos días donde por el contexto que se vive de la dispersión del virus COVID-19 a nivel global, muchas de estas operaciones de la industria de tercerización de servicios se han visto afectadas, donde se ha probado la flexibilidad de esta industria para continuar su operación (Gallimore, 2020), muchos empleados de dicha industria laboran actualmente desde casa, incrementando el riesgo del manejo de información (Innovature Consulting, 2021). Ya que la organización no tiene control total del ambiente de trabajo en casa, a pesar de que muchos de los controles son aplicados en el equipo de tecnología entregado (computador) por la organización al empleado; no obstante, el que la información navegue a través de redes públicas a pesar de los controles estrictos de encriptación, configuraciones fuertes de firewall y navegación de VPN (apegadas a buenas prácticas de seguridad de la información como ISO27001, PCI y/o HIPPA), no hacen que esta industria esté exenta de actividades

maliciosas en internet, incrementando potencialmente el riesgo en seguridad de la información que debe manejar las industrias que tercerizan servicios (Gallimore, 2020).

De todas maneras, proveedores de tercerización de servicios, pueden no entender la naturaleza de sus clientes, en el peor de los casos organizaciones de tercerización de servicios podrían ofrecer soluciones generalizadas para sus clientes corporativos (Magnu & Chou, 2010), sin entender la naturaleza del negocio y especialmente los requerimientos de seguridad de la información que sus clientes manejan.

Es por esto qué, los proveedores de tercerización de servicios necesitan establecer relaciones de confianza con sus clientes corporativos, desarrollando soluciones seguras que tengan en cuenta la relación de negocio (Zhang et al., 2010). Yendo más allá, se requiere un entendimiento de la cultura corporativa de la organización y el contexto operacional (Magnu & Chou, 2010), por parte de la organización de tercerización de servicios con su cliente corporativo.

De todas formas, es de evidenciar que, en estudios realizados, existe un común denominador tanto para la organización que terceriza servicios como para el cliente corporativo. Cumplimiento legal y regulatorio, madurez tecnológica en la organización que terceriza servicios, habilidad de la organización que terceriza servicios para cumplir con los requerimientos del cliente corporativo en políticas, estándares y procesos de la seguridad de la información, disipación del conocimiento por parte de la organización que terceriza servicios, al final, la competencia en seguridad de la información por parte de la organización que terceriza, son los factores comunes entre cliente corporativo y la organización a tercerizar servicios (Bhatti et al., 2017; Dhillon et al., 2017).

2.8 Riesgo en sistemas tecnológicos de información

2.8.1 Definiciones básicas de Riesgo.

El riesgo es la medida que permite establecer a una organización, si está en amenaza por un evento potencial o circunstancia, generalmente, el riesgo está dado en función de: 1. Los impactos adversos que surgieran si se llegara a materializar el riesgo y

2. La probabilidad de ocurrencia. El riesgo en seguridad de la información para sistemas tecnológicos de la información, son los riesgos que atentan contra: la confidencialidad, integridad o disponibilidad de la información o de los sistemas que procesan dicha información, trayendo resultados adversos para la operación, activos, y/o individuos para las organizaciones o las naciones que hacen uso de dichos sistemas (National Institute of Standards and Technology Gaithersburg, 2012).

El riesgo en sistemas tecnológicos de información se asocia con los factores de riesgo, dichos factores son usados en las comunicaciones internas dentro de una organización para poder resaltar de forma acertada los niveles de riesgo a los que está expuesto la organización, en situaciones, circunstancias o contextos particulares. Generalmente los factores de riesgo son: amenazas, vulnerabilidades, impacto, probabilidad y condiciones de predisposición (National Institute of Standards and Technology Gaithersburg, 2012). En los numerales 2.8.2, 2.8.3 y 2.8.4, se habla sobre amenazas, vulnerabilidades y condiciones de predisposición respectivamente. Al final de este capítulo, en los numerales 2.10.1 y 2.10.2 se refiere a la probabilidad e impacto, ya que estos dos últimos factores son claves para poder determinar el riesgo dentro de una organización (National Institute of Standards and Technology Gaithersburg, 2012).

2.8.2 Factor de Riesgo 1: Amenaza.

La amenaza es definida como cualquier circunstancia o evento, con el potencial de impactar adversamente la organización a nivel de su operación, activos o individuos mediante un sistema de información tecnológico haciendo uso de un acceso no autorizado a dicho sistema que puede causar destrucción, publicación o modificación de información y/o denegación de servicio (National Institute of Standards and Technology Gaithersburg, 2012).

Los eventos de amenaza son causados por fuentes de amenaza, dichas fuentes son caracterizadas como: 1. La intención y métodos dirigidos por una entidad, organización, gobierno o persona natural, para la explotación de una vulnerabilidad en un sistema tecnológico de información; 2. La situación y método que quizás

accidentalmente explotan una vulnerabilidad. Como consecuencia dicha explotación de vulnerabilidades generan ventajas en los sistemas tecnológicos de información, frente a otras organizaciones. Dichas ventajas se materializan de forma intencional o accidental, a través de la fuente de amenaza sin importar su naturaleza (Kelley, 2014; National Institute of Standards and Technology Gaithersburg, 2012).

La tabla 4 NIST define las fuentes de amenaza más comunes que pueden impactar los sistemas tecnológicos de información de una organización.

Tabla 4. Fuentes de amenaza comunes.

Fuente de amenaza	Descripción
Amenazas Naturales	Inundaciones, terremotos, tornados, avalanchas, derrumbes, tormentas eléctricas y otros eventos similares.
Amenazas Humanas	Eventos que son habilitados o causados por seres humanos, como lo son actos sin intención (entrada de datos errónea) o acciones deliberadas (Ataques a la red, propagación de software malicioso, acceso no autorizado a información confidencial).
Amenazas ambientales	Falla eléctrica de largo plazo, polución, químicos, goteo de líquidos.

Fuente: Recuperado de(Kelley, 2014).

Los seres humanos, son por defecto las más potencialmente peligrosas fuentes de amenaza, ya que, pueden tener diferentes motivaciones y recursos para poder efectuar un ataque en contra de un sistema tecnológico de información. En el anexo 5.1, se hace un resumen de las actuales amenazas que pueden ser ejecutadas por un ser humano, se enuncian posibles motivaciones y acciones de amenaza para materializar un ataque. A modo de conclusión, una lista de fuentes potenciales de amenaza debe ser desarrollada individualmente por la organización, teniendo en cuenta el entorno en el cual desarrolla su operación.

2.8.3 Factor de Riesgo 2: Vulnerabilidades.

La vulnerabilidad en un sistema tecnológico de información se define, como un falla o debilidad en los procesos de seguridad, diseño, implementación y/o controles internos, que podrían ser activados (de manera accidental o intencionada) y terminar en una brecha de seguridad o violación de la seguridad de un sistema tecnológico de información. La mayoría de vulnerabilidades en sistemas de información pueden ser asociados con controles de seguridad, los cuales pudieron no haber sido aplicados (ya sea intencionalmente o no intencionalmente) o que fueron aplicados, pero mantienen alguna debilidad frente a la vulnerabilidad que se intentaba mitigar (Kelley, 2014; National Institute of Standards and Technology Gaithersburg, 2012).

Las fuentes de vulnerabilidades, ya sean técnicas o no técnicas asociadas al entorno del procesamiento del sistema tecnológico de información, pueden ser recolectadas y documentadas de varias maneras. Siendo inicialmente una forma de recolección de valoración interna, ya que, dentro de la organización, se puede aplicar diferentes métodos como: cuestionarios, entrevistas en sitio, revisión de documentación y/o uso de herramientas automáticas de escaneo. Seguidamente la revisión con fabricantes referentes a las vulnerabilidades encontradas en sus sistemas son una buena fuente de documentación, ya que el fabricante, expondrá la vulnerabilidad y posiblemente los pasos a seguir para mitigarla. Finalmente, fuentes documentadas de vulnerabilidades deberían ser consideradas dichas fuentes pueden ser: anteriores evaluaciones de riesgo, reportes de auditoría a los sistemas de información tecnológicos, listas de vulnerabilidades, avisos de seguridad expuestos por entidades dedicados al estudio de seguridad de la información, avisos de fabricantes, análisis de seguridad de software, alertas y boletines expedidos por entidades militares (Kelley, 2014).

Las vulnerabilidades no son solamente identificadas a nivel técnico, las vulnerabilidades pueden ser encontradas en estructuras de gobierno organizacional (por ejemplo: la falta de la apropiada estrategia para la administración del riesgo, pobre comunicación entre departamentos de la misma organización, decisiones inconsistentes sobre prioridades en función de la misión y/o negocio de la organización), también, dichas vulnerabilidades, se pueden encontrar en relaciones de la organización con entidades externas (por ejemplo, dependencias particulares en el suministro eléctrico,

cadena de suministro, proveedores de telecomunicaciones, proveedores de tecnología, entre otros), más aún, se pueden encontrar vulnerabilidades en la misión o procesos del negocio (por ejemplo, definiciones pobres de procesos o procesos que se ejecutan sin tener en cuenta el riesgo que involucra para la organización) y en definitiva se puede encontrar vulnerabilidades en arquitecturas de seguridad para la información y/o la organización (por ejemplo, decisiones pobres de arquitectura que concluyen en una falta de diversidad o resistencia en sistemas organizacionales de información) (National Institute of Standards and Technology Gaithersburg, 2012).

El uso de métodos proactivos contribuye a tener una mejor identificación de vulnerabilidades en los sistemas tecnológicos de información, dichos métodos pueden ser: el uso de herramientas automáticas que escanean vulnerabilidades, evaluaciones y pruebas de seguridad, pruebas de penetración, aplicación de entrevistas, entendimiento organización, entre otros (Kelley, 2014). El uso de los métodos mencionados, contribuyen a que la organización tenga una visión más holística de las posibles vulnerabilidades que pueden tener sus sistemas tecnológicos de información y a su vez el entorno donde prestan servicios. En el anexo 5.2, se enuncian algunos ejemplos de pares de vulnerabilidades y amenazas, se hace referencia la fuente de amenaza y la acción de amenaza que podría ser ejecutada para poder tomar provecho de la vulnerabilidad encontrada. Como conclusión el riesgo se materializa como el resultado de una serie de amenazas, donde cada evento tomará ventaja de una o más vulnerabilidades (National Institute of Standards and Technology Gaithersburg, 2012).

2.8.4 Factor de Riesgo 3: Condiciones de predisposición.

Se define como la condición que existe entre la organización y su misión o proceso de negocio, arquitectura empresarial, sistema tecnológico de información, en torno de operación que afecta (por ejemplo: incrementar o decrementar) la probabilidad de un evento de amenaza la cual, una vez sea iniciada, concluye en impactos adversos para operación, activos, individuos de la organización. Condiciones de predisposición involucran, por ejemplo: la ubicación de las instalaciones de una organización propensa a eventos naturales (huracanes, inundaciones, terremotos, etc.). Vulnerabilidades que

resulten de una condición de predisposición que no puede ser corregidas fácilmente incluyen, por ejemplo, brechas en planes de contingencia, uso de tecnologías antiguas o debilidades y/o deficiencias en el respaldo de sistemas tecnológicos de información y mecanismos de continuidad del negocio. En todos los casos los tipos de vulnerabilidades que se han mencionado crean una predisposición frente un evento de amenaza trayendo un impacto adverso para la organización (National Institute of Standards and Technology Gaithersburg, 2012).

2.9 Marcos para la evaluación del riesgo

En este apartado, se pretende dar al lector un conocimiento sobre algunos de los marcos que existen para la evaluación del riesgo en tecnologías de la información, cabe resaltar que existen diferentes tipos de marcos los nombrados a continuación son los que más se ajustan a la problemática que se desea resolver para la Organización XYZ.

El éxito de la evaluación del riesgo es completamente dependiente de la información recogida con el fin de hacer conciso y exacto el planeamiento de decisiones en seguridad de la información (Shamala et al., 2013).

Podría ser muy conveniente para las organizaciones un método comprensivo que acomode los diferentes requerimientos de los métodos existentes, en una buena y mejorada forma. Esto soportaría una compatibilidad de la evaluación del riesgo a través de diferentes organizaciones, ofreciendo un ambiente común y seguro para el negocio (Saleh & Alfantookh, 2011).

La mayoría de las metodologías existentes, concuerdan que profesionales que los evalúan el riesgo, deben tener habilidades, cualidades, experiencia y entrenamiento. Esto debido, a que quienes tienen estas características, podrían ser capaces de recolectar y analizar la información acertadamente y hacer admisible las decisiones determinadas durante la evaluación del riesgo (Shamala et al., 2013).

2.9.1 Marcos sujetos al ciclo de Deming.

Varios de los marcos encontrados en la investigación están alineados al ciclo propuesto por el Dr. W. Edwards Deming y el posterior análisis hechos por ejecutivos japoneses (Imai, 1986), el ciclo resultante de esta investigación es nombrado *PDCA cycle*. (Ciclo PDCA) (Moen & Norman, 2009)



Figura 5. Ciclos de Propuesto Dr. Edwards Deming

Fuente: recuperado de(Moen & Norman, 2009).

Los 4 pasos del ciclo expuestos en la figura se describen a continuación. *Plan* (planear): definir el problema e hipótesis sobre posibles causas y soluciones. *Do* (hacer): Implementar. *Check* (verificar): Evaluación de los resultados. *Action* (acción): retornar al plan si los resultados son insatisfactorios o estandarización si los resultados son satisfactorios (Moen & Norman, 2009).

2.9.1.1. A conceptual framework of info-structure¹⁵ for ISRA¹⁶ (Marco conceptual de info-estructura para la evaluación del riesgo).

Este marco es el resultado de la investigación hecha por Shamala, Ahmad y Yusoff, donde se analizaron 5 metodologías que son comunes para la evaluación de riesgo las cuales son: CRAMM¹⁷, CORAS¹⁸, OCTAVE¹⁹, ISRAM²⁰, NIST 800-30²¹.

Las metodologías analizadas, concuerdan en que tienen características similares en el estudio de comparación realizado. El objetivo principal de todas las metodologías ISRA es el reducir, mitigar transferir o aceptar el riesgo a un nivel aceptable. Cualquier organización sin importar el tamaño, tienen que asegurarse que la siguiente información sea recolectada de manera precisa: Requerimientos de la gerencia, establecer un contexto organizacional, identificar riesgos y vulnerabilidades en los recursos, mejora en la gestión del riesgo (Shamala et al., 2013). Dicha información es la estructura base para el marco propuesto el cual se expone en la figura 6.

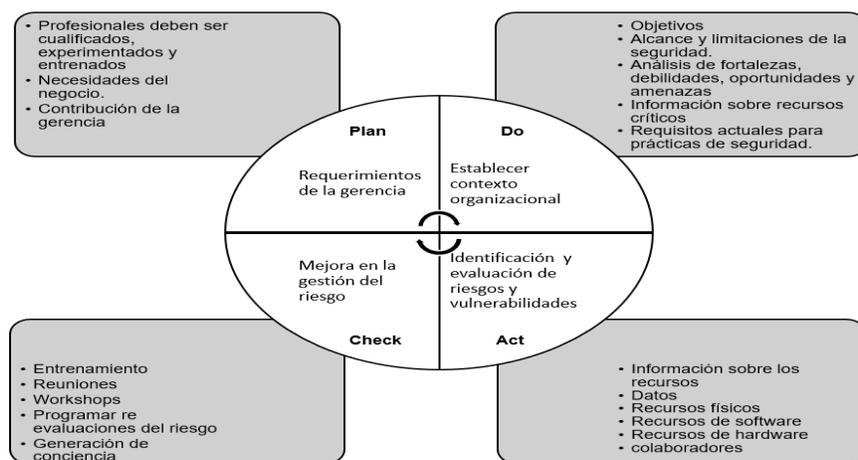


Figura 6. Estructura base

Fuente: (Shamala et al., 2013).

¹⁵ Info-structure (Info-estructura): Es el diseño de la información la cual está organizada de una forma que pueda ser usable y que puede ser analizada en cualquier momento (Shamala et al., 2013).

¹⁶ ISRA (Information Security Risk Assessment): evaluación del riesgo para seguridad de la información (Shamala et al., 2013).

¹⁷ CRAMM, CTA Risk Analysis and Management Method.

¹⁸ CORAS, Método para Conducir Evaluaciones de Riesgo.

¹⁹ OCTAVE, The Operationally Critical Threat, Asset, and Vulnerability Evaluation SM.

²⁰ ISRAM, Information Security Risk Analysis Method.

²¹ NIST 800 -30, National Institute of Standards and Technology. Guide for Conducting Risk Assessments.

Cada fase hace mención de una serie de actividades, las mismas son importantes para poder hacer la evaluación de riesgo y posterior monitoreo del riesgo.

Las características que resaltan de este método son dos, inicialmente el límite de la evaluación de riesgo es establecido en las actividades referentes a la identificación de recursos críticos para identificar la prioridad en protección de los recursos mencionados. (Shamala et al., 2013). Como segunda característica, el marco hace referencia entrenamiento, reuniones, workshops, entre otros en la fase de verificación. ISRA es considerado como un proceso continuo que necesita ser monitoreado y generador de conciencia en los colaboradores (Shamala et al., 2013). En pocas palabras, Shamala, Ahmad y Yusoff, concluyen que el marco expuesto anteriormente para ISRA puede ser usado para complementar la planificación requerida en seguridad de la información, seguido de la selección de las más adecuadas metodologías con el fin de tener una buena evaluación del riesgo en sistemas de información (Shamala et al., 2013).

2.9.1.2 ISRA framework for the cloud computing environments (marco de evaluación del riesgo para ambientes de computación en la nube).

El autor de este documento hace la integración de un marco del análisis de riesgos de computación en la nube, ya que, hoy en día un gran número de empresas tercerizan servicios en la nube. Al mismo tiempo, este marco se desarrolla en un entorno similar al caso de estudio de la Organización XYZ.

Xuan Zhang, Wuwong, Li y Xuejie Zhang, desarrollaron este marco a partir de la integración del ciclo de Deming, estándar ISO 27001, guía de evaluación del riesgo de NIST y el marco de Gobierno de Seguridad de la Información para la computación de la nube desarrollado por Bozz Allen Hamilton.

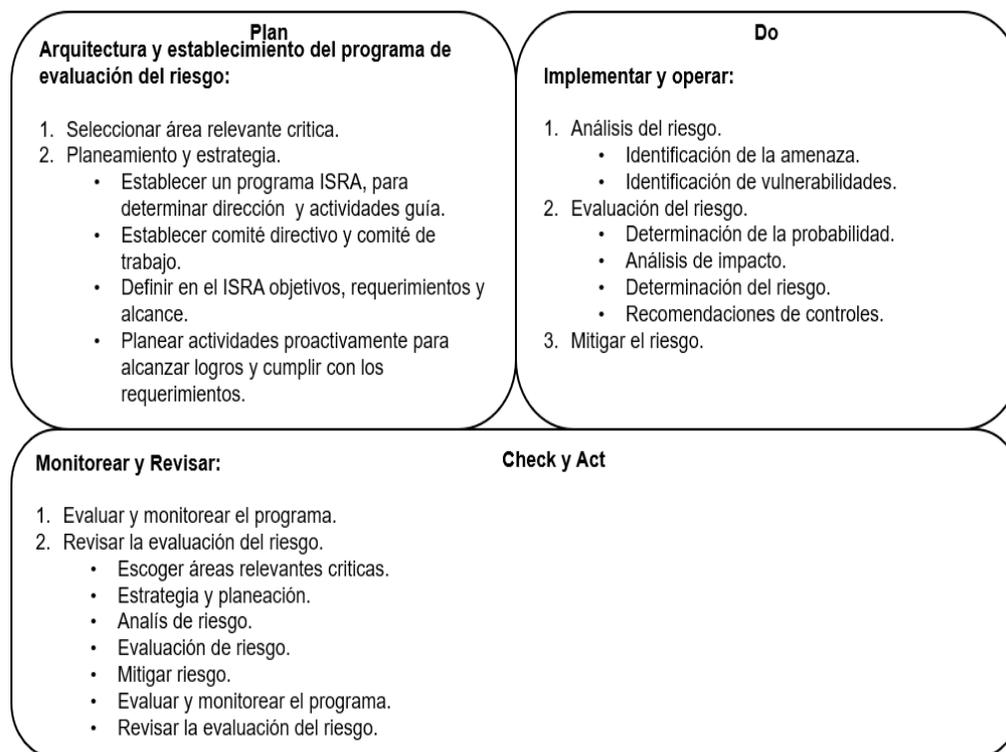


Figura 7. Integración del Ciclo Deming

Fuente: Recuperado de (Zhang et al., 2010).

La nube ofrece un modelo eficiente, escalable y una forma de costo efectivo para las organizaciones de hoy en día, con el objetivo de entregar servicios, consumo de tecnologías de la información a través de internet (Zhang et al., 2010).

Xuan Zhang, Wuwong, Li y Xuejie Zhang, hacen referencia a tres fases, donde se enlistan siete procesos fundamentales para la evaluación del riesgo, dichos procesos son: Áreas de relevancia crítica, estrategia y planeación, análisis de riesgo, evaluación del riesgo, mitigación del riesgo, evaluar y monitorear el programa; y, por último, la revisión de la evaluación del riesgo (Zhang et al., 2010). En la figura 8 se muestra de una forma más simplificada el marco expuesto, vale la pena resaltar que en el proceso número 1 se hace referencia a áreas relevantes críticas propias de la computación en la nube.

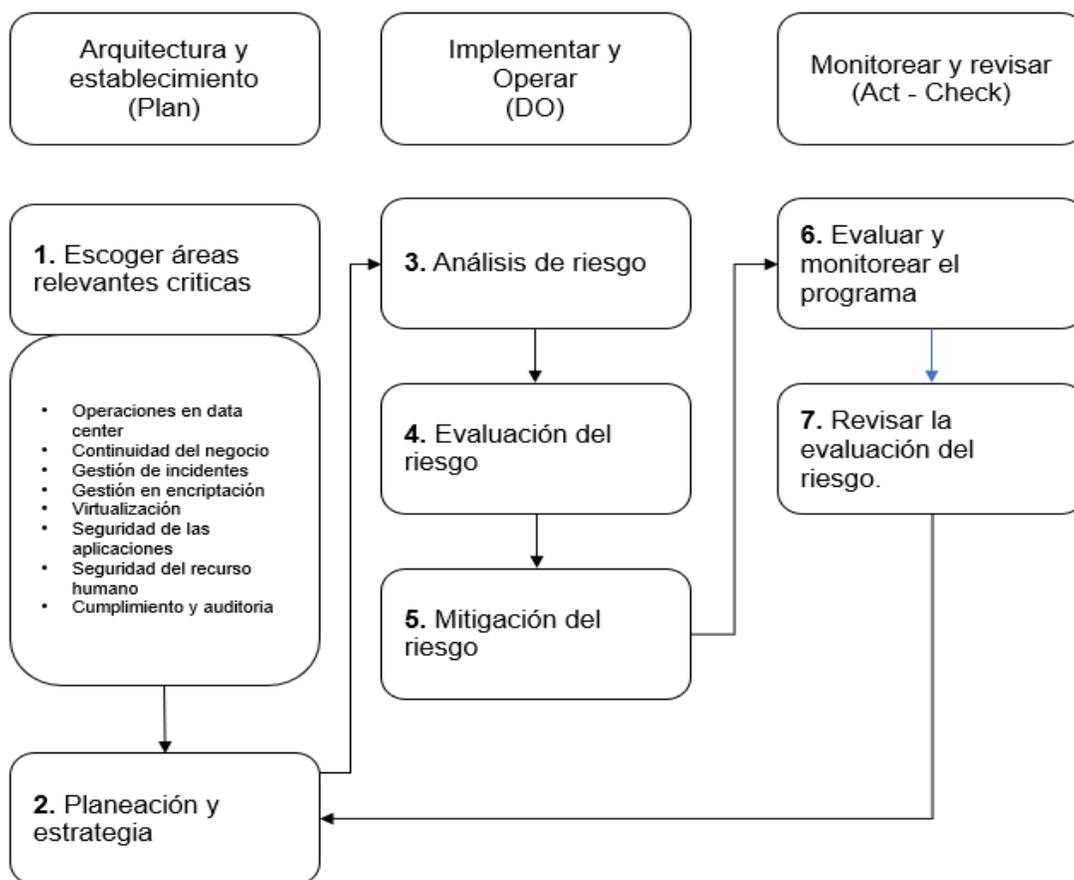


Figura 8. Procesos fundamentales para la evaluación del riesgo

Fuente: Recuperado de (Zhang et al., 2010).

En definitiva, se concluye que, cantidades masivas de recursos de tecnologías de la información son compartidos a través de varios usuarios, los procesos de seguridad usualmente están más escondidos detrás de capas de abstracción. Computación en la nube está siendo ofrecida usualmente como servicio, entonces, el control sobre los datos y la operación es movida a organizaciones que tercerizan el servicio, requiriendo establecer relaciones de confianza entre el cliente corporativo y organizaciones que tercerizan servicios (Zhang et al., 2010).

2.9.1.3 Risk and compliance management framework for outsourced GSD²² (Marco de riesgo y cumplimiento para tercerización de desarrollo de software)

SABSA²³ provee marcos integrados, modelos, métodos y procesos que tienen orientación al riesgo, manejando amenazas y oportunidades (Burkett, 2012).

En un ambiente de tercerización, la cultura y distancia geográfica, incrementan la complejidad y el riesgo (Magnu & Chou, 2010), en el momento de entregar el servicio a clientes corporativos. Magnu y Chou identifican en su investigación cuatro categorías de riesgo a los que está expuesto un servicio tercerizado, los cuales son: eficiencia, presencia, talento, flexibilidad (Magnu & Chou, 2010).

SABSA le da herramientas a los profesionales de seguridad para convertirse en proveedores de soluciones de seguridad en vez de inhibidores, como se ha intentado estigmatizar. El reportar la seguridad de la información de la organización, idea de que el riesgo existe, aun así, no muestra a las organizaciones cómo convertirse más seguras mientras se mitiga el riesgo. SABSA le entrega a la organización una ruta para proteger los recursos críticos de la organización a través del desarrollo del proceso de SABSA, entregando soluciones seguras a la vista de las seis capas de la organización (Burkett, 2012).

Se ha identificado que varias organizaciones diseñan adquieren e instalan soluciones de seguridad de la información como parte de la táctica básica de la organización (Sherwood et al., 2009), claro ejemplo de esto es la implementación de infraestructura básica la cual acarrea grandes costos.

Dichas soluciones no contemplan varios factores que deberían estar considerados en la visión estratégica de la organización, estos son soporte de las soluciones que están instaladas, tales costos operativos, entre otros; como lo define SABSA en su whitepaper.

²² GSD, Global Software Development, Desarrollo Global de Software

²³ SABSA. The Sherwood Applied Business Security Architecture.

El desarrollo de una arquitectura empresarial en seguridad de la información impulsada por el negocio donde describa una relación estructurada entre lo técnico y soluciones procedimentales es el marco propuesto por SABSA.

El modelo está compuesto por 6 capas 5 horizontales y 1 vertical, como se observa en la figura 9, se toma como base el modelo desarrollado por John A. Zachman y se adapta al mundo de seguridad de la información. Cada capa representa la visión de los diferentes jugadores involucrados en el proceso. En cada capa se tienen 6 factores los cuales son: recursos, motivaciones, procesos, personas, ubicación y tiempo (Magnu & Chou, 2010).



Figura 9. Modelo de relación estructurada.

Fuente: Recuperado de (Sherwood et al., 2009)

En el marco propuesto por Magnu y Chou, clasifican la evaluación del riesgo en 3 diferentes tipos: tipo 1: evaluación del riesgo a un nivel de negocio, tipo 2: evaluación del riesgo al nivel operacional, tipo 3: evaluación del riesgo a nivel de proyectos (Magnu & Chou, 2010).

La capa contextual hace referencia en el poder extraer los requerimientos del ambiente del negocio basado en los recursos y restricciones organizacionales. La capa conceptual generaliza objetivos de la gerencia dentro de políticas, procedimientos y procesos. La capa lógica, es donde los controles de seguridad son detallados, igualmente procedimientos gerenciales son diseñados y definidos. La capa lógica es esencial para la transformación de requerimientos abstractos a especificaciones del

sistema. La capa física y de componentes, de acuerdo con la estrategia de servicio a proveer, es donde los profesionales pueden generar tácticas para los mecanismos de seguridad y aplicarlos dentro de los servicios de tercerización.

En conclusión, la capa de gerencia del servicio es el facilitador para las 5 capas expuestas previamente, esta capa requiere actividades colaborativas para asegurar que las características de la arquitectura de seguridad están alineadas con los requerimientos del negocio (Magnu & Chou, 2010; Sherwood et al., 2009).

Magnu y Chou integran ISO27001, ISO2000 y COSO-ERM, junto con SABSA para poder ofrecer un modelo más robusto de evaluación del riesgo. Afirman que se puede lograr un mayor cumplimiento de seguridad de la información ya que el grupo de interesados está más involucrado. Los requerimientos serán transformados gradualmente en estrategias de seguridad, políticas, estructuras de sistemas y características funcionales, el modelo se puede observar en la figura 10.

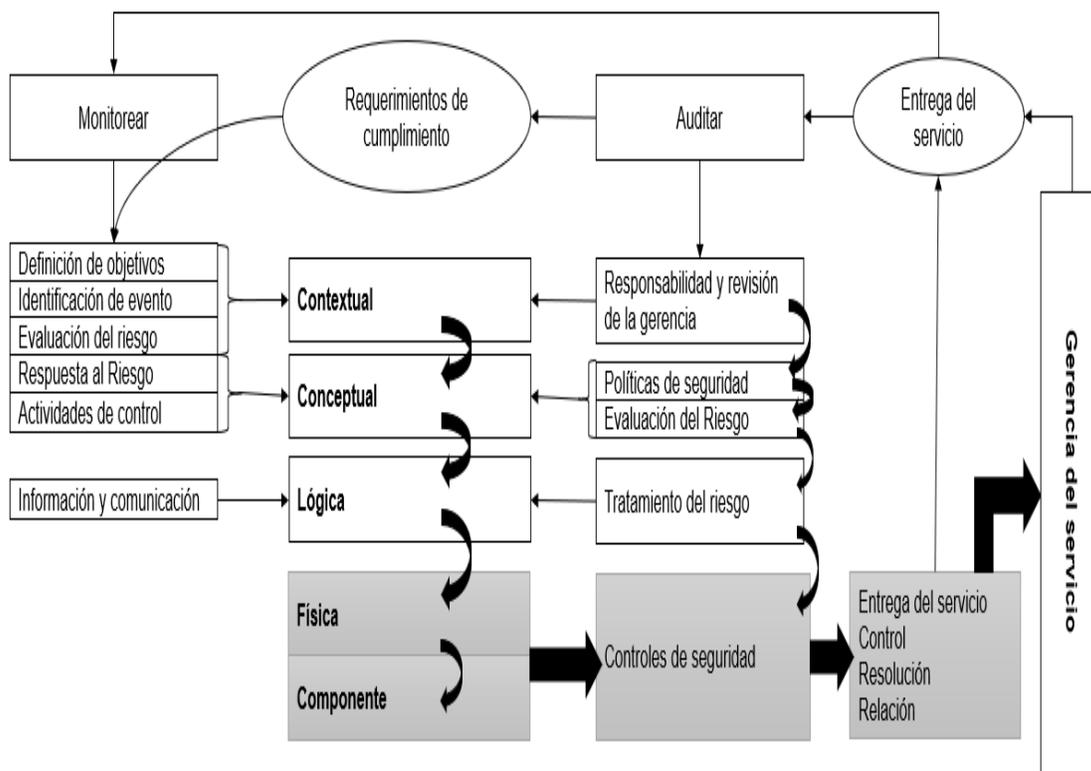


Figura 10. Modelo en estrategias de seguridad, políticas, estructuras de sistemas y características funcionales.

Fuente: Recuperado de (Magnu & Chou, 2010).

Magnu y Chou (2010), dividen el marco en 4 fases. Fase de estrategia: administrada por el cliente corporativo que desea tercerizar el servicio. Fase de implementación: administrada por la organización que está dispuesta a tercerizar. Fase de la gestión del cambio y configuración: administrada en conjunto por el cliente corporativo y la organización que terceriza servicios. Fase de auditoría: administrada por el cliente. (Magnu & Chou, 2010). En la figura 10 se muestra la relación de las fases con el modelo SABSA.

La fase de estrategia, integra la capa contextual, conceptual y de lógica del modelo SABSA. Esta fase cubre el proceso estratégico en la preparación de servicios de tercerización. Esta fase da respuesta a los riesgos tipo 1 y tipo 2 (Magnu & Chou, 2010).

En la fase de implementación, el arquitecto de la organización que terceriza servicios genera tácticas para la aplicación de controles de seguridad. El arquitecto escoge el más apropiado mecanismo de seguridad permitiéndole a la organización que terceriza, implementar dichos controles en la capa física y de componentes (Magnu & Chou, 2010). En la Figura 10 se evidencia este proceso en los rectángulos de color gris.

Fase de la gestión del cambio y configuración: esta fase está asociada con la capa de gerencia del servicio en el modelo SABSA, esta fase establece apropiados procedimientos entre el cliente corporativo y la organización que terceriza servicios. Estos dos procesos de gestión son cruciales para sostener la operación tecnológica del cliente corporativo (Magnu & Chou, 2010). Esta fase da respuesta al riesgo tipo 3 previamente definido.

Eventualmente, la fase de Monitoreo y cumplimiento, ayudan al cliente corporativo a validar si el servicio cumple con los requerimientos previamente definidos. (Magnu & Chou, 2010). Esta fase da respuestas a todos los niveles de riesgo previamente expuestos. Con lo anterior, se concluye que un modelo de tercerización es una opción para la reducción de costos, aunque, los servicios ofrecidos por organizaciones que tercerizan deben estar construidas bajo un buen diseño de arquitectura empresarial, el cual contribuye a identificar e implementar los controles de seguridad que estos requieran. Por otro lado, el autor enfatiza en los riesgos de gerenciamiento remoto de

personas, barreras socioculturales, distancia en tiempo y geográfica, obstáculos de comunicación y la integración de fuerzas de trabajo (Magnu & Chou, 2010).

2.10 Determinación del Riesgo

Con el objetivo de poder determinar de una forma efectiva el riesgo en un sistema tecnológico de información, es necesario definir la probabilidad y el impacto que pudiera llegar a materializarse.

2.10.1 Factor de Riesgo 3: Probabilidad.

NIST sugiere que la calificación de probabilidad general para que una potencial vulnerabilidad sea materializada debe tomar en cuenta las amenazas asociadas al entorno donde opera o presta servicios el sistema tecnológico de información, los siguientes factores gobernantes deben ser considerados: 1. Motivaciones y capacidades de la fuente de amenaza, 2. Naturaleza de la vulnerabilidad, 3. Existencia y efectividad de los controles actuales (Kelley, 2014).

La tabla a continuación toma en cuenta los factores gobernantes mencionados previamente y permiten definir la probabilidad de que una potencial vulnerabilidad sea ejecutada, dicha definición de probabilidad se define en tres niveles, bajo, medio y alto.

Tabla 5. Definición de Probabilidad.

Nivel de Probabilidad	Definición de probabilidad
Alto	La fuente de amenaza está altamente motivada, suficientemente capaz y los controles para prevenir la vulnerabilidad de que sea ejecutada no son suficientes.
Medio	La fuente de amenaza está motivada y capaz, pero los controles están dispuestos, lo cual podría impedir una ejecución efectiva de la vulnerabilidad.
Bajo	La fuente de amenaza carece de motivación, o capacidad, o los controles están dispuestos para prevenir o al menos suficientemente impedidos para que la vulnerabilidad sea ejecutada.

Fuente: Recuperado de (Kelley, 2014).

2.10.2 Factor de Riesgo 4: Impacto.

Para poder determinar el impacto que pueda resultar de la ejecución efectiva de una vulnerabilidad, es necesario determinar qué tan sensible es el sistema tecnológico de información impactado, dicha sensibilidad puede ser compartida por el administrador o por los usuarios a quienes se les presta el servicio, ya que estos, comprenden que información y/o servicio es procesada en dichos sistemas. Por lo tanto, el impacto adverso de un evento de seguridad puede ser descrito en términos de los objetivos principales de seguridad de la información: pérdida de integridad, de disponibilidad, de confidencialidad. El impacto de un evento de seguridad puede ser medido de forma cuantitativa o cualitativa, en términos de cuantía se hace referencia en pérdida de ingresos, costos de reparación del sistema tecnológico de información, o el esfuerzo hecho para poder corregir el problema. Impactos como la pérdida de confidencialidad, de credibilidad, daños a los intereses de una organización, no pueden ser medidos en cantidades; ya que, se pueden describir en términos de alto, medio o bajo impactos (Kelley, 2014).

Tanto de forma cuantitativa como cualitativa, el evaluador puede determinar qué tan alto medio o bajo puede llegar a ser el impacto causado por la ejecución efectiva de la vulnerabilidad en la tabla 6, se brinda una mejor definición.

Tabla 6. Definición de magnitud de impacto,

Magnitud del impacto	Definición de impacto
Alto	Ejecución de vulnerabilidad que resulta en una pérdida muy costosa de activos mayores tangibles y/o recursos de una organización.
	Ejecución de vulnerabilidad que significativamente viola, daña o impide el desarrollo de la misión, reputación o intereses de una organización.
	Ejecución de vulnerabilidad que resulta en una muerte humana o una seria lesión.
Medio	Ejecución de vulnerabilidad que puede resultar en pérdida costosa de activos mayores tangibles y/o recursos de una organización.
	Ejecución de vulnerabilidad que viola, daña o impide el desarrollo de la misión, reputación o intereses de una organización.
	Ejecución de vulnerabilidad que resulta en una lesión humana.
Bajo	Ejecución de vulnerabilidad que puede resultar en la pérdida de algunos activos y/o recursos
	Ejecución de vulnerabilidad que puede afectar notablemente la misión, reputación o interés de una organización.

Fuente: Recuperado de (Kelley, 2014).

La determinación del riesgo para una vulnerabilidad/amenaza puede ser expresada en función de: 1. La probabilidad de que fuentes determinadas de amenaza, intenten ejecutar una vulnerabilidad conocida, 2. La magnitud de impacto en caso de que una fuente de amenaza ejecute de forma exitosa una vulnerabilidad, 3. Adecuación de los controles de seguridad existentes o lo que se planificaran para reducir o eliminar el riesgo (Kelley, 2014).

La determinación de riesgo puede ser subjetiva, es evaluada por el experto en seguridad de la información, a continuación, se enuncia un ejemplo (tabla 7), en donde se asignó por cada nivel de amenaza (alto, medio y bajo) un valor de probabilidad, para un nivel de amenaza alto se asigna un valor de probabilidad de 1, para media 0.5 y para baja 0.1. Para cada nivel de impacto, se asignan los siguientes valores 100 para un nivel alto de impacto, 50 para medio y 10 para bajo.

Tabla 7. Matriz Nivel de Riesgo.

Probabilidad de Amenaza	Impacto		
	Alto (10)	Medio (50)	Bajo (100)
Alto (1.0)	Alto $100 \times 1.0 = 100$	Medio $50 \times 1.0 = 50$	Bajo $10 \times 1.0 = 10$
Medio (0.5)	Medio $100 \times 0.5 = 50$	Medio $50 \times 0.5 = 25$	Bajo $10 \times 0.5 = 5$
Bajo (0.1)	Bajo $100 \times 0.1 = 10$	Bajo $50 \times 0.1 = 5$	Bajo $10 \times 0.1 = 1$

Fuente. Recuperado de Kelley (2014).

Por lo tanto, con los tres niveles de riesgos expuestos, NIST sugiere acciones que deben ser llevadas a cabo por la alta gerencia con el fin de mitigar a niveles razonables el riesgo en los sistemas tecnológicos de información, para su funcionamiento y/o prestación de servicios sea cual sea la organización o industria donde opere, dichas sugerencias se enuncian en la tabla 8.

Tabla 8. Escala de riesgo, recomendación de acciones y sugerencias.

Nivel De Riesgo	Descripción de Riesgo y sugerencia
Alto	Si una observación es calificada como riesgo alto, es muy necesario aplicar medidas correctivas. Un sistema existente podría continuar su operación, pero un plan de acciones correctivas debe ser desarrollado tan pronto como sea posible.
Medio	Si una observación es calificada como riesgo medio. Acciones correctivas son necesarias y un plan de mitigación debe ser aplicado en un periodo de tiempo razonable.
Bajo	Si una observación es descrita como baja, la autoridad designada de aprobación para el sistema deberá determinar ya sea: acciones correctivas pendientes para controlar totalmente el riesgo o decidir si se acepta el riesgo.

Fuente: Recuperado de Kelley (2014).

2.11 Controles del Riesgo.

Con el fin de poder controlar el riesgo que se determina en un sistema tecnológico de información, se emplean buenas prácticas que ayudan a poder mitigar de una forma más efectiva el riesgo, dicha mitigación se hace mediante controles sugeridos por dichas buenas prácticas. Dentro de estas buenas prácticas se debe tener en cuenta que están alineadas al entorno en el que opera la Organización XYZ, por ejemplo, un entorno donde se maneja información de tarjetas de crédito entre otra información sensible.

Las buenas prácticas hacen referencia a dos estándares muy acogidos en la industria, dichos estándares son PCI DSS e ISO/IEC 1799:2005. Los estándares ofrecen una guía a los Gerentes de Seguridad de la Información para determinar de una forma más acertada el riesgo al que puede estar expuesto el sistema tecnológico de información y/o la operación para la que está dispuesto, y sugiere qué controles debe implementar el equipo de tecnología con el fin de garantizar una apropiada mitigación del riesgo. Esta evaluación se debe ajustar a que el negocio no se impacte

negativamente y que se cumplan las políticas de seguridad de la información. Por lo que, la mayoría de las evaluaciones de riesgo son de carácter cualitativo.

2.11.1 PCI DSS.

Payment Card Industry Data Security Standard PCI DSS (Estándar de seguridad de datos para industria de pagos con tarjetas de crédito) Dicho estándar está enfocado en la seguridad de la información para tarjetahabientes con el fin de: motivar y mejorar la seguridad de datos de tarjetas de crédito, facilitar una completa adopción que sea consistente a nivel global. PCI DSS provee una línea base de requerimientos técnicos y operacionales diseñados con el fin de proteger información de tarjetas. Dicho estándar es aplicado a todas las entidades involucradas en el procesamiento de pagos. PCI DSS también involucra a entidades terceras que almacenan, procesan y/o transmiten información de tarjetahabientes (PCI Security Standards Council, 2013). En la tabla 9 se muestra a un alto nivel de qué trata este estándar el cual tiene 12 requerimientos principales a cubrir.

Tabla 9. Controles PCI DSS a alto nivel.

Alcance	Requerimiento Principal
Construir y mantener una red y sistemas seguros	1. Instalar y mantener la configuración de un firewall para proteger datos de un tarjetahabiente. 2. No usar contraseñas u otro parámetro de seguridad entregados por defectos por proveedores.
Proteger información de tarjetahabiente	3. Proteger información almacenada de tarjetahabiente. 4. Encriptar transmisión de datos de tarjetahabiente a través de redes abiertas y/o públicas.
Mantener un programa de administración de vulnerabilidades.	5. Proteger todos los sistemas en contra de malware y actualizar regularmente software referente a antivirus o programas usados para operación. 6. Desarrollar y mantener sistemas y aplicaciones seguros.
Implementar medidas fuertes de control de acceso	7. Restringir acceso a información de tarjetahabientes por necesidad del negocio en saber. 8. Identificar y autenticar el acceso de los componentes

Alcance	Requerimiento Principal
	del sistema. 9. Restringir acceso físico a datos de tarjetahabiente
Regularmente monitorear y probar redes	10. Monitorear y hacer seguimiento a todos los accesos a los recursos de la red y datos del tarjetahabiente. 11. Regularmente probar seguridad de sistemas y procesos.
Mantener una política de seguridad de la información.	12. Mantener una política que guíe en seguridad de la información a los miembros de la organización.

Fuente: Recuperado de PCI Security Standards Council (2013).

Cada requerimiento principal se divide en requerimientos de segundo nivel, que deben satisfacer al requerimiento principal, dichos requerimientos de segundo nivel se asocian con unos procedimientos de pruebas, los cuales sirven de guía para el evaluador con el fin de validar si los requerimientos de segundo nivel se cumplen y a su vez los requerimientos principales establecidos por PCI DSS. Es decir, por cada requerimiento de segundo nivel y procedimiento de pruebas se asocia un alcance, que enuncia el objetivo de seguridad que se pretende cubrir con cada requerimiento de segundo nivel. En el anexo 5.6, se muestra una página de cómo es el documento que se toma como base al momento de hacer el análisis de riesgos tomando como base el estándar PCI DSS. Por motivos de derecho de autor no se puede anexar la totalidad del documento.

2.11.2 ISO/IEC 27002:2005.

Es un estándar desarrollado por ISO ²⁴ e IEC²⁵, el cual ofrece guía y fundamentos básicos para la iniciación, implementación, mantenimiento y mejoramiento de un sistema de seguridad para la información en cualquier organización. El estándar hace referencia a “controles”, este término es definido como una forma de manejar el riesgo. El objetivo del control es mitigar el riesgo identificado en la evaluación de riesgo (ISO & IEC, 2013).

²⁴ The International Organization for Standardization (Organización Internacional de Estandarización).

²⁵ The International Electrotechnical Commission (Comisión Internacional Electrotécnica).

El estándar ISO/IEC 27002:2005 está diseñado en 11 cláusulas y cada una de ellas contiene un número definido de categorías principales de seguridad. Por cada categoría principal de seguridad se enuncia un control objetivo refiriéndose a que es lo que se desea alcanzar, también se enuncian uno o más controles que pueden ser aplicados para alcanzar el objetivo del control (ISO & IEC, 2013).

A continuación, en la tabla 10, se ofrece una descripción a alto nivel sobre las cláusulas y categorías de seguridad abordados por el estándar.

Tabla 10. Cláusulas y Categorías de Seguridad de ISO/IEC 27002:2005

Cláusula de Seguridad	Categoría principal de seguridad
Política de seguridad	Política de seguridad de la información
Seguridad de la información en la organización	Organización interna
	Partes externas
Manejo de activos	Responsabilidad por Activos
	Clasificación de la información
Seguridad del recurso humano	Antes de emplear
	Durante el empleo
	Terminación o Cambio de empleo
Seguridad física	Áreas Seguras
	Seguridad Equipos
Comunicación y gestión de la operación	Procedimientos y responsabilidades Operacionales
	Gestión de la entrega de servicio con terceros
	Planeación y aceptación de sistemas de información
	Protección contra códigos maliciosos y móviles
	Respaldo de la información (Backups)
	Administración seguridad de la red
	Administración de dispositivos de almacenamiento de información
	Intercambio de información.
	Servicios de comercio electrónico
Monitoreo	

Cláusula de Seguridad	Categoría principal de seguridad
Control de acceso	Requerimientos del negocio para control de acceso
	Administración de acceso para usuarios
	Responsabilidades del usuario
	Control de acceso a la red
	Control de acceso a sistema operativo
	Aplicaciones e información del control de acceso.
	Computadores portátiles y teletrabajo
Adquisición de sistemas de información, desarrollo y mantenimiento	Requerimientos de seguridad para sistemas de información
	Procesamiento correcto en aplicaciones
	Controles de criptografía
	Seguridad de archivos del sistema
	Seguridad en procesos de desarrollo y soporte
	Administración de vulnerabilidades técnicas
Administraciones incidentes de seguridad de la información	Reportar eventos y debilidades de seguridad de la información
	Administración de incidentes de seguridad de la información y mejoras
Administración de continuidad del negocio	Aspectos de seguridad de la información para la administración de la continuidad del negocio
Cumplimiento	Cumplimiento con requerimientos legales
	Cumplimiento técnico, políticas y estándares de seguridad de la información
	Consideraciones en auditoría a sistemas de información

Fuente: ISO & IEC (2013).

3. Metodología de Investigación

3.1 Tipo de investigación

La investigación hizo uso de métodos cualitativos, dichos métodos contribuyeron en la recolección de la información que sirvió de base para la interpretación y análisis por parte del investigador para el hecho empresarial. Se hizo uso de 3 instrumentos para la recolección de información, con el objetivo de encontrar convergencia y corroboración a través del uso de diferentes fuentes de información y métodos (Bowen, Rowley Healy, & Perry, 2009). Se requirió la colaboración de las 3 áreas claves en la resolución de este hecho empresarial, dichas áreas fueron: operaciones, tecnología y seguridad de la información, donde fue mandatorio extraer información mediante el uso de técnicas robustas en la recolección de datos, las cuales fueron requeridas por el método de investigación cualitativo (Bowen et al., 2009).

3.2 Instrumentos para la recolección de la información

Para el desarrollo de esta investigación se procedió a hacer uso de los siguientes métodos cualitativos: observación, análisis de documentos y entrevista; dichos métodos fueron esenciales para la obtención de la información.

3.2.1 Observación

Este instrumento posee 2 tipos de enfoques estructurado o desestructurado (Pretzlik, 1994), para el hecho empresarial que es materia de estudio de este documento, se enfocó a una perspectiva desestructurada. De esta forma se corroboró si lo expresado por las personas efectivamente estaba ocurriendo y contrastarlo con lo que sucedió en realidad al momento en que el investigador observó el caso de estudio (Mulhall, 2003).

El investigador que realizó la observación hace parte de uno de los 3 equipos que están involucrados en el problema, por lo que, se puede afirmar que el comportamiento de las 3 áreas no se vio afectado en el momento que se aplicó este instrumento de investigación. En la sección de sesgo se hablará sobre posibles limitaciones que el investigador pudo llegar a experimentar al momento de hacer uso del instrumento.

Tomando como punto de partida el hecho empresarial descrito en capítulos previos, se observó el flujo del proceso de la excepción de acceso en la Organización XYZ, el investigador tuvo en cuenta el inicio, ejecución y finalización del proceso. Las 3 fases involucran una gran cantidad de interesados, por lo cual se observaron las acciones que los miembros desarrollaron al interactuar con el proceso en mención.

La observación se documentó mediante unas notas tipo log, que el investigador elaboró con el fin de poder captar de una mejor forma la información que se recolectó mediante el instrumento de observación. Dicho log se usó en las diferentes reuniones o interacciones donde se reunieron los grupos de interesados al momento de discutir una excepción de acceso, el investigador se limitó a documentar lo que observó y escuchó en el momento de que se estaban llevando a cabo discusiones sobre excepciones particulares. Una vez se finalizó la recolección de la información con la ayuda del log, el investigador analiza las notas de observación, con el fin de poder determinar patrones sobre el proceso de excepción de acceso de las reuniones a las cuales asistió, las mismas se expondrán en el siguiente capítulo de este documento.

De esta forma se pudo evidenciar que tan rápido fue el proceso, si se entorpece de alguna manera, la conducta y comportamiento del grupo de interesados. Las notas fueron codificadas con el fin de permitir al investigador tomar más rápido la nota, ya que fueron discusiones que en lo general tomaron de 30 a 60 minutos. Dicha codificación fue aplicada en no mencionar los clientes corporativos, se codificó mediante el acrónimo clienteCorp, de igual forma el rol de cada persona que interviene en las discusiones fue codificado, por ejemplo, el gerente de operaciones en las notas quedó identificado como Gops, el gerente de tecnología como Gti, gerente de seguridad de la información como Ginofsec. En el anexo 5.4 se da una pequeña muestra de Log usado para documentar

los sucesos que ocurrieron en diferentes reuniones donde el investigador asistió y tomó las respectivas anotaciones de las discusiones.

3.2.2 Análisis de documentos

Este instrumento es considerado como uno de los más potentes dentro de esta investigación, ya que el proceso de excepción de acceso es documentado mediante editores de texto donde se evidencia la interacción de los departamentos de operaciones y seguridad de la información. El departamento de seguridad de la información de la Organización XYZ, con el fin de documentar la excepción de acceso genera archivos de texto que son almacenados por el gerente de seguridad de la información que está a cargo de otorgar o denegar la excepción. El archivo de texto es manejado por varios interesados y se comparte a través del correo corporativo de la Organización XYZ, es por esto que, se tienen varias versiones de los documentos al momento de analizar una excepción de acceso, para la elaboración de esta investigación, se analizó exclusivamente las versiones marcadas como finales para las diferentes muestras de excepción de acceso que fueron parte del estudio, el acercamiento que se tuvo hacia la documentación fue enfocado a la fuente (Bell, 2005). La documentación analizada entregó al investigador un historial y contexto del caso de la excepción de acceso que estuvo bajo estudio, este instrumento sirvió de insumo para la herramienta de entrevistas, ya que se pudieron incluir preguntas adicionales para que fueran respondidas por el grupo de interesados, así mismo, los documentos contribuyeron a una forma más efectiva de recolección de datos, porque al momento de observar y entrevistar se pudo estar olvidando algún detalle (Bowen et al., 2009).

El instrumento de análisis documental está compuesto por cuatro fases, las cuales fueron: explicación del requerimiento, justificación del negocio; estas dos fases iniciales fueron completadas por el departamento de operaciones, las dos últimas fases: evaluación del riesgo y definición de controles estuvieron desarrolladas por el departamento de seguridad de la información. Dichas fases fueron alineadas al flujo del proceso de la excepción de acceso. El investigador por cada fase realizó un análisis

sobre lo plasmado en la documentación, por lo demás, el investigador emitió un concepto donde se indicó si es asertiva la información entregada por el interesado en la fase a analizar. El instrumento recolectó información adicional, como numeración del documento, nombre de la excepción de acceso, categoría de la excepción²⁶, cliente solicitante²⁷, número de ticket, geografía y el nombre del gerente de la seguridad de la información, debido a restricciones de confidencialidad el nombre de los clientes en ningún momento será compartido en el documento.

La documentación examinada provee excelente información donde el investigador puede corroborar la minucia y asertividad por parte del grupo de interesados al momento de desarrollar el proceso de excepción de acceso. Algunas ventajas del documento expuesto en el anexo 5.4 son que el documento conserva un buen cubrimiento, exactitud, estabilidad y no se tienen restricciones de desconfianza y reactividad hacia el investigador (Bowen et al., 2009).

3.2.3 Entrevistas

Este instrumento complementa a los dos expuestos previamente, mediante el uso de entrevistas se extrajo información de fondo a un grupo selecto de interesados, los cuales contribuyeron con sus experiencias y puntos de vistas sobre el tema de estudio (Turner, 2010). Este instrumento puede ser orientado de la siguiente manera: entrevista informal conversacional, entrevista general con acercamiento enfocado y entrevistas general abierta (Borg, Gall & Gall, 2003). Para el desarrollo de esta investigación se hizo uso de la orientación de acercamiento enfocado y entrevista general abierta.

Las entrevistas de acercamiento enfocado requiere que el entrevistador y entrevistado tengan confianza para poder aplicar, esta orientación de entrevista requiere una habilidad del entrevistador en asegurarse que las áreas generales de la información

²⁶ Categoría de la excepción: Con el fin de simplificar el análisis documental, se codificarán parte de la información que es repetitiva (Russel Bernard, 2004), esto ayudará al investigador a poder documentar de una forma más efectiva y la codificación será aplicada para el tipo de excepción de acceso

²⁷ Cliente solicitante, debido a las restricciones de seguridad, no se mencionan los nombres de los clientes que hacen parte del estudio.

son recolectadas de cada entrevistado, adquiriendo un mayor foco, debido a qué, se pueden adaptar en obtener la información del entrevistado (Turner, 2010). Es por esto qué, se requiere el uso de técnicas de construcción de confianza, como lo es la auto divulgación y escucha activa (Vallano & Compo, 2011), en el momento que se aplicó la entrevista. La auto divulgación en un solo sentido ayudó a que las preguntas iniciales que realizó el entrevistador se enfocaron específicamente al entrevistado con el fin de construir la confianza que necesita. Referente a la escucha activa, esto hizo saber al entrevistado que existe una conexión armoniosa referente al tema que se estaba discutiendo (Vallano & Compo, 2011).

En la entrevista general abierta se pretendió que el entrevistado contribuye a aportar de una manera más detallada la información que ellos consideraron importante sobre el caso de estudio (Turner, 2010).

En ambos casos se tuvo como guía un cuestionario semi estructurado, ya que estaba centrado al tópico central (Bell, 2005), el cual es la excepción de acceso. Por lo tanto, este tipo semi estructurado se alineó con las entrevistas de acercamiento enfocado y entrevistas generales abiertas (Bell, 2005; Turner, 2010).

Se efectuaron entrevistas mediante grupos de foco entre los miembros de los departamentos de estudio (operaciones, tecnología y seguridad de la información) con el fin de que los participantes interactuaron entre ellos, para que estuvieran abiertos a escuchar con el fin de lograr un consenso sobre el tema de discusión (Bell, 2005).

En el anexo 5.5 se encuentra el esquema de las entrevistas que se aplicó a las 3 áreas que se involucraron para el cumplimiento de las entrevistas. En el anexo 5.5.1 se encuentra la entrevista aplicada al departamento de operaciones, en el anexo 5.5.2 la entrevista aplicada al departamento de seguridad de la información; y, finalmente el anexo 5.5.3 se encuentra la entrevista utilizada en el departamento de tecnología. Dichas entrevistas fueron desarrolladas de acuerdo a las fases que cada departamento tiene que estar relacionado o interviniendo con el proceso de excepción de acceso. En los 3 cuestionarios se hizo referencia a lecciones aprendidas donde se le dio la oportunidad al entrevistado en conocer su punto de vista para mejorar este proceso.

Las entrevistas fueron grabadas, con el fin de que el investigador pudiera sintetizar de una forma más tangible la información recolectada mediante este instrumento de investigación y a su vez ser objeto de análisis junto con la información recolectada mediante los otros instrumentos de investigación.

3.3 Muestra de estudio

El propósito de usar tres instrumentos de esta investigación para todo el desarrollo, se basó en que dichos instrumentos fueron aplicados a muestras diferentes. A continuación, se menciona cuáles fueron las muestras a las que se expusieron los instrumentos de investigación.

3.3.1 Muestra de estudio para instrumento de observación.

Este instrumento hizo uso de las excepciones de acceso más trascendentales, que han sido manejadas en la ciudad de Bogotá, el cual se realizó de esta forma, ya que, el investigador puede tener acceso a estas reuniones y pudo tomar nota de lo observado y escuchado sin que se altere el comportamiento de los participantes; cabe resaltar, el hecho de que, el análisis se hubiera hecho sobre una operación que reside en Bogotá, no interfirió en que participantes de otros países hicieran parte de las reuniones y/o discusiones, y por la gravedad de la excepciones manejadas, se alcanzó un nivel de escalación directivo en las oficinas principales de la Organización XYZ en Estados Unidos, dichos empleados accedieron de forma telefónica o videoconferencia a las reuniones pactadas. En las discusiones se tuvieron un gran número de participantes desde niveles gerenciales hasta niveles C, dichos niveles reportan al Chief executive officer de la Organización XYZ.

3.3.2 Muestra de estudio para instrumento de análisis de documentos.

Como se mencionó previamente, los documentos analizados fueron las excepciones de acceso generadas por los Gerentes de Seguridad de la Información, con la ayuda de la vicepresidenta de dicho departamento para las Américas, se logró tomar muestras aleatorias de mínimo 4 excepciones de acceso, para gerentes ubicados en países como Colombia, Jamaica y Estados Unidos. Dicha muestra al haber sido aleatoria involucró diferentes tipos de excepciones de acceso, desde niveles simples de controles hasta niveles elevados de controles propuestos por los Gerentes de Seguridad de la Información.

3.3.3 Muestra de estudio para instrumento de entrevistas.

Como muestra de estudio, se consideró a los gerentes y directores que hacen parte de las áreas de operaciones, tecnología y seguridad de la información; aclarando que la cantidad de gerentes y directores de operaciones varía de acuerdo con el número de clientes corporativos que tenga la Organización XYZ, generalmente a cada cliente corporativo, se le asigna un gerente o director de cuenta el cual es el encargado de la operación del servicio contratado por el cliente corporativo

Referente a los gerentes de tecnología y seguridad de la información, es enfático aclarar que el número de integrantes de estos 2 equipos es reducido a comparación de los que conformaron el equipo de operaciones, ya que se consideró segmentos de áreas administrativas para la Organización XYZ, a modo de ejemplo, se cuenta con 1 gerente de seguridad de la información para la región de Latinoamérica; respecto a tecnología la región cuento con 1 director y 2 gerentes, al momento de aplicar la entrevista.

Se tuvo en cuenta a gerentes y directores que estuviesen localizados en los diferentes países pertenecientes a la región de América, donde opera la organización, con el fin de tener diversidad global al momento de efectuar el estudio de investigación y suficiente información para los instrumentos que se aplicaron. Esta muestra ofreció una visión a nivel operacional de las 3 áreas principales involucradas en este caso de estudio.

Además, se intervino a un nivel estratégico donde se involucraron a vicepresidentes, para visualizar a un nivel estratégico la perspectiva que ellos tenían sobre el proceso de excepción de acceso, con el fin de poder tener argumentos en sugerir intervenciones a niveles estratégicos, especialmente a lo que hace referencia al Gobierno de Seguridad de la Información para la Organización XYZ.

3.4 Recolección de información

El investigador recolectó la información con ayuda de los instrumentos enunciados, previamente; para el instrumento de observación, se procedió a inspeccionar las excepciones de acceso que se están manejando por la Organización XYZ para la geografía de Colombia al momento del desarrollo de este documento. Referente al análisis documental, se procedió a solicitar las excepciones de acceso generadas por el departamento de seguridad de la información durante el último año (de la elaboración de este documento), cada excepción estaba asociada a un número de ticket, el cual puede ser consultado en la herramienta de ITSM²⁸; donde se documentó parte de las acciones tomadas en el proceso de excepción de acceso, el análisis de correos y minutas de reuniones, donde se garantizó el acceso al investigador será analizado y se extrajo la información más relevante. Las entrevistas realizadas son la última fuente de obtención de información ya que se tuvo en cuenta las vivencias que tuvieron los entrevistados con el proceso de excepción de acceso.

3.5 Análisis de información

Con la información recolectada mediante los tres instrumentos de investigación, el investigador pudo corroborar la sustentación de varias proposiciones a través del conjunto de información o evidencia recolectada, reduciendo el impacto del sesgo que puede existir con el uso de un solo instrumento (Bowen et al., 2009; Eisner, 1991).

²⁸ ITSM, IT Service Manager, herramienta de gestión de servicios IT.

Dicha información recolectada ayudó al investigador en concurrir en proposiciones que genere credibilidad (Bowen et al., 2009), es decir, que el análisis que se usó en los datos recolectados contribuyó en la generación de proposiciones que ofrece solución al tema de estudio de este documento. Ya que se tuvieron tres fuentes de información que contribuyeron a denotar comunes denominadores para la generación de un análisis que propuso una alternativa de solución al caso de estudio.

3.6 Sesgo

Referente al instrumento de observación, se corrió el riesgo de alterar el comportamiento de las personas que interactuaron en el proceso de excepción de acceso, por lo que, se pudo ver limitada la aplicación de dicho instrumento. En el análisis documental, el sesgo estuvo atado de la cantidad de documentación que el investigador debió analizar, lo cual pudo haber incurrido en una errónea sinterización y análisis por parte del investigador; por ello, la importancia que se tuvo al seleccionar de una manera efectiva los documentos que estaban en concordancia con el hecho empresarial de estudio, así mismo, en el momento que se analizaron los documentos, el investigador lo hizo de manera rigurosa y transparente (Bowen et al., 2009). Referente a las entrevistas, el sesgo se relaciona a la confianza que el entrevistador pudo desarrollar con el entrevistado, si no se generó dicha confianza las respuestas se hubieran visto limitadas y distorsionadas, debido a esto no se le hubiese podido extraerse el mayor provecho de este instrumento

Como es de evidenciar cualquier investigación corre el peligro de incurrir en un sesgo, no obstante, el investigador mediante el uso de los tres instrumentos, expuestos previamente, desea asegurarse en poder reducirlo de la forma más asertiva posible.

3.7 Piloto

En esta investigación se realizó un piloto para el instrumento de entrevista, mediante el mismo se desea afianzar las preguntas que se estructuraron para poder

extraer la información. Dicho piloto pretende sondear qué tan efectivo es el instrumento y validar si se está cubriendo los aspectos a los cuales están orientadas las entrevistas.

3.8 Consideraciones éticas

Desde el inicio de este documento se ha hablado de no difundir el nombre de la Organización XYZ, sus clientes o colaboradores, debido a dichas razones, la ética, caracterizó un papel fundamental en el desarrollo de este documento. Igualmente, en el momento que se aplicaron los instrumentos de investigación se informó a las personas que estaban involucradas, sobre cuál era el objetivo de la aplicación del instrumento, y porque se estaba haciendo; ya que se deseaba alcanzar un nivel personal para el investigador y un nivel organizacional para la compañía XYZ. Así mismo, se solicitó el debido permiso al momento de observar y efectuar las entrevistas para poder grabar dichos resultados y afianzar de una mejor manera los resultados de la aplicación de los instrumentos. Referente a los documentos, se solicitó aprobación para ser usados sin nombres propios de colaboradores o de la Organización XYZ, con fines académicos y poder brindar al lector un mejor contexto.

4. Recolección de información y Análisis de datos

4.1 Recolección de información

Debido a que se usaron 3 instrumentos de investigación, se da a conocer por separado la forma como se recolectó la información para esta investigación, para cada método se aplicó fases de planeación, ejecución y cierre. Por último, se da a conocer al lector los retos que se tuvieron al aplicar los diferentes métodos al momento de recolectar la información.

4.1.1 Proceso de recolección de información para: Observación

En la etapa de planeación, se indujo a que este instrumento capturara la mayor cantidad de información de diferentes reuniones que a consideración del investigador, eran reuniones trascendentales debido a las discusiones que se llevaban entre los diferentes grupos de interesados. Como muestra de observación se tomaron 2 excepciones de acceso que estaban en alta discusión durante la elaboración de este documento. Por cada excepción de acceso se tuvieron como mínimo 20 reuniones, donde todos los grupos de interesados (tecnología, operaciones y seguridad de la información), accedían con el fin de mantener las diferentes discusiones sobre la excepción de acceso que estaba bajo estudio. Durante la ejecución se tomaron notas mediante dispositivos electrónicos cuando era posible, también se tomaron notas manuales, en ambos casos se aplicó la codificación descrita en el capítulo 3. En el cierre se condensó la información mediante un documento de Excel, donde se estandarizaron las notas siguiendo un formato de Log, organizado dichas notas en orden cronológico, numerando cada captura de información, dentro del instrumento se identifica como “anotación número”, al final se tienen 76 anotaciones para un log donde solo se analizaba 1 sola excepción de acceso. Para la segunda excepción se lograron recolectar 30 anotaciones.

Retos que tuvo este instrumento fue que el investigador era parte de las discusiones, por lo que, en momentos él investigador debía participar en las reuniones, la participación del investigador no era tan alta como lo hacían los miembros de operación y seguridad de la información, dando espacio a que se perdieran algunas notas; sin embargo, el investigador se aseguró de que los sucesos más importantes quedarán documentados, ya que en el momento que el investigador tenía que intervenir, hacía anotación de forma manual de ideas clave sobre la discusión que se estaba llevando a cabo, para luego ser sintetiza la información dentro del log. Si bien pudo darse campo a un sesgo, el investigador se aseguró de hacer revisiones adicionales en los documentos resultados de las reuniones y/o consultando con alguno de los miembros que hicieron parte de la discusión con el fin de complementar lo observado, esto con el fin de mitigar las posibles omisiones mientras el investigador intervenía en las discusiones.

4.1.2 Proceso de recolección de información para: Análisis de documentos.

Se planeó inicialmente analizar excepciones de acceso de 6 países diferentes Brasil, Canadá, Colombia, Estados Unidos, Jamaica y México. La muestra recolectada se tomó de 5 gerentes de seguridad de la información los cuales compartieron 4 excepciones de acceso aleatorias, las cuales son procesadas mediante un documento de Word, al momento de que se realizó esta investigación. Durante la aplicación de entrevistas, se evidenció que varias personas hacían referencia al contrato firmado entre la Organización XYZ y los diferentes clientes corporativos, ya que el investigador en la etapa final de recolección de información decidió recolectar algunos de los contratos para las operaciones de Colombia de forma aleatoria, con el objetivo de analizar dichos documentos.

Para las excepciones de acceso se hizo uso del instrumento expuesto en el anexo 5.5, el cual permitió condensar la información en un solo documento de Excel. En dicho instrumento el investigador analiza cualitativamente cada fase que compone el documento y valida si la información analizada era asertiva o no, en base al requerimiento hecho. El requerimiento se documenta por medio de un ticket a través de una

herramienta ITSM, el investigador también validó esta información el cual se accede a través de la intranet de la Organización XYZ. El requerimiento hecho en el ticket se comparaba con la justificación del negocio que se plasma dentro del formato de excepción de acceso, en las 2 últimas fases se analizaba la evaluación del riesgo y los controles sugeridos por los gerentes de seguridad de la información. El instrumento permitió al investigador poder identificar la evaluación de riesgo y controles sugeridos para el mismo tipo de requerimientos, pero los cuales se solicitaron en geografías diferentes.

Para los contratos se tomaron contratos aleatorios de los clientes corporativos que operan en Colombia, la recolección de datos se centró en poder identificar los segmentos del contrato donde se mencionan cláusulas relacionadas a seguridad de la información.

Algunas dificultades fueron presentadas al momento de solicitar las excepciones de acceso a los gerentes de seguridad de la información, por lo que, inicialmente no cooperan en facilitar la información, debido a esto se habló con la vicepresidente de seguridad de la información para las Américas (principal patrocinadora de esta investigación) la cual muy amablemente hizo seguimiento con los gerentes, algunos de los gerentes sintieron que se trataba de una auditoría, hecha por parte de los directivos del área de seguridad de la información, esto causó una demora para recoger la muestra de estudio. Referente a los contratos se tuvo que seguir un gran proceso de aprobación ya que no son de fácil acceso, sin embargo, el investigador como ha mencionado previamente al momento de elaborar este documento ejercía como gerente de tecnología dentro de la Organización XYZ, lo cual contribuyó a que se agilizará el proceso de obtención de dichos documentos.

4.1.3 Proceso de recolección de información para: Entrevistas

Como se definió en el capítulo 3, se desarrollaron 3 tipos de entrevistas para las diferentes áreas involucradas en el proceso de excepción de acceso. Las entrevistas fueron aplicadas a 5 gerentes y 1 directores del departamento de operaciones, 1 gerente y 1 director del departamento de tecnología; finalmente, para el departamento de

seguridad de la información, la entrevista se aplicó a 2 gerentes y 1 vicepresidente. Las personas que contribuyeron a esta recolección de datos se ubican en países como Brasil, Colombia, Estados Unidos y México. Una vez finalizaron las entrevistas, el investigador examinó los audios para proceder con el respectivo análisis. Por último, por cada entrevista se extrajeron los aportes más relevantes que contribuyeron a la realización de esta investigación, dichos aportes se almacenaron a través de un procesador de texto, donde se etiquetó el nombre de la persona, departamento y rol perteneciente, con el fin de poder acceder de forma fácil.

Como reto de este método de investigación, fue el poder contar con el tiempo de las personas que hacían parte del listado inicial para aplicar la entrevista, en varias ocasiones algunos miembros del equipo entrevistado habían confirmado, pero al momento de efectuar la entrevista, cancelaron debido al día a día que llevan en la Organización XYZ. Para ello, se lograron aplicar alrededor de 11 entrevistas dentro de la muestra determinada para esta investigación. El objetivo era tomar una muestra de 15 entrevistas.

4.2 Análisis de datos

Para efectos de análisis de la información recolectada con los instrumentos de investigación, se procedió a tomar como guía el método comparativo constante. Típicamente dicho método es empleado en información que ha sido recolectada mediante entrevistas, observación y análisis de documentos (Grove, 2010). El método para analizar la información se dividió en dos etapas. La etapa inicial tiene como objetivo analizar la información recolectada por cada instrumento de investigación. En la etapa final se procederá a generar proposiciones en base a la información extraída del análisis inicial, dichas proposiciones sugerirán soluciones para el caso de estudio.

Se extrajeron notas por separado de los instrumentos de investigación analizados, con el fin de poder documentar de una mejor manera la información y poder generar categorías, dichas notas se extrajeron de forma crítica a la información recolectada.

4.2.1 Análisis de información: Observación.

En los logs recolectados de las diferentes reuniones a las que asistió el investigador, se extrajeron 5 categorías al momento de analizar de forma comparativa constante dichos logs, a continuación, se describen las categorías que se lograron extraer una vez finalizado el análisis:

1. **Reprocesamiento:** Es evidente que existe un alto reprocesamiento por parte del área de seguridad de información al momento que se interpretan los requerimientos. Por ejemplo, en varias de las interacciones, se logró evidenciar que el departamento de seguridad de la información, solicitaba al departamento de operaciones aclarar la razón del porqué se debía exceptuar el requerimiento, lo cual en repetidas ocasiones llevaba al departamento de operaciones, en explicar desde un contexto en general cómo funcionaba el negocio para un cliente corporativo en específico, hasta llegar al porqué se hacía el requerimiento y cómo podría beneficiar al departamento de operaciones desde una perspectiva del negocio. De otra parte, para que el departamento de seguridad de la información entendiera el por qué se debía exceptuar, se efectuaron varias sesiones hasta que finalmente se aclaraba el requerimiento. Aparentemente daba la sensación de que el departamento de seguridad de la información no entendía bien el negocio del cliente corporativo y por consiguiente no encontraban sentido al requerimiento al cual se debía exceptuar.
2. **Claridad del requerimiento:** La información compartida por el departamento de operaciones no fue entregada de forma clara desde el inicio, por lo que, varias reuniones debieron ser agendadas con el fin de alinear las dos áreas al momento de interpretar el requerimiento. Al momento que se agendaban las reuniones iniciales para discutir el requerimiento, los departamentos debían compartir una serie de documentación y poder llegar preparados a la reunión (obtener un buen contexto de la situación). Ahora bien, dicha documentación no era lo suficientemente clara al momento que se agendaban las reuniones, ya que en varias de las reuniones se hacía uso del tiempo para que el

departamento de operaciones pudiera aclarar el requerimiento que estaban llevando al departamento de seguridad de la información.

3. **Alineamiento global:** El departamento de seguridad de la información no tenía claridad sobre los requerimientos hechos en regiones alternas (APAC, EMEA, etc.) hubieran sido implementados ya en otro país de dichas regiones, debido a esto se inicia una indagación con los gerentes de seguridad de la información que operan en dichos países. Por ejemplo, en varias ocasiones, el departamento de operaciones le indicaba al departamento de seguridad de la información que validara con sus pares de seguridad de la información localizados en la región de APAC para qué corroboraran que algunas de las excepciones en discusión habían sido aprobadas en dicha región. Dicha aclaración se efectuaba mediante el agendamiento de otra reunión donde se excluía al departamento de operaciones y a la cual asistían los miembros del equipo de tecnología y seguridad de la información, en esas reuniones intervienen principalmente los miembros de seguridad de la información de Américas y APAC con el fin de poder aclarar los controles definidos a la excepción de acceso concedida en dicha región.
4. **Definición de niveles de servicio:** El proceso de excepción de acceso toma demasiado tiempo, ya que los niveles de servicio por parte del área de seguridad de la información hacían el departamento de operaciones no están claramente establecidos.
5. **Atención al cliente:** Existe una constante presión por parte del área de operaciones hacía seguridad de la información mencionando que el cliente está a la continua espera del requerimiento (esto se evidencia desde que inicia el proceso). Por ejemplo, por las diferentes discusiones que se llevaron para excepciones de acceso particulares, y debido al tiempo que llevaban bajo discusión el departamento de operaciones manifestaba que el cliente estaba muy pendiente de la resolución. Como caso particular se puede dar como ejemplo la excepción que hacía referencia a la inclusión de un laboratorio de tecnología para un cliente corporativo (permitir a los empleados de la Organización XYZ tener contacto directo con el producto del cliente corporativo

para el cual prestaban soporte dichos empleados). La excepción tardó alrededor de 5 meses en ser discutida, estudiada y aprobada por el departamento de seguridad de la información, trajo una gran molestia por parte del cliente corporativo y del departamento de operaciones hacia el departamento de seguridad de la información. No se mantenía informado al departamento de operaciones ni al cliente corporativo del porqué la demora en poder aprobar la excepción de acceso.

4.2.2 Análisis de información: Análisis de documentos.

De la información recolectada mediante el instrumento de análisis de documentos y aplicando análisis comparativo de dicha información se puede inferir:

1. **Precisión:** Los requerimientos y justificaciones entregadas por el departamento de operaciones mediante el formato de excepción de acceso no eran lo suficientemente precisos, para que el departamento de seguridad de la información pudiera tener un buen contexto del requerimiento, por lo cual, el gerente de seguridad de la información divagaba al momento de interpretar la documentación.
2. **Homogeneidad:** Las evaluaciones de riesgo para requerimientos de las mismas características no son homogéneas al momento de efectuar la evaluación de riesgo, por parte de los diferentes gerentes de seguridad de la información que operan en las distintas regiones de la Organización XYZ. Ejemplo de la falta de homogeneidad se evidenció al momento de analizar un mismo tipo de requerimiento el cual es gestionado por gerentes de la seguridad de la información localizados en 3 países diferentes (Colombia, Jamaica y Estados Unidos), el requerimiento era permitir comunicación a través de la herramienta de mensajería instantánea corporativa entre la Organización XYZ y el cliente corporativo. Los controles sugeridos entre los 3 gerentes de seguridad de la información fueron diferentes. Se otorgó el permiso en los 3 casos, pero los controles son diferentes. En otros tipos de requerimientos se evidenció el mismo patrón de falta de homogeneidad.

3. **No apego al proceso:** En repetidas ocasiones los gerentes de seguridad no hacen uso de la escala de medición de riesgo para ofrecerle al lector una mejor interpretación de la evaluación realizada. Por otro lado, procesaron excepciones de acceso sin que estuvieran debidamente documentadas en la sección donde el departamento de operaciones debe incluir la justificación del negocio. Algunas de las excepciones de acceso analizadas que se consideraron como versiones finales y fueron facilitadas al investigador, no contaban con la información necesaria; no obstante, los gerentes de la seguridad de la información procedieron a hacer las evaluaciones de riesgo sin tener dicha información documentada en el documento de excepción de acceso o el tiquete que se abrió dentro de la herramienta ITSM.
4. **Dueño del control:** Para los controles sugeridos no se asignaron áreas responsables para implementar los controles sugeridos, se detalla el control, pero no se asigna un responsable en desarrollarlo. Como dueño se entiende a la persona o departamento encargado de implementar dicho control para tener un responsable o dueño del control descrito por seguridad de la información.
5. **Inclusión en contratos:** De los contratos analizados, se tienen 2 perspectivas para clientes corporativos no PCI y para clientes corporativos que requieren ser PCI. Para los que no deben ser certificados como PCI, se tocan temas generales de tecnología como el tipo de hardware, software requerido para la operación del cliente corporativo; adicionalmente, se hace mención de los niveles de servicio tecnológico (SLA) en la resolución de incidentes y/o requerimientos, se habla a un nivel muy elevado haciendo referencia a infraestructura, todo esto basado de los servicios que presta la Organización XYZ hacia el cliente corporativo, en resumen no se detallaron en los contratos algún contenido referente a seguridad de la información. Para los clientes corporativos que requieren ser PCI, si se habla sobre seguridad de la información, ya que el cliente exige una cantidad mínima de auditorías por un ente externo para que se otorgue dicha certificación a su operación con la Organización XYZ. Sin embargo, de los contratos analizados solo 2 tenían definido el alcance de ser PCI. Igualmente, dichos contratos incluían contenidos similares en términos

tecnológicos a los cuales hacen uso los clientes corporativos que no son PCI referentes a hardware, niveles de servicio, etc.

4.2.3 Análisis de información: Entrevistas.

Para este análisis de entrevistas, se contó con la información recolectada a los 3 departamentos que intervienen principalmente en este proceso, el mismo se subdivide en el análisis hecho a la información generada para los departamentos de operaciones, tecnología y seguridad de la información.

4.2.3.1. Análisis de entrevistas Operaciones.

A continuación, se condensa la información recolectada a través de las entrevistas, se enumeran las categorías más relevantes donde hubo más coincidencias por parte de los diferentes entrevistados.

- 1. Reprocesamiento:** Varios de los entrevistados, indicaron la existencia de reprocesamiento por parte del departamento de seguridad de la información, al momento de ejecutar el proceso, que conlleva a una gran demora en completar este proceso. Manifestando que, si se quiere añadir un elemento más a la excepción ya concedida, el proceso se debe ejecutar desde cero. Por ejemplo uno de los clientes corporativos al momento de hacer esta investigación contaba con un laboratorio para que los agentes de la Organización XYZ tuvieran mejor interacción de la aplicación que estaban manejando para el cliente corporativo, dicha interacción o experiencia de usuario la lograban obtener a través de la instalación de la aplicación en diferentes elementos como lo son teléfonos móviles, tabletas, portátiles, (existía a ese momento un listado de dispositivos aprobados) cualquier clase de dispositivo que soporte la aplicación. Para poder agregar un dispositivo nuevo al laboratorio, seguridad de la información le solicitaba al departamento de operaciones correr el proceso de excepción de acceso desde el inicio, en vez de agregar el nuevo dispositivo al listado de

dispositivos ya aprobados, generando un reproceso innecesario y desgaste para el departamento de operaciones.

- 2. Entender el negocio:** Los entrevistados coinciden en afirmar que el departamento de seguridad de la información no conocía a fondo la operación y/o el negocio, lo cual conlleva a que los miembros del departamento de seguridad de la información indagaran bastante para poder entender los requerimientos hechos por el departamento de operaciones. Esto como conclusión a las diferentes indagaciones que el departamento de seguridad de la información hacía sobre el tipo de requerimientos, varios entrevistados informaron que tuvieron que explicar al gerente de seguridad de la información y la vicepresidenta a nivel regional de cómo funcionaba el negocio para el cliente corporativo y el porqué del tipo de requerimiento hecho para poder exceptuar, con el fin de que pudieran entender de qué manera podría mejorar la operación para el cliente corporativo y cómo podría contribuir al desarrollo del negocio.
- 3. Alineamiento global:** El departamento de operaciones, aseguraba que no existía un alineamiento global dentro de los diferentes grupos de seguridad de la información que operaban en la Organización XYZ, si se solicitaba la excepción de acceso en otra geografía que no fuera Américas, era más sencillo obtener la aprobación, ya que se demostraba que el requerimiento había sido aprobado. Esto con base a la experiencia que el departamento de operaciones ha tenido al intentar aprobar una excepción de acceso, en una de las entrevistas como caso particular el gerente de operaciones solicitó a su par ubicado en la región APAC, que le compartiera la aprobación previamente otorgada para dicha región, referente el mismo tipo de requerimiento que surgía en la operación de Colombia, una vez obtenida la aprobación por parte de seguridad de la información para esa región (APAC), el gerente de operaciones de Colombia procedió a solicitar la misma excepción para el mismo cliente corporativo, pero con operación en Colombia, como argumento sustentado ante el departamento de seguridad de la información, se informó que el mismo tipo de requerimiento había sido aprobado en la región de APAC.

- 4. Base de conocimiento:** Los entrevistados coinciden que el departamento de seguridad de la información no tenía una base de conocimiento donde se pudiera consultar las excepciones que fueron manejadas ni las que se estaban manejando. En repetidas ocasiones los entrevistados informaron que la documentación que manejaba el departamento de seguridad de la información no era manejada ni almacenada de forma apropiada, han evidenciado que el gerente de seguridad de la información en algunas ocasiones les solicita a los gerentes de operaciones que les comparta el archivo más reciente sobre las excepciones de acceso. De igual forma en varias ocasiones, el departamento de operaciones es el departamento que entregaba la excepción de acceso que fueron manejadas en otras geografías con el fin de que el equipo de seguridad de la información en Américas pueda tener acceso a la excepción de acceso aprobada en dichas regiones, buscando acelerar un poco el proceso.
- 5. Captura de requerimiento:** El formato usado por el departamento de seguridad de la información no era el más intuitivo, se daba espacio a que mucha información no quedará documentada, el formato se puede mejorar con el fin de que ayude a seguridad de la información poder entender de mejor forma los requerimientos.
- 6. Homogeneidad:** el departamento de operaciones evidenció que no existía un patrón homogéneo al momento de efectuar evaluaciones de riesgo, lo observaron debido a evaluaciones hechas en otras geografías. La comparación la hicieron 2 gerentes de operaciones en Colombia, donde se evidenció que los controles sugeridos son diferentes en las geografías.
- 7. Niveles de servicio:** El departamento de operaciones tenía la percepción de que el departamento de seguridad de la información no tiene un buen nivel de servicio, debido a los tiempos que se toman para poder procesar los requerimientos que tienen que pasar a través de una excepción de acceso. Para poder obtener mejores tiempos de respuesta acudían a escalaciones a altos niveles con el fin de obtener una respuesta más ágil.
- 8. Estructura de aprobación:** La estructura de aprobación no es la más adecuada, ya que en varias ocasiones se involucran vicepresidentes que no

tienen entendimiento del requerimiento, que pueden aprobar sin saber qué es lo que están haciendo, dichas aprobaciones deberían ser a un nivel más local. Ejemplo de esto son los directores de operaciones, que manifestaron, que son ellos quien entienden más la operación; y por ende, están trabajando de la mano con los gerentes de las operaciones para poder aprobar las excepciones, los directores manifiestan que en ocasiones son tantos los vicepresidentes que involucran que no toman en cuenta el riesgo que están aprobando y lo hacen con el fin de que se agilice el proceso, sin embargo, son los directores de operaciones quienes deberían ser el nivel más alto dentro del departamento de operaciones al momento de aprobar una excepción de acceso.

9. **Inclusión en contratos:** Varios de los gerentes entrevistados afirman que seguridad de la información no se le da la importancia dentro de los contratos, al no estar contemplado dentro del contrato y al momento que el cliente indaga de porque se ponen tantas trabas, el cliente se dirige al contrato y no observa como tal una anotación hacía seguridad de la información, que genera un descontento del cliente hacia la Organización XYZ.
10. **Gobernabilidad:** De los entrevistados, la gran mayoría coincidió en que evidencian una falta de gobernabilidad a nivel interno del departamento de seguridad de la información, por los elementos en general mencionados previamente.

4.2.3.2. Análisis entrevistas tecnología.

A continuación, se condensó la información recolectada a través de las entrevistas, se enumeran las categorías más relevantes donde hubo más coincidencias por parte de los diferentes entrevistados.

1. **Tecnología interfaz de comunicación:** En varias ocasiones la tecnología tomaba el rol de interfaz de comunicación entre el departamento de operaciones y seguridad de la información, con el fin de que ambos departamentos tuvieran una comunicación más asertiva. Con base a que el equipo de tecnología está más involucrado en la operación, son ellos quien entienden más el

requerimiento hecho por el departamento de operaciones hacia el departamento de seguridad de la información, lo cual contribuye a una mejor interpretación del requerimiento, de los miembros entrevistados del departamento de tecnología, todos llegaron a la misma conclusión en esta categoría.

2. **Alineamiento global:** El grupo de entrevistados concluyó que le hacía falta mejorar el alineamiento global al departamento de seguridad de la información. El equipo de tecnología al funcionar como interfaz de comunicación son los que contribuyen a que se mejore dicha alineación, siendo que el equipo de tecnología válida con los equipos pares ubicados en otras geografías al momento de recibir los requerimientos que controles se deben implementar de excepciones de acceso. Contribuyendo a complementar el trabajo hecho por seguridad de la información.
3. **Claridad del requerimiento:** El equipo de tecnología evidencia que el requerimiento no es claro por parte del equipo de operaciones hacia seguridad de la información, y conlleva a que el proceso se desarrolle de forma más lenta. El equipo de tecnología al momento que se genera el requerimiento por el equipo de operaciones hacia el departamento de seguridad de la información tiene un rol de observador, los entrevistados concluyen que la claridad no es la más certera con base a este rol de observador, siendo que en repetidas ocasiones el departamento de tecnología es el encargado de clarificar los requerimientos entre seguridad de la información y el departamento de operaciones. Generando una lentitud en la ejecución del proceso.
4. **Base de conocimiento:** La falta de la base de conocimiento hace que se genere un reproceso por parte de seguridad de la información, ya que deben ejecutar evaluaciones de riesgo, las cuales no son homogéneas y conlleva a que se quejen las áreas de operaciones al validar una evaluación más restrictiva de una región a otra. Esto lo evidencia el departamento de tecnología, porque evidencian la diferencia entre la evaluación de riesgo de una región diferente y la comparan junto con la que se hizo localmente, los mismos, hablan sobre el mismo requerimiento.

5. **Flexibilidad en la evaluación:** En repetidas ocasiones los controles son muy restrictivos asumiendo que todos los clientes deberían certificarse PCI, afirma el equipo de tecnología en las entrevistas realizadas. Varios de los entrevistados indican que los controles aplicados encajan fácilmente en clientes que requieren ser PCI, a pesar de esto, el departamento de seguridad de la información parece que deseara que todos los programas fueran PCI, ya que no es flexible de acuerdo con el modelo de negocio y operación de clientes corporativos que no requieren ser PCI.
6. **Niveles de servicio:** El equipo de tecnología concuerda en evidenciar que no se aplican niveles de servicio para este proceso, y conlleva a generar quejas por parte del equipo de operaciones hacia el equipo de seguridad de la información. En el caso del departamento de tecnología si se aplican los niveles de servicio, los cuales están predefinidos en la intranet de la Organización XYZ para cualquier tipo de servicio tecnológico que requieran los empleados, referente a seguridad de la información dichos tiempos deberían ser aclarados con el departamento de operaciones, porque pareciera que este nivel de servicio no fuera tenido en cuenta por parte del departamento de seguridad de la información y generación de malestares.
7. **Entender el negocio:** Con base a la experiencia y hechos observados por el equipo de tecnología, varios de los entrevistados concuerdan en afirmar que el departamento de seguridad de la información está muy alejado de entender el negocio, esto hace que las reuniones se tornan repetitivas, con el fin de poder entender el requerimiento y la operación desde donde se está haciendo el requerimiento. Esto como conclusión de las preguntas que hacen los miembros de seguridad de la información hacia el departamento de operaciones en las diferentes interacciones en la que se involucran los dos departamentos, asimismo, mencionan que la presencia en las operaciones debiera ser mayor por parte del departamento de seguridad de la información.
8. **Captura requerimiento:** El formato de la excepción de acceso debería ser más preciso con el fin de poder extraer mejor información del requerimiento hecho por el departamento de operaciones de seguridad de la información. Esto lo

afirman la totalidad de entrevistados donde informan que el formato usado para capturar la información es muy simple y se deja abierto a que no aporte la información requerida por parte del departamento de seguridad de la información.

9. **Estructura de aprobación:** La estructura que se usa hoy en día no es la más apropiada, ya que la mayoría de los requerimientos solicitan que apruebe un vicepresidente, que quizás no tiene entendimiento del requerimiento, la estructura de aprobación debería ser aplicada a un nivel más local.
10. **Homogeneidad:** En las excepciones de acceso implementadas por el equipo de tecnología, se observan que las evaluaciones no son homogéneas debido a que los controles sugeridos de requerimientos similares varían. Esto lo observan al comparar excepciones de acceso que tratan del mismo requerimiento, pero sugieren controles diferentes debido a que las evaluaciones de riesgo son llevadas a cabo por personas diferentes.
11. **Auditoría al control:** En las excepciones de acceso solo se mencionan los controles que se deberían aplicar, no se audita si los controles fueron aplicados. De acuerdo al equipo de tecnología, no existe un equipo que esté a cargo de validar si los controles se aplicaron o si siguen siendo útiles para la excepción aprobada, el equipo de seguridad de la información solo cumple con mencionar el control, pero no se tiene claridad sobre quien recae la responsabilidad de validar dichos controles una vez sean implementados.
12. **Gobernabilidad:** Con base a los elementos previamente expuestos, el equipo de tecnología considera que hace falta gobernabilidad dentro del equipo de seguridad de la información.

4.2.3.3. Análisis entrevistas seguridad de la información.

1. **Base de conocimiento:** El equipo de seguridad de la información es consciente de la necesidad de tener una base de conocimiento que actúe como repositorio para poder almacenar las excepciones de acceso que han sido manejadas por el equipo de seguridad de la información. Debido a la falta de dicho repositorio, el equipo de seguridad de la información aseguran que son

conscientes en el entorpecimiento del proceso, al momento de hacer las evaluaciones de riesgo, debido a que tienen que iniciar indagaciones con el equipo global con el fin de poder asemejar la evaluación de riesgo, esto en el mejor de los casos, por otra parte, existen otros casos donde la evaluación es diferente al que se ha realizado en otra geografía debido a la falta de mantener la debida documentación.

2. **Captura del requerimiento:** El formato de Word que se usa no es el más adecuado, porque permite dejar mucha información sin capturar. En repetidas ocasiones el equipo de seguridad de la información intercambia un alto número de correos con el departamento de operaciones y/o agendamiento de reuniones con el fin de poder aclarar el requerimiento hecho para poder hacer la excepción de acceso, haciendo consumir bastante tiempo del proceso y a la vez permite dejar escapar información importante sobre el requerimiento hecho a seguridad de la información.
3. **Estructura de aprobación:** Varios de los entrevistados afirman que la estructura de aprobación para una excepción de acceso no es la mejor, las aprobaciones se deberían solicitar a un nivel más local. El equipo de seguridad de la información manifiesta que en repetidas ocasiones han evidenciado que los actuales aprobadores no se toman el tiempo para poder entender el requerimiento, estudiarlo y aprobarlo, debido al día que llevan dentro de la Organización XYZ, aprueban el requerimiento como parte de un papeleo necesario para poder tener su operación funcionando
4. **Concientización:** Varios de los miembros del equipo de seguridad de la información reiteran que si los empleados tuvieran una mejor conciencia y/o noción de seguridad los requerimientos disminuirían de gran manera.
5. **Gobernabilidad:** Para niveles de gerente hacia abajo, es importante notar que los miembros del equipo que encajan en esos roles consideran una falta de gobernabilidad, por ejemplo, para tener una base de datos, evaluaciones de riesgo más homogéneas. De todas formas, a niveles de director y superiores, consideran que a nivel de gobernabilidad el departamento funciona bien.

4.3 Generación de proposiciones

Como se comentó en la sección 4.2, el análisis de datos en este trabajo de investigación se guía bajo el método comparativo constante el cual ayudó en la generación de proposiciones, a continuación, se explica el mencionado proceso.

Para asociar la información, se debió seguir un procedimiento de integración, seguido por un proceso de agrupación de dicha información, esto permitió generar un conjunto de variables, con las cuales abrió paso a generar proposiciones para el caso de empresarial analizado en este documento, a continuación, se guiará al lector por este procedimiento con el fin de obtener su total entendimiento.

4.3.1 Integración de las categorías.

Como se observó en la sección 4.2, generaron una serie de categorías asociadas al análisis de los instrumentos de investigación. Como procedimiento inicial, se enlistan las 35 categorías obtenidas, cada categoría se asoció con la fuente del instrumento de investigación donde se extrajo. En la tabla 11 se ejemplifica una sección de dicha consolidación, el ejemplo solo hace referencia para los instrumentos de análisis de documentos y observación.

Tabla 11. Integración categorías y análisis de instrumentos de investigación

Fuente	Categoría
Análisis de información: Análisis de documentos	No apego al proceso
Análisis de información: Análisis de documentos	Dueño del control
Análisis de información: Análisis de documentos	Homogeneidad
Análisis de información: Análisis de documentos	Precisión
Análisis de información: Observación	Reprocesamiento

Fuente	Categoría
Análisis de información: Observación	Alineamiento global
Análisis de información: Observación	Claridad del requerimiento
Análisis de información: Observación	Definición de niveles de servicio
Análisis de información: Observación	Atención al cliente

Fuente: Elaboración propia.

4.3.2 Agrupación de las categorías.

Para poder efectuar el proceso de agrupación, se procedió a generar conjuntos numéricos para las categorías que se relacionaban sobre el mismo tema de discusión, en base al análisis cualitativo realizado por el investigador. A continuación, se mencionan algunos ejemplos de cómo se agruparon las categorías obtenidas a partir de diferentes fuentes del análisis de los instrumentos de investigación.

Por ejemplo se nombró la categoría “niveles de servicio” 2 veces nombradas en las categorías (obtenidas de entrevistas para los departamentos de operaciones y tecnología), “definición de niveles de servicio” 1 vez nombrada en las categorías (extraída del instrumento de observación) y “atención del cliente” 1 vez nombrada en las categorías (obtenida del instrumento de observación), en base al análisis cualitativo realizado, las 4 categorías mencionadas, hablan del mismo tema de discusión, por lo cual se asoció el número 7 a este conjunto de categorías.

Otro ejemplo es para las categorías llamadas: flexibilidad en la evaluación, auditoría y control, concientización, no apego al proceso y dueño del control, dichas categorías al ser analizadas de forma cualitativa por el investigador, en base a la información recolectada con los instrumentos de investigación, no se encontró que tuvieran relación con otras categorías, por no ser agrupadas, es por esto que, estas 5 categorías quedaron como independientes y no se ve una asociación numérica en el anexo 5.9.

En la tabla 12, se le da al lector un ejemplo de la asociación que se llevó a cabo, para que el lector tenga un mejor contexto de la asociación realizada.

Tabla 12. Agrupación de categorías y análisis de instrumentos de investigación.

Fuente	Categoría	Asociación categorías
Análisis de información: Observación	Alineamiento global	3
Análisis entrevistas Operaciones	Alineamiento global	3
Análisis entrevistas tecnología	Desconexiones	3
Análisis entrevistas Operaciones	Captura de requerimiento	5
Análisis entrevistas seguridad de la información	Captura del requerimiento	5
Análisis entrevistas tecnología	Tecnología interfaz de comunicación	5
Análisis entrevistas tecnología	Captura requerimiento	5
Análisis de información: Observación	Definición de niveles de servicio	7
Análisis entrevistas Operaciones	Niveles de servicio	7
Análisis entrevistas tecnología	Niveles de servicio	7
Análisis de información: Observación	Atención al cliente	7

Fuente: Elaboración propia.

4.3.3 Generación de variables.

En base al proceso mencionado en la sección 4.3.2, dicha agrupación, permitió al investigador poder agrupar las 35 categorías en 15 grupos, esta reducción se debe a la relación guardada entre la descripción de la categoría, en base al análisis cualitativo realizado por el investigador.

El investigador renombra estos 15 grupos de categorías en 15 variables para el tema empresarial de estudio (tomando en cuenta la frecuencia de repetición del nombre de la categoría), con el fin de conservar relación entre las categorías que conforman el grupo, su descripción y la variable. Un ejemplo es la variable niveles de servicio, está

compuesta por las categorías: definición niveles de servicio (obtenida del instrumento de observación) niveles de servicio (obtenida 2 veces de las entrevistas hechas al equipo de operaciones y tecnología), para terminar con la categoría llamada atención al cliente (Obtenida del instrumento análisis de información), como se puede ver el nombre que se conservó para esta variable es niveles de servicio.

Cabe aclarar que algunas variables hacen relación 1:1 con categorías que no se pudieron agrupar, en la sección 4.3.2 debido a que el análisis cualitativo no permitió hacer dicha agrupación, es por esto que, 5 variables guardan relación directa con 5 categorías.

En la tabla 13, se puede ver el listado de variables que se obtuvo y ver la frecuencia de repetición de las categorías estudiadas por cada variable.

Tabla 13. Conjunto final de variables.

Variable número	Nombre Variable	Frecuencia Repetición
1	Flexibilidad en la evaluación	1
2	Auditoría	1
3	Concientización	1
4	No apego al proceso	1
5	Dueño del control	1
6	Reprocesamiento	2
7	Entender el negocio	2
8	Alineamiento global	3
9	Base de conocimiento	3
10	Homogeneidad	3
11	Estructura de aprobación	3
12	Gobernabilidad	3
13	Claridad del requerimiento	3
14	Captura del requerimiento	4
15	Niveles de servicio	4

Fuente: Elaboración propia.

En el anexo 5.9 se puede observar la tabla consolidada, para todas las categorías estudiadas, la tabla se encuentra organizada de tal forma que se pueden ver inicialmente las categorías con menos repeticiones y finaliza con las categorías que más repeticiones tuvieron en el análisis de la información extraída a través de los instrumentos de investigación.

4.3.4 Generación de proposiciones.

Finalmente, definidas las variables mediante un análisis cualitativo se generaron una serie de proposiciones que dan solución al hecho empresarial parte de este estudio:

Los niveles de servicio ofrecidos por el departamento de seguridad de la información, para el proceso de excepción de acceso, está sujeto a la claridad del requerimiento compartido por el departamento de operaciones y la captura del requerimiento hecho por el departamento de seguridad de la información, con el fin de evitar reprocesamientos al momento de la ejecución del proceso.

El alineamiento global por parte del departamento de seguridad de la información está relacionado con la capacidad de entender el negocio, poseer una base de conocimiento y la homogeneidad para la realización de las evaluaciones de riesgo.

La gobernabilidad de seguridad de la información tiene implícito el poder corroborar la estructura de aprobación que se sigue para las excepciones de acceso, por otro lado, se debe reforzar el alineamiento global dentro del departamento de seguridad de la información. El Gobierno debería también poder establecer una concientización a nivel de toda la organización referente a la importancia de la seguridad de la información, finalmente estipular los dueños de los controles y poder auditar dichos controles son una arista adicional que debería cubrir la gobernabilidad de seguridad de la información.

5. Propuesta

5.1 Transformación digital de la excepción de acceso

La Organización XYZ cuenta con una herramienta de ITSM (ServiceNow) que traería una gran contribución a la solución de este problema, actualmente la herramienta es usada para administrar mediante sistema de tiquetes los diferentes requerimientos hechos a diversas áreas de soporte de la organización, entre ellas el departamento de tecnología. Esta herramienta es usada para el control de cambios tecnológicos y se puede ajustar para mejorar el proceso de excepción de acceso.

Se hace referencia a transformación digital, debido a que esta herramienta permite mejorar los flujos de trabajo y poder automatizar algunos de los procesos con el fin de que el proceso sea más ágil y esté alineado con las necesidades de la Organización XYZ y el departamento de seguridad de la información.

Se resalta que esta herramienta actúa como facilitador del proceso de excepción de acceso y no como una herramienta para hacer gobierno, a lo largo de la sección 5 se mencionaran diferentes campos de acción que deben ser tenidos en cuenta por el gobierno de seguridad de la información con el fin de mejorar el proceso de excepción de acceso.

5.1.1 Estandarizar la información.

Esta herramienta permite que la información a compartir se centralice de forma que todos los departamentos involucrados en el proceso puedan ver el estado actual de la información de excepción de acceso, ya que se puede configurar un formulario por defecto donde se solicite la información que el departamento de seguridad de la información requiere para alimentar la evaluación de riesgo. Si alguna información está pendiente por ser ingresada la herramienta informará al usuario con el fin asegurarse de que la información es suministrada en su totalidad.

La información siempre será la misma que manejan los departamentos involucrados en la excepción de accesos, ya que será manejada por la herramienta y estará almacenada en una nube privada, si se hacen cambios será fácil de identificar quien lo realiza, ya que el sistema tiene la característica de dejar en evidencia la fecha, hora y quien realizó el cambio.

5.1.2 Identificación numérica.

La herramienta permite poder asignar un identificador numérico, el cual contribuye a organizar de mejor forma las excepciones de acceso a manejar, actualmente las excepciones se manejan por nombre, esto hace que sea muy tedioso poder encontrarlas, ya que se quedan como documentos adjuntos en correos, se genera dependencia en los gerentes de los departamentos de operaciones o seguridad de la información, lo cual complica la situación al momento de que una de estas personas deje la organización. Igualmente, con el identificador numérico se asegura que la excepción sea única, y se puede hacer fácil la referencia a otra excepción de acceso nombrando dicho código numérico.

5.1.3 Acceso para consulta.

Actualmente, para consultar las excepciones de acceso, se hace mediante la búsqueda de los documentos adjuntos en los correos, sin embargo, esto genera una alta dependencia en quienes administran los departamentos de operaciones (gerentes y/o directores) o el gerente de seguridad de la información, la herramienta permite almacenar dichas excepciones y mantenerlas en la nube privada, garantizando que sean accesibles en cualquier momento por los usuarios que necesitan consultar dichas excepciones, se podría configurar de forma que las personas que responden por una operación a nivel global pueden corroborar que las excepciones generadas en diferentes geografías están alineadas.

5.1.4 Evaluaciones de riesgo.

La herramienta se puede configurar de forma que las excepciones de riesgo más comunes puedan ser cargadas predeterminadamente y solamente se genere cambios particulares en información referente al usuario que la solicita y/o el departamento que será cobijado por la excepción, esto alineará de gran manera las excepciones generadas por el equipo de seguridad de la información, manteniendo una homogeneidad al momento de que se generen en diferentes geografías, siendo una forma de automatizar este proceso que aliviana la carga de trabajo del departamento de seguridad de la información, brindando una transformación digital a este departamento y proceso.

Por otra parte, esta herramienta puede ser configurada de tal forma que permita al gerente de seguridad de la información poder corroborar excepciones de acceso similares a las que está trabajando actualmente, con el fin de poder validar como en escenarios similares fue evaluado el riesgo.

5.1.5 Flujo del proceso.

La interfaz de la herramienta puede ser ajustada para que permita a los usuarios ver el estado de cada etapa que toma para la generación de la excepción de acceso, la herramienta permite dejar consular el estado de cada etapa del proceso con el fin de que todos los grupos de interesados estén actualizados del proceso, se permite ver el nivel de servicio y corroborar si existe algún retraso al momento de generar la excepción de acceso.

Si se requiere alguna información adicional o algún documento, dicha información puede ser incluida en la herramienta, de esta forma se puede tener toda la información documentada dentro del mismo sistema.

En el anexo 8.10 se pudo ver un formato de control de cambios de tecnología, manejado a través de ServiceNow, las imágenes compartidas resaltan aspectos importantes, de cómo la información básica es solicitada y capturada, igualmente de

justificaciones y de proceso de aprobaciones. De esta forma se puede moldear la propuesta de transformación digital para el proceso de excepción de acceso.

5.2 Mejorar interrelación de los departamentos involucrados

Esta comunicación debe ser mejorada para todos los grupos de interés que hacen parte de este proceso, se propone al menos un encuentro semestral entre los diferentes miembros para asegurar una alineación y actualización entre los diferentes grupos de interés que hacen parte de este proceso, en dichos encuentros se puede tocar diferentes aspectos a que a continuación se dan a conocer, la Organización XYZ cuenta con un departamento de Engagement, el cual puede contribuir a mejorar esta interrelación mediante la implementación de diferentes estrategias como lo son: coffee talks, entre otras.

Con base a esto se pueden reducir de gran forma reuniones y dar una mejor perspectiva entre el grupo de interesados, fomentando una nueva cultura que se enfoque más al trabajo en equipo y evitando confrontaciones.

5.2.1 Entender el departamento de operaciones.

Es de vital importancia que el departamento de seguridad de la información y tecnología puedan entender el contexto en el que manobra el departamento de operaciones, principalmente al momento de interactuar con el cliente.

Poder dar a conocer por operaciones a los demás grupos de interesados, como reciben el requerimiento por parte del cliente, siendo esto fundamental; adicionalmente, en que le beneficiaría a nivel operativo y del negocio dicho requerimiento, siendo fundamental para que el departamento de seguridad de la información se ponga en los “zapatos” del departamento de operaciones. Esto referente a los requerimientos que requieren ser manejados a través de una excepción de acceso

Es por esto que, se pueden reducir de gran forma reuniones y dar una mejor perspectiva por parte de seguridad de la información y tecnología hacia el departamento de operaciones.

5.2.2 Entender el departamento de seguridad de la información.

Al igual que la sección anterior, el poder dar un contexto de cómo operará el departamento de seguridad de la información, se pudo contribuir en mejorar la relación entre los departamentos que hacen parte de este proceso, ya que fue posible mencionar las validaciones que deben hacerse de forma global, con el fin de mantener una integridad global al momento de realizar una evaluación de riesgo; así mismo, se informan estados globales referentes a seguridad de la información para clientes corporativos particulares con el fin de mantener la alineación global.

Por consiguiente, es importante que el departamento de seguridad de la información haga validar la importancia de dicho departamento, aprovechando el papel estratégico que juega con el fin de mantener la confidencialidad, integridad y disponibilidad de la información que se confía por parte de los clientes corporativos a la Organización XYZ.

5.2.3 Entender el departamento de tecnología.

El entender el contexto del departamento de tecnología por parte de las otras áreas de interés ayuda en que se interprete el tiempo que toma implementar la solución, con base a los diferentes factores que conlleva (ejemplo: alguna compra o proceso tecnológico que lleve una aprobación adicional como un cambio controlado de infraestructura), es común que al momento que el requerimiento es tomado por el departamento de tecnología sea este departamento presionado de tal forma que se omiten en ciertos casos los niveles de servicio predefinidos en las políticas de servicios de tecnología. Con este espacio se puede informar y poder aclarar expectativas con los grupos de interés adicionales que hacen parte de este proceso.

5.3 Cultura Organizacional

El mejorar la interrelación entre los 3 departamentos, como se expuso en la sección anterior, se puede entender como un cambio de la cultura organizacional; ya que, este cambio se está haciendo a niveles de liderazgo, no llega a quienes en realidad son el primer control de cualquier política de seguridad de la información, los agentes de la Organización XYZ, es vital que se desarrollen acciones adicionales para poder inculcar de forma crítica la importancia de la seguridad de la información, especialmente en estos días, debido a la pandemia que inicio desde finales del 2019, varios de los empleados trabajan desde casa.

Según la estructura organizacional para el departamento de operaciones, un rol muy importante es el Team manager que dirige un grupo de agentes en las diferentes operaciones de los clientes corporativos, si se le inculca a este rol la importancia de seguridad de la información, este rol transmitirá a los agentes el conocimiento sobre la importancia de la seguridad de la información, es un rol vital para compartir el conocimiento y también para poder hacer seguimiento de que las políticas de seguridad de la información se siguen. El poder fomentar una buena relación entre el departamento de seguridad de la información y operaciones puede contribuir a llegar un acuerdo para la implementación de esta recomendación, ya que se deben dedicar recursos de operaciones y de seguridad de la información a esta recomendación.

Por lo que, solamente con el actual gerente de seguridad de la información no es suficiente para poder cubrir la totalidad de team managers, debería existir al menos un especialista de seguridad de la información que pueda ayudar por una cantidad de clientes determinados y poder impartir un entrenamiento de seguridad de información más enfocado a dichas operaciones, esta recomendación referente al equipo directivo de seguridad de la información.

5.4 Gobierno

Varias de las recomendaciones realizadas en este capítulo dependen del Gobierno de Seguridad de la Información, donde se requiere que los directivos de la organización puedan intervenir, con el fin de que las propuestas expuestas en los numerales 5.1 a 5.3 sean implementadas y acatadas, ya que el esfuerzo se debe hacer desde niveles directivos hacia los niveles operativos con el fin de que se pueda implementar las soluciones mencionadas. De aquí, la importancia de la gerencia estratégica o directiva como se mencionó en la sección 2.3.

Adicionalmente en esta sección se dan a conocer factores adicionales que debe tener en cuenta el gobierno de seguridad de la información, para que la propuesta pueda cubrir holísticamente factores adicionales de importancia para la propuesta de solución, a continuación, se mencionan dichos factores.

5.4.1 Contratos

La importancia de que se haga mención de los parámetros de seguridad de la información a los que se alinea la Organización XYZ es importante a la hora de la firma de los contratos con los clientes corporativos, de esta forma se podrá mencionar al cliente que un pilar fundamental de la Organización XYZ es velar por la seguridad de la información, el cliente tendrá el conocimiento de la importancia de esta arista crítica para poder iniciar la implementación de su operación con la Organización XYZ.

5.4.2 Patrocinador de la transformación digital

Hacer los ajustes necesarios en la herramienta de Servicenow como se mencionó en la sección 5.1 son vitales con el fin de poder consolidar la información que se usa para la excepción de acceso, dicha herramienta presenta varios beneficios para la correcta ejecución de este proceso, especialmente para la recolección de información y evaluación del riesgo, con el fin de poder evidenciar resultados efectivos como se mencionó en la sección 2.4. Es el Gobierno de Seguridad de la Información el principal

patrocinador para que sea implementada esta transformación digital, la cual puede ser explotada hasta el punto de generar un nivel de automatización y hacer más ágil este proceso de excepción de acceso.

5.4.3 Estructura de aprobación

La estructura debe ser modificada a un nivel más local, donde las aprobaciones sean manejadas al nivel del país y con los recursos locales que entienden totalmente el contexto de la excepción de acceso, de tal manera, que se dará agilidad a las aprobaciones y dichos aprobadores entenderán de mejor forma el contexto de la necesidad del negocio. El Gobierno de Seguridad de la Información debe hacer notar por qué la importancia de esta estructura con el fin de buscar que el negocio sea más ágil y afrontar de forma eficaz y eficiente los requerimientos de esta índole.

Además, se puede configurar la herramienta que se expone en la sección 5.1., para que dichas aprobaciones queden registradas dentro del sistema de ServiceNow, se podrá mantener un repositorio de las personas que han aprobado. En el apéndice 8.10 se puede evidenciar un ejemplo de cómo se podría configurar la herramienta para el registro de aprobaciones.

5.4.4 Excepciones concedidas en otras geografías para clientes con operaciones globales.

En este escenario el Gobierno de Seguridad de la Información debe implementar una política donde se indique a los Gerentes de Seguridad de la Información que prima la primera excepción de acceso que se generó para clientes globales, estos gerentes deben consultar la documentación de cada cliente mediante la propuesta de la transformación digital para el proceso de excepción de acceso, una vez consultada pueden proceder a conservar la evaluación de riesgo; si dicha evaluación varía, es importante que estos generen, quienes hacen parte de la elaboración de la excepción, puedan discutir y actualizar la excepción de acceso con base al nuevo requerimiento.

6. Recomendaciones y conclusiones

Del análisis hecho a la información recolectada se puede resumir lo siguiente

1. Debería existir una herramienta homogénea y/o base de conocimiento que permita manejar las excepciones de acceso, esto lo concluye en general los 3 departamentos (operaciones, seguridad de la información y tecnología). El proceso que tienen de llenar un formato en un procesador de texto es muy antiguo y dado a tener varias versiones, esto contribuye a que el proceso sea más tortuoso y desgastante. Al tener una herramienta se puede dar cabida a automatizar ciertas evaluaciones de riesgo para definir las excepciones de acceso que son muy comunes de todas las geografías, siendo que mejora el rendimiento del proceso.
2. Los miembros del departamento de seguridad de la información entrevistados afirman que establecer un marco común para la evaluación del riesgo ayudará en tener más homogeneidad al momento de ejecutar dichas evaluaciones, ya que un problema que observan es que no todos los gerentes de seguridad piensan igual, por lo tanto, las evaluaciones son distintas, esto también se evidencia en el análisis de documentos hecho sobre la muestra de documentos tomados para las excepciones de acceso.
3. El implementar la transformación digital para la excepción de acceso contribuye a tener un proceso más ordenado y ágil que satisface las necesidades expuestas en el numeral 1 y 2. Optar por metodologías ágiles para este proceso involucraría un impacto financiero para el departamento de seguridad de la información, ya que, con los recursos limitados (humanos y financieros), con que cuenta dicho departamento, no sería posible la realización de las tareas diarias que deben ejecutar, ya que no poseen el tiempo suficiente para poder ejecutar el proceso bajo dichas metodologías; y las misma, hacen que en momento no se pueda contemplar dicha solución; sin embargo, cabe resaltar que con la funcionalidad de

ServiceNow, si se implementa de la forma correcta, la herramienta puede contribuir a que el proceso se desarrolle de forma ágil, e inclusive automatizada, para la generación de excepciones de accesos particulares a lo largo de las diferentes geografías.

4. Las operaciones deben ser más conocidas por el departamento de seguridad de la información, esto es un común denominador para el área de operaciones y tecnología. Operaciones indica que las discusiones sobre las excepciones de acceso se retrasan, porque deben explicar en reiteradas ocasiones como funciona la operación de un cliente corporativo. Adicionalmente, tecnología y operaciones consideran que seguridad de la información quisieran aplicar controles muy restrictivos, como es el caso de PCI a todos los clientes corporativos, inclusive cuando la operación no tiene contacto con el manejo de tarjetas de crédito.
5. El departamento de tecnología y seguridad de la información, indican que se debe promover a fomentar una conciencia más segura en operaciones, esto se debe iniciar desde la punta de la pirámide hacia abajo. Ya que muchos de los controles son implementados con el fin de poder evitar acciones maliciosas o involuntarias por parte de usuarios, el departamento de seguridad informa que fomentar una conciencia de seguridad de la información es el control más “barato” pero el más difícil de implementar. Con dicha conciencia las operaciones entenderían que lo que busca seguridad de la información es un bien común para toda la Organización XYZ y no exponer a los clientes corporativos a los que se les presta el servicio.
6. El Gobierno de Seguridad de la Información debe reforzarse, esto lo concluye el departamento de operaciones, tecnología y algunos Gerentes de Seguridad de la Información. Se observa por ejemplo que en los contratos firmados entre la Organización XYZ y los clientes corporativos no se nombra en ninguna sección la seguridad de la información, a excepción de los clientes que deben cumplir con certificaciones PCI, dejando en una especie de “nube gris” las reglas de juego de

seguridad de la información con las que opera la Organización XYZ. Operaciones no entiende porque en geografías que pertenecen a la región APAC es más fácil obtener una aprobación de seguridad de la información, pero en América son muchas las discusiones y explicaciones que tienen que dar al momento de implementar un requerimiento que ya funciona sin problemas en geografías de APAC.

7. En general, vale la pena resaltar la importancia que juegan los directivos que conforman el gobierno de Seguridad de la Información, sin su patrocinio, varias de las propuestas mencionadas en este documento no sería posible su ejecución, como lo son: la implementación de la herramienta de ServiceNow para hacer una transformación digital al proceso de excepción de acceso, el mejoramiento en la cultura organizacional referente a la interrelación de los departamentos que están involucrados en el proceso; por último, indicar a los directivos de Operaciones y Comerciales, la importancia de tener en cuenta en los contratos las cláusulas de seguridad de la información. Dichas propuestas deben ser impulsadas por los directivos, ya que, como menciona Shinagl y Sahim (2020), el papel del gobierno de seguridad de la información ha surgido del sótano a las mesas directivas de las organizaciones, contribuyendo al desarrollo del negocio.
8. El no hacer uso de la propuesta expuesta en este documento, conllevaría a que la organización XYZ siga con la problemática, impactando el negocio y empeorando la interrelación de los grupos de interesados y clientes corporativos. Dichos clientes corporativos podrían migrar fácilmente a otros proveedores de la industria de BPO u otras geografías donde opera la organización XYZ. Sin embargo, como la organización XYZ es uno de los líderes de esta industria, la idea es que alcance la madurez en este proceso, especialmente en Colombia para que la organización XYZ pueda seguir creciendo y generando más puestos trabajo, acogiendo más clientes y dichas excepciones sean menos traumáticas de discutir e implementar. Convirtiendo el proceso en uno más ágil que cumple con los estándares de evaluación de riesgo, donde se puede mitigar dicho riesgo de

la forma más conveniente, tanto para el cliente corporativo como para la organización XYZ.

Referencias

- Bell, J. (2005). *Doing your Research Project a guide for frits-time researchers in education, health and social science*. McGraw-Hill Education.
- Bhatti, B. M., Murbak, S., & Nagalingam, S. (2017). A Framework for Information Security Risk Management in IT Outsourcing. *Australian Conference on Information Systems*, 1–9.
- Bhimani, A. (2009). Risk management, corporate governance and management accounting: Emerging interdependencies. *Management Accounting Research*, 20(1), 2–5. <https://doi.org/10.1016/j.mar.2008.11.002>
- Borg, W. R., Gall, M. D., & Gall, J. P. (2003). *Educational Research: An Introductiono Title* (7th ed.). A&B Publications.
- Bowen, G. A., Rowley, J., Healy, M., & Perry, C. (2009). *Document Analysis as a Qualitative Research Method* (Vol. 9, Issue 3). <https://doi.org/10.3316/qrj0902027>
- Brotby, K. (2009). *Information Security Governance*. John Wiley & Sons, Inc. <https://doi.org/10.1002/9780470476017>
- Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. *Information Security Journal*, 21(1), 47–54. <https://doi.org/10.1080/19393555.2011.629341>
- Cascajo Castro, J. L., & García Álvarez, M. (1994). *Constituciones contemporáneas*. Tecnos.
- Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics*

Information Management, 15(5/6), 358–368.

<https://doi.org/10.1108/09576050210447046>

Coertze, J., & von Solms, R. (2012). A Model for Information Security Governance in Developing Countries. *Africomm*, 119, 279–288.

Dhillon, G., Syed, R., & Sá-Soares, F. de. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information and Management*, 54(4), 452–464. <https://doi.org/10.1016/j.im.2016.10.002>

di Serio, L. C., de Oliveira, L. H., & Schuch, L. M. S. (2011). Organizational risk management - A case study in companies that have won the Brazilian quality award prize. *Journal of Technology Management and Innovation*, 6(2), 230–243. <https://doi.org/10.4067/S0718-27242011000200016>

Dinero. (2013). *BPO en Colombia*. <https://www.dinero.com/empresas/articulo/bpo-colombia/189955>

Dinero. (2017). *Tercerización de servicios en Colombia 2017*.

<https://www.dinero.com/edicion-impres/negocios/articulo/tercerizacion-de-servicios-en-colombia-2017/246830>

Eisner, E. W. (1991). *The enlightened eye: Qualitative inquiry and the enhancement of educational practice*. Collier Macmillan.

Ekmekdjian, M. Á. (1999). *Manual de la Constitución Argentina* (4ta ed.). Depalma.

Friedman, B., Khan, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM*, 43(12), 34–40. <https://doi.org/10.1145/355112.355120>

Gallimore, D. (2020). *Ensuring Data Security with Business Process Outsourcing Companies*. Ensuring Data Security with Business Process Outsourcing

- Companies. <https://heimdalsecurity.com/blog/data-security-with-business-process-outsourcing/>
- González, R., Gascó, J., & Llopis, J. (2016). Information systems outsourcing reasons and risks: Review and evolution. *Journal of Global Information Technology Management*, 19(4), 223–249. <https://doi.org/10.1080/1097198X.2016.1246932>
- Grove, R. W. (2010). *International Journal of Qualitative Studies in Education An analysis of the constant comparative method An analysis of the constant comparative method*. September 2014, 37–41. <https://doi.org/10.1080/0951839900030105a>
- Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, 42(4), 80–85. <https://doi.org/10.1145/299157.299175>
- Imai, M. (1986). *Kaizen: The Key To Japan's Competitive Success*. McGraw-Hill Education.
- Innovature Consulting. (2021). *Information Security: The biggest challenge for BPO providers | BPO Accounting and Business solutions*. INFORMATION SECURITY: THE BIGGEST CHALLENGE FOR BPO PROVIDERS. <https://innovatureinc.com/information-security-the-biggest-challenge-for-bpo-providers/>
- International Organization for Standardization - International Electrotechnical Commission. (2005). Information technology : security techniques : code of practice for information security management = Technologies de l'information: techniques de sécurité : code de pratique pour la gestion de sécurité

- d'information. International Standard, ISO/IEC 17799 (2005), xi, p. 115.
- ISACA. (2009). *Marco de Riesgos de TI*.
- ISACA. (2012). *COBIT 5 Para la Seguridad de la Información*. ISACA.
- ISO. (2008). ISO/IEC 27001:2005 - Information technology — Security techniques — Information security management systems — Requirements Technologies. *Information Systems*, 2008, 34.
- ISO & IEC (2013). ISO/IEC 27002:2005 (E). 2005, p. 25–27. www.iso.org
- IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management Guidance for Boards of Directors and Executive Management*. <https://doi.org/www.itgi.org>
- IT Governance Institute. (2007). COBIT Security Baseline: An Information Survival Kit, 2nd Edition. In *Information Security* (2nd ed.).
- Kelley, D. (2014). *NIST Risk Management Framework Overview*. 1–43.
- Kovacich, G., & Haliobazek, E. (2016). *Security Metrics Management* (Elsevier (ed.); 2nd ed.). Elsevier.
- López Guerra, L. (2001). *Estudios de derecho constitucional : homenaje al profesor Dr. D. Joaquín García Morillo* (Editorial Tirant Lo Blanch (ed.); 1st ed.). Tirant lo Blanch.
- Magnu, C., & Chou, S.-C. (2010). Risk and Compliance Management Framework for Outsourced Global Software Development. *2010 5th IEEE International Conference on Global Software Engineering*, 228–233. <https://doi.org/10.1109/ICGSE.2010.34>

- Moen, R., & Norman, C. (2009). Evolution of the PDCA Cycle. *Society*, 1–11.
- Mulhall, A. (2003). *METHODOLOGICAL ISSUES IN NURSING RESEARCH In the field: notes on observation in qualitative research*.
<https://doi.org/https://doi.org/10.1046/j.1365-2648.2003.02514.x>
- National Institute of Standards and Technology Gaithersburg. (2012). Guide for conducting risk assessments. *NIST Special Publication*, 1, 95.
<https://doi.org/10.6028/NIST.SP.800-30r1>
- Oecd. (2015). OECD Principles of Corporate Governance. *World*, 46.
<https://doi.org/10.1787/9789264015999-en>
- PCI Security Standards Council. (2013). *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures (Version 3.0)*. May, 1–112. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
- Pretzlik, U. (1994). Observational methods and strategies. *Nurse Researcher*, 2(2), 13–21. <https://doi.org/10.7748/nr.2.2.13.s3>
- Real Academia Española. (2017). *gobernanza | Definición de gobernanza - Diccionario de la lengua española - Edición del Tricentenario*. Diccionario de La Lengua Española | Edición Del Tricentenario . <http://dle.rae.es/?id=JHRSmFV>
- Ross, J. W., Weill, P. D., & Robertson, D. C. (2006). *Enterprise Architecture as Strategy — Creating a Foundation for Business Execution*. Harvard Business School Press.
- Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, 9(2), 107–118. <https://doi.org/10.1016/j.aci.2011.05.002>

- Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, 18(1), 45–52. <https://doi.org/10.1016/j.jisa.2013.07.002>
- Sherwood, J., Clark, A., & Lynas, D. (2009). Enterprise Security Architecture. *SABSA White Paper*, 6(4), 43–54. <https://doi.org/10.1080/10658989809342548>
- Singh, T., & Manusama, B. (2016). *Gartner - Magic Quadrant for Customer Management Contact Center BPO*. December.
- Tohidi, H. (2011). The role of risk management in IT systems of organizations. *Procedia Computer Science*, 3(2010), 881–887.
<https://doi.org/10.1016/j.procs.2010.12.144>
- Turner, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report*, 15(3), 754–760.
<https://doi.org/http://www.nova.edu/ssss/QR/QR15-3/qid.pdf>
- Vallano, J. P., & Compo, N. S. (2011). A comfortable witness is a good witness: Rapport-building and susceptibility to misinformation in an investigative mock-crime interview. *Applied Cognitive Psychology*, 25(6), 960–970.
<https://doi.org/10.1002/acp.1789>
- Veiga, A. Da, & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management*, 24(4), 361–372.
<https://doi.org/10.1080/10580530701586136>
- Von Solms, B. (2000). Information Security — The Third Wave? *Computers & Security*, 19(7), 615–620. [https://doi.org/https://doi.org/10.1016/S0167-4048\(00\)07021-8](https://doi.org/https://doi.org/10.1016/S0167-4048(00)07021-8)
- Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information Security

Governance control through comprehensive policy architectures. *2011 Information Security for South Africa*, 1–6.

<https://doi.org/10.1109/ISSA.2011.6027522>

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information Security Risk Management Framework for the Cloud Computing Environments. *2010 10th IEEE International Conference on Computer and Information Technology, 2007*, 1328–1334. <https://doi.org/10.1109/CIT.2010.501>

Anexos

Anexo 1. Amenazas Humanas: Fuente de amenaza. Motivación y acciones de amenaza.

Tabla 14. Amenazas Humanas: Fuente de amenaza. Motivación y acciones de amenaza.

Fuente de amenaza	Motivación	Acciones de amenaza
Hacker, Cracker	Reto Ego Rebelión	Hacking ingeniería Social Intrusión a un sistema Acceso no autorizado a un sistema.
Criminal Computacional	Destrucción de información Publicación ilegal de información Ganancias monetarias Alteración ilegal de datos	Crimen computacional (ciber asecho) Actos fraudulentos (interceptación, etc.) Alteración de información Falsificación Intrusión a un sistema
Terrorismo	Chantaje Destrucción Explotación Venganza	Bomba / Terrorismo Guerra de Información Ataque a sistema (Denegación de servicio) Penetración de sistema Manipulación del sistema
Espionaje Industrial (Compañías, gobiernos extranjeros)	Ventaja Competitiva Espionaje económico	Explotación económica Robo de información Intrusión a información personal Ingeniería Social Penetración a un sistema Acceso no autorizado a sistemas.

Insiders (con poco entrenamiento, maliciosos, negligente, deshonestos o empleados terminados)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores no intencionales y omisiones	Asalto a un empleado Chantaje Navegación de información propietaria Abuso de computador Fraude y robo Alteración de información Entrada de información falsa o corrupta Interceptación Código malicioso Venta de información personal bugs del sistema Intrusión a sistemas sabotaje de sistemas Acceso no autorizado de sistemas.
---	---	---

Fuente: Recuperado de Kelley (2014).

Anexo 2. Pares de vulnerabilidad y amenaza.

Tabla 15. Pares de vulnerabilidad y amenaza.

Vulnerabilidad	Fuente de amenaza	Acción de Amenaza
Usuario de empleado terminado no es removido del sistema	empleado terminado	Comunicación a la red interna de la compañía para acceder información de propiedad de la organización.
Firewall de la compañía permite telnet entrante, Usuario invitado está habilitado en servidor XYZ.	usuarios no autorizados	Usar telnet para comunicarse con servidor XYZ y navegar en archivos de la organización mediante el usuario invitado.
Fabricante ha identificado fallas en el diseño de seguridad del sistema, sin embargo, nuevos parches no han sido aplicado al sistema.	usuarios no autorizados	Obtener acceso no autorizado a información de sistemas sensibles
Data center usa aspersores de agua para suprimir fuego, control para proteger el hardware y equipos del agua no están preparados.	Fuego, persona negligente	Activar aspersores de agua dentro del data center

Fuente: Recuperado de Kelley (2014).

Anexo 3. Documento PCI DSS.



Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirements	Testing Procedures	Guidance
<p>1.1 Establish and implement firewall and router configuration standards that include the following:</p>	<p>1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:</p>	<p>Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network.</p> <p>Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.</p>
<p>1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations</p>	<p>1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all:</p> <ul style="list-style-type: none"> • Network connections and • Changes to firewall and router configurations 	<p>A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall.</p> <p>Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.</p>
	<p>1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.</p>	

Fuente: Payment Card Industry – PCI. Data Security Standard, v3.2.1

Anexo 4. Instrumento de observación

LOG número: 1**Cliente:** Cliente Corporativo 1**Requerimiento Inicial:** Instalación de laboratorio para manipula con de malware dentro de las instalaciones de la Organización XYZ.

Anotación Número	Notas de Campo
1	Gops del programa ClienteCorp hace solicitud al departamento TI mediante un número de ticket RITM0384749, la solicitud hace referencia en agregar unos dispositivos móviles electrónicos que no son estándares dentro del área de operación del cliente, bajo la figura de laboratorio de pruebas. Adicionalmente el Gops solicita un acceso de internet abierto para hacer la respectiva conexión de dichos dispositivos.
2	Gti indaga más a profundidad sobre el requerimiento con Gops , por lo cual Gti elabora más a profundidad el requerimiento sobre el laboratorio, Gops expresa que el objetivo del laboratorio es permitir a los empleados tener experiencia sobre el manejo del producto que manejan el cual es un antivirus. Gti , mediante correo electrónico que comparte con el Ginfosec , le informa de que trata el requerimiento realizado por parte de Gops .
3	Ginfosec informa que este tipo de configuración se debe completar mediante una conexión a internet abierta, sin embargo, expresa que está esperando aprobación de Vinfosec para poder autorizar la configuración del laboratorio, mediante una conexión a internet abierta. La comunicación es entregada al Gops y Gti .
4	El Gops solicita una actualización a Ginfosec sobre el estado de la aprobación por parte de Vinfosec . No obstante, Vinfosec no ha validado el requerimiento de acuerdo a lo comunicado por Ginfosec
5	Gops solicita a Gti en iniciar la implementación de la solución requerida por el cliente, pero Gti involucra a Ginfosec , para poder validar el estado de la aprobación por parte de Vinfosec

-
- | | |
|---|--|
| 6 | Ginfosec , comparte EA con Gops y Gti , EA contempla los riesgos percibidos por Ginfosec , así mismo, se comparten los controles que pueden mitigar el riesgo. |
| 7 | Gti informa al Dti regional (LATAM) y Vti de Américas sobre la EA |
| 8 | Gti , solicita clarificación a Ginfosec sobre algunos de los controles sugeridos ya que técnicamente no cumplen con lo requerido por parte de operaciones |
-

Fuente: Elaboración propia.

Anexo 5. Herramienta de análisis documental.

Anexo 5.1. Herramienta para análisis de documentos de excepción de acceso

Numeración documento	Nombre excepción de acceso	Categoría Excepción	Cliente solicitante	Número Ticket	Geografía	Gerente de Seguridad	Explicación Requerimiento		Justificación del Negocio		Evaluación del Riesgo			Controles	
							Análisis	Asertividad	Análisis	Asertividad	Análisis	Asertividad	Uso de escala de medición	Análisis	Asertividad
1	Acceso a Social Media	C16	Soporte	RITM0241805	Colombia	Javier B	Usuario en el requerimiento solo informa que debe acceder a ciertos sitios de social media, sin embargo no se tiene claridad del porque	No es asertivo	En el documento compartido, no se documenta justificación del negocio para poder estudiar el requerimiento.	No es asertivo	Sin la documentación necesaria por parte de operaciones, el gerente de seguridad hace evaluación, sin entender el porque el usuario solicita el acceso mencionado.	No es asertiva, ya que no se ha identificado la necesidad de negocio para validar si los riesgos evaluados van acordes a la evaluación del riesgo.	Si cualitativa	Se mencionan los controles que mitigaran los riesgos expuestos por el gerente, sin embargo no se asigna un responsable en implementar cada control.	No es asertivo por la falta del total entendimiento del requerimiento por parte del gerente de infosec
2	Vendor ID Creación	C1	Soporte	RITM0458035	Colombia	Javier B	El usuario hace requerimiento sin mayor detalle.	No es asertivo ya que no se entiende porque se hace el requerimiento	En el documento compartido, no se documenta justificación del negocio para poder estudiar el requerimiento.	No es asertivo	Sin la documentación necesaria por parte de operaciones, el gerente de seguridad hace evaluación, sin entender el porque el usuario solicita el acceso mencionado.	No es asertiva, ya que no se ha identificado la necesidad de negocio para validar si los riesgos evaluados van acordes a la evaluación del riesgo.	Si cualitativa	Se mencionan los controles que mitigaran los riesgos expuestos por el gerente, sin embargo no se asigna un responsable en implementar cada control.	No es asertivo por la falta del total entendimiento del requerimiento por parte del gerente de infosec
3	Web access to Email	C3	Soporte	RITM0458396	Colombia	Javier B	El usuario hace requerimiento sin mayor detalle.	No es asertivo ya que no se entiende porque se hace el requerimiento	En el documento compartido, no se documenta justificación del negocio para poder estudiar el requerimiento.	No es asertivo y este requerimiento conlleva a una gran escalación	Sin la documentación necesaria por parte de operaciones, el gerente de seguridad hace evaluación, sin entender el porque el usuario solicita el	No es asertiva, ya que no se ha identificado la necesidad de negocio para validar si los riesgos evaluados van acordes a la evaluación del riesgo.	Si cualitativa	Se mencionan los controles que mitigaran los riesgos expuestos por el gerente, sin embargo no se asigna un responsable en implementar	No es asertivo por la falta del total entendimiento del requerimiento por parte del gerente de infosec
4	Use of Sticky notes and calculator	C17	Operations	RITM0357639	Colombia	Javier B	El usuario hace requerimiento mencionando una falla en unos aplicativos del sistema operativo.	No es asertivo ya que no se entiende a profundidad cual es la falla	En el documento compartido, no se documenta justificación del negocio para poder estudiar el requerimiento.	No es asertivo y este requerimiento conlleva a una gran escalación	Sin la documentación necesaria por parte de operaciones, el gerente de seguridad hace evaluación, sin entender el porque el usuario solicita el	No es asertiva, ya que no se ha identificado la necesidad de negocio para validar si los riesgos evaluados van acordes a la evaluación del riesgo.	Si cualitativa	Se mencionan los controles que mitigaran los riesgos expuestos por el gerente, sin embargo no se asigna un responsable en implementar	No es asertivo por la falta del total entendimiento del requerimiento por parte del gerente de infosec
5	Federation access - skype for business	NA	Operations	RITM0432430	EELU	John L	En la descripción del requerimiento no es claro del porque se necesita el acceso, se hace el requerimiento de forma muy simple	No es asertivo en la explicación del requerimiento	La descripción es clara ya que el usuario provee el caso de uso al gerente de seguridad de la información dentro del documento de excepción de acceso	Si es asertivo ya que menciona los beneficios que se esperan tener del acceso solicitado	En los riesgos contemplados, se mencionan la mayoría de problemas que pudiese llegar a ocasionarse por habilitar el acceso, adicionalmente se mencionan las posibles amenazas de habilitar el acceso	La evaluación del riesgo si es asertiva, ya que plasma las amenazas y riesgos de conceder el acceso	ND	La descripción de los controles hacen intuir que la mayoría de los riesgos serán controlados	se mencionan los equipos de tecnología en general, no se especifica en realidad quien es el owner de tecnología que deberá implementar los controles. Debería ser mas metodoso al momento de exponer quien es el dueño del control
6	Enabling USB port	C6 C18	Operations	INC0472496	EELU	John L	En el incidente abierto solo se informa que el dispositivo de escaneo no funciona.	No es asertivo.	El usuario da el caso de uso de la excepción de acceso, solamente informan que necesitan escanear documentos de pacientes pero no se explica a fondo la razón del negocio para	No es asertivo.	No se hace evaluación del riesgo por parte del gerente	NA	ND	Se menciona un controles que están pocos detallados, dichos controles son: USB no esta habilitado para el almacenamiento de información y el portátil donde	no es asertivo ya que la evaluación de riesgo es muy pobre y no se entiende si el control ayudara a suplir los riesgos.
7	NT ID and e-mail access to be created for intern	C1 / C2	Soporte	RITM0328973	Jamaica	Paulina W	El requerimiento es claro	Si es asertivo ya que indica para que la persona necesita el acceso.	El usuario informa el caso de uso para que se de el acceso	La explicación no indica de que forma se beneficiaria el negocio de concederle a la persona el acceso.	Se deja en claro los riesgos que conllevan la otorgación del acceso a las personas	Si es asertivo ya que se determina un dueño, adicionalmente se hace hincapié en las amenazas que podrían afectar la organización	Si cualitativa	Se sugieren los controles pero no se mencionan quien es el dueño de completarlo, por ejemplo se necesita ayuda de RH, Operaciones y tecnología para poder tener los controles	Si es asertivo a pesar de que no se menciona con claridad quien es el responsable de cada control.
8	Request to take paper into production floor	NA	Operations	RITM0165435	Jamaica	Paulina W	El requerimiento es muy bien explicado, se entiende muy claramente la necesidad que tiene el usuario de introducir papel para escribir al piso de producción	Si es asertivo.	La justificación del negocio es clara, se menciona de que forma se beneficiaria el cliente al introducir papel a su operación.	Si es asertivo.	El gerente de seguridad de la información informa que el programa no maneja información sensible como numero des tarjetas de crédito, sin embargo la evaluación hecha queda corta en argumentos por parte de seguridad de la	No es asertivo, ya que considero que se deben hacer una inspección mas a profundidad.	Si cualitativa	Se mencionan los controles sin embargo no se asigna quien es el responsable	no es asertivo.

Fuente: Elaboración propia.

Anexo 5.2. Categoría de excepciones

Categoría Excepciones	Código
Usuario NT para contratistas / proveedores	C1
Usuario de correo para contratistas / proveedores	C2
Acceso web correo para contratistas / proveedores	C3
Acceso a escritorio remoto	C4
Privilegios de administrador local	C5
Acceso a puerto USB, unidad de CD/DVD	C6
Usuario NT concurrente	C7
Uso de USB / permiso de administrador para portátiles	C8
Recuperación de datos	C9
Solicitud de cámara WEB	C10
Respaldo de información en disco duro externo	C11
Instalación de clientes de mensajería no corporativos (Yahoo!!!, Messenger, Skype)	C12
Instalación de herramientas para compartir pantalla	C13
Escritura de CD / DVD	C14
Conectividad DSL, instalación de laboratorio	C15
Acceso a un nuevo sitio web	C16
Software que no es estándar dentro de la organización	C17
Excepción a dispositivos electrónicos	C18
Excepción a uso de teléfonos móviles	C19

Fuente: Elaboración propia.

Anexo 6. Ejemplo excepción de acceso

Exceptional Access Request Form	
<p><u>Program name / Function and location:</u> Corporate Client Name</p> <p><u>Program / Function Head:</u> Name Account Manager</p> <p><u>Avaya No / Contact #</u> 790343</p>	<p><u>Date of request:</u> 12th June</p>
<p><u>Access requested by:</u> Name requester</p> <p><u>Employee #</u> : if Consultant – NDA signed date:</p>	<p>Period of Access (From - To date): Indefinite</p>
<p><u>Describe the type of request</u></p>	<p><u>Ticket#:</u> RITM0365029</p>
<p>To be filled by SD / Function</p> <p><u>Business Justification: Perceived Risk:</u> Lab devices to be set up in lock and key</p> <p><u>Has the client been informed, if client data is being shared:</u> There is no client data shared in lab devices</p>	
<p><u>If records are shared:</u> Records are not shared</p> <p><u>1. Mode of sharing / access</u></p> <p><u>2. Retention period</u> (up to what date)</p> <p><u>3. Destruction of Data</u> (Mention the date after which the date to be deleted)</p> <p>Can Company XYZ Audit the outsourced / external source</p>	

Risk As perceived by InfoSec

Infosec Risk Assessment				
Business Case: Set Up a Lab room with Open Internet for training AV installation, check errors and other tasks.				
Vulnerabilities	Threats	Criticality	Owner	InfoSec Requirements
Data Leakage	SGS Data/Client Data/Customer Data can be leaked outside of Company XYZ infrastructure via external DSL using web based e-mail, file sharing websites/software, blogs, forums without a way to track the user/source, etc.	High	IT	Apply a local GPO, whenever possible, based on the principle of least privilege - (ex. No run command, no control panel, only permit approved executables, block all websites/browsers/software/USBStore/Optical drive disablement, bios password etc.) USB Devices must be locked from the BIOS, and also applying a GPO.
Connection of non-Corp Client devices	Non corporate client employees can connect to the Wireless Network with malicious purposes	High	IT	Only the ports needed for connecting the corporate client devices can be enabled on Lab Router. The subnet mask of the network should have as many hosts as the number of devices that will be connected. For ensuring external devices can't be connected to the Lab Router, they must be secured by the MAC address. All devices that have a LAN port must be connected by cable, and not by Wi-Fi. Devices that will be connected Wirelessly, must also be secured by MAC so not external devices can be connected to the network. If a device should be removed, the subnet mask must be reduced if the removal is permanent.

Unauthorized Software	Download of unauthorized software, hacking/cracking tools, scanning tools and also Installation of unauthorized software may lead into legal penalties	High	IT	Apply a local GPO based on the principle of least privilege - (ex. No run command, no control panel, block all websites/browsers/software/USBStore/Optical drive disablement, bios password etc.) The most restrictive GPO hardening policies should be applied. USBs must be disabled from BIOS
Virus	Risk of Virus and Malware which can steal critical information and destroy potential information and data, and also infect network systems	High	IT	Ensure AV software is always up to date, so do the Operating System patches.
Complete control over the system as an administrator	Local GPO and other parameters can be overridden if default system login has administrator rights	High	IT	System will be configured with two accounts: User account (minimal rights (Training use)) and a maintenance account (admin rights only IT has access to this account) No generic users should be used. All users configured in the lab systems, must come from Active Directory. External users access is not allowed to those Devices. Initial password should be required and ask for change after the first login. Domain password, users and Audit policies should be replicated locally on those Devices whenever possible. No RDP connection is allowed to / from Lab Devices
Physical Access Accountability	Non corporate client employees may try to access Lab room for malicious purposes	HIGH	Physical Security	Access to Lab room should be granted only to the Corp Client employees that require such access. In Lab room no other Devices, different from those pertaining to the Lab can be located. CCTV cameras, one focusing the main door entrance and the other inside the room covering all Devices should be implemented.
System Misuse	Systems could be used for a purpose other than intended	High	SD	Employees need to be fully aware and reminded that this system shall be used only for business purposes only

Access to non-authorized / inappropriate / malicious websites	Lab systems can be used for accessing non-appropriate websites, such access may lead to network infection, copyright issues, bandwidth saturation and so on.	High	SD	A whitelist, based on the one current in place for Corp Client Production Floor, should be implemented on Lab Systems. It is suggested to always use a whitelist instead a category-based list.
---	--	------	----	---

Disclaimer

The element of risk associated with this exposure is not eliminated / not absolved / not mitigated by providing an approval by InfoSec

- The risk remains with The requestor
- The responsibility of watching The time line and take action to get back to normal process rests with The requestor. – Confirmation is required from The requestor.
- Requestor to make sure that The exception is not miss-utilized

Approval from Client:
Approval from L8 / Country head:
Approval from Infosec Head / Manager.

Nota: El contenido de este anexo está en idioma inglés, para no alterar dicho contenido. (Idioma original).

Fuente: Elaboración propia. Recuperado de Organización XYZ.

Anexo 7. Instrumento de entrevistas

Anexo 7.1. Entrevista para el departamento de operaciones.

Recolección de requerimientos del negocio y definición de alcance

1. ¿Considera usted que el cliente tiene un buen conocimiento sobre las políticas de seguridad de la información que maneja la Organización XYZ?
2. ¿Los requerimientos que necesitan una excepción de acceso, están acordes al contrato pactado entre el cliente corporativo y la Organización XYZ?
3. ¿De los requerimientos recibidos por el cliente, alguno está implementado en otra geografía? ¿Cómo ha intentado replicar dicha implementación en su operación?

Socialización con el departamento de Seguridad de la información

4. ¿Cuándo usted efectúa el requerimiento al departamento de seguridad de la información, tiene conocimiento si está acorde a las políticas de seguridad de la información de la compañía XYZ?
5. ¿Qué conocimiento tiene usted sobre las políticas de seguridad de la información desarrolladas por la Organización XYZ?
6. ¿Usted como gerente de la cuenta, ejemplifica el caso de uso de llegar a ser aprobada la excepción de acceso?
7. ¿Cuándo usted hace el requerimiento al área de seguridad de la información, considera que ellos tienen pleno entendimiento del requerimiento?

Para excepciones de acceso aprobadas

8. ¿Los controles sugeridos, están acordes al requerimiento hecho?
9. ¿El cliente está satisfecho con la solución ofrecida?
10. ¿Los controles sugeridos por el departamento de seguridad de la información son de fácil implementación por parte del departamento de tecnología?

Para excepciones de acceso negadas

11. ¿El cliente corporativo está informado sobre las políticas de seguridad de la información que se manejan en la Organización XYZ?
12. ¿Cómo se afectó el desarrollo y/o operación del negocio?
13. ¿Qué negocio se ha perdido por la denegación e la excepción de acceso?
14. ¿En el contrato que hace SGS con el cliente corporativo, se aclara el procedimiento a exceptuar mediante la excepción de acceso?
15. ¿El cliente estaría dispuesto a incluir dicha excepción como una adición al contrato que mantiene con la Organización XYZ?

Lecciones aprendidas

16. ¿Como usted puede sugerir una mejora a este proceso?
17. ¿El documento compartido por seguridad de la información es lo suficientemente inclusivo para describir el requerimiento?
18. ¿Observa algún tipo de desalineamiento entre los departamentos de seguridad de la información y tecnología?
19. ¿El acompañamiento del departamento de seguridad de la información y tecnología es el adecuado en el proceso?
20. ¿El documento generado por seguridad de la información es de fácil entendimiento por parte de operaciones?
21. ¿Considera que el documento generado para la excepción de acceso es de fácil entendimiento para otras geografías donde opera el mismo cliente corporativo?
22. ¿Observa desconexiones en el departamento de seguridad de la información a nivel regional, en el momento de aprobar una excepción de acceso?

Fuente: Elaboración propia.

Anexo 7.2. Entrevista para el departamento de seguridad de la información.

Recibimiento del requerimiento por el área de seguridad de la información.

1. ¿Considera usted que el área de operaciones es claro al explicar el requerimiento?
2. ¿El requerimiento posee una sólida justificación del negocio?
3. ¿El requerimiento está acorde con las políticas de seguridad de la información establecidas por la Organización XYZ?
4. ¿El área de operaciones comparte suficiente documentación para validar el requerimiento del cliente?
5. ¿El área de operaciones le informa si la excepción fue concedida y está en funcionamiento en otro sitio?
6. ¿Tiene conocimiento si el requerimiento hecho por el departamento de operaciones está acorde con el contrato establecido por el cliente corporativo y la Organización XYZ?

Etapas de análisis del requerimiento por el departamento de seguridad de la información

7. ¿Usualmente que metodología de evaluación del riesgo aplica para conceder o denegar la excepción de acceso?
8. ¿El formato que es usado por la Organización XYZ es lo suficientemente claro para recoger la mayor cantidad de información por parte del solicitante de la excepción?
9. ¿Considera usted que la implementación de un marco común, para la evaluación del riesgo, podría traer beneficios al área de seguridad de la información?

Para excepciones de acceso aprobadas

10. ¿Los controles sugeridos son alcanzables al momento de implementar por parte del departamento de tecnología?
11. ¿Como considera que asume el departamento de operaciones los controles sugeridos por el área de seguridad de la información?
12. ¿Tiene conocimiento si el cliente está satisfecho con la solución ofrecida?
13. ¿El departamento de operaciones le ha sugerido cambios en los controles desarrollados?
14. ¿El costo de implementar los controles sugeridos por la excepción de acceso razonable vs el riesgo a mitigar?
15. ¿En algún momento ha transferido el riesgo como parte de la aprobación hacia el cliente?

Para excepciones de acceso negadas

16. ¿Como se ve afectado el área de seguridad de la información ante la Organización y el cliente al momento de no aprobar una excepción de acceso?
17. ¿Las negaciones de acceso han contribuido de alguna manera al negocio de la Organización XYZ?
18. ¿Parte de la negación de la excepción de acceso ha sido a consecuencia de la no aceptación de los controles sugeridos por parte del área de seguridad de la información a operaciones?
19. ¿Qué opina la persona a quien usted reporta de las excepciones no aprobadas?

Lecciones aprendidas

20. ¿Cómo considera se puede mejorar el proceso de excepción de acceso?
21. ¿Considera que una herramienta más especializada en el tomar este requerimiento puede contribuir mejor al funcionamiento del proceso?
22. ¿Cómo cree usted que se le puede dar agilidad a este proceso?
23. ¿Qué propone usted para que el cliente corporativo y el área de operaciones entiendan más a profundidad las políticas de seguridad de la información establecidas por la Organización XYZ?
24. ¿Considera usted que las políticas de seguridad de la información son muy restrictivas?
25. ¿Evidencia desalineamiento entre los requerimientos y justificación de negocio hechos por el área de operaciones?
26. ¿Cómo considera que se puede mejorar la estructura de aprobación para excepciones de acceso que involucran operaciones de clientes globales?

Fuente: Elaboración propia.

Anexo 7.3. Entrevista para el departamento de Tecnología.

Previa observación

1. ¿Cómo percibe la interacción entre los departamentos de seguridad de la información y operaciones, ante la discusión de una excepción de acceso?
2. ¿Ha podido evidenciar una desalineación entre los departamentos de seguridad de la información y seguridad de la información?
3. ¿Considera usted que el departamento de seguridad de la información tiene un buen conocimiento sobre las políticas de seguridad de la información?
4. ¿El departamento de operaciones es lo suficientemente claro al momento de sustentar el requerimiento hecho por el cliente corporativo?
5. ¿Qué opina sobre la interpretación que le da el departamento de seguridad de la información al requerimiento realizado por el departamento de operaciones?
6. ¿Observa alguna de las partes aclarar puntos en específico sobre el requerimiento y/o la excepción de acceso?

Recibimiento e implementación de la excepción de acceso

7. En el momento que recibe la excepción de acceso por parte del departamento de seguridad de la información, ¿considera que es acorde con el requerimiento hecho por el departamento de operaciones?
8. ¿Los controles sugeridos van acordes con los recursos que dispone la Organización XYZ?
9. ¿Ha solicitado el analizar nuevamente una excepción de acceso al departamento de seguridad de la información?
10. ¿Una vez el departamento de tecnología implementa los controles sugeridos por el departamento de seguridad de operación, cree usted que el departamento de operaciones está satisfecho con la solución implementada para mitigar el riesgo?
11. ¿Son sostenibles los controles de mitigación de riesgo sugeridos por el departamento de seguridad de la información?
12. ¿Los controles sugeridos por el departamento de seguridad de la información son de entendible administración por parte del departamento de tecnología?

Lecciones aprendidas

13. ¿Cómo considera que se puede mejorar este proceso?
14. ¿Los controles sugeridos por seguridad de la información son lo suficientemente claros para la implementación?
15. ¿Considera que alguna herramienta podría mejorar la recolección de requerimientos que debe entregar el departamento de operaciones?
16. ¿Considera que alguna herramienta podría ayudar a mejorar la visibilidad en el proceso?
17. ¿Qué opina de la estructura de aprobación de excepciones de acceso que involucra operaciones de clientes globales?

Fuente: Elaboración propia.

Anexo 8. Integración y asociación de categorías

Fuente	Categoría	Asociación categorías	Variable número	Nombre Variable	Frecuencia Repetición
Análisis entrevistas tecnología	Flexibilidad en la evaluación	11	1	Flexibilidad en la evaluación	1
Análisis entrevistas tecnología	Auditoría al control	12	2	Auditoría	1
Análisis entrevistas seguridad de la información	Concientización	13	3	Concientización	1
Análisis de información: Análisis de documentos	No apego al proceso	14	4	No apego al proceso	1
Análisis de información: Análisis de documentos	Dueño del control	15	5	Dueño del control	1
Análisis de información: Observación	Reprocesamiento	1	6	Reprocesamiento	2
Análisis entrevistas Operaciones	Reprocesamiento	1			
Análisis entrevistas Operaciones	Entender el negocio	2	7	Entender el negocio	2
Análisis entrevistas tecnología	Entender el negocio	2			
Análisis de información: Observación	Alineamiento global	3	8	Alineamiento global	3

Análisis entrevistas Operaciones	Alineamiento global	3			
Análisis entrevistas tecnología	Desconexiones	3			
Análisis entrevistas Operaciones	Base de conocimiento	4	9	Base de conocimiento	3
Análisis entrevistas seguridad de la información	Base de conocimiento	4			
Análisis entrevistas tecnología	Base de conocimiento	4			
Análisis de información: Análisis de documentos	Homogeneidad	6	10	Homogeneidad	3
Análisis entrevistas Operaciones	Homogeneidad	6			
Análisis entrevistas tecnología	Homogeneidad	6			
Análisis entrevistas Operaciones	Estructura de aprobación	8	11	Estructura de aprobación	3
Análisis entrevistas seguridad de la información	Estructura de aprobación	8			
Análisis entrevistas tecnología	Estructura de aprobación	8			
Análisis entrevistas Operaciones	Gobernabilidad	9	12	Gobernabilidad	3
Análisis entrevistas seguridad de	Gobernabilidad	9			

la información					
Análisis entrevistas tecnología	Gobernabilidad	9			
Análisis de información: Análisis de documentos	Precisión	10	13	Claridad del requerimiento	3
Análisis de información: Observación	Claridad del requerimiento	10			
Análisis entrevistas tecnología	Claridad del requerimiento	10			
Análisis entrevistas Operaciones	Captura de requerimiento	5	14	Captura del requerimiento	4
Análisis entrevistas seguridad de la información	Captura del requerimiento	5			
Análisis entrevistas tecnología	Tecnología interfaz de comunicación	5			
Análisis entrevistas tecnología	Captura requerimiento	5			
Análisis de información: Observación	Definición de niveles de servicio	7	15	Niveles de servicio	4
Análisis entrevistas Operaciones	Niveles de servicio	7			
Análisis entrevistas tecnología	Niveles de servicio	7			
Análisis de información: Observación	Atención al cliente	7			

Fuente: Elaboración propia.

Anexo 9. Interfaz de ServiceNow.

1 ← CHG0043077

2 ← New ✓ Assess ✓ Authorize ✓ Scheduled ✓ Implement ✓ Review ✓ Closed Canceled

3 ←

4 ←

Number: CHG0043077

Requested by: Gabriel Martinez

Configuration item: Security and safety systems

Change classification: Infra structure change

Business service: Deskside Support

Category: Hardware

Sites affected: Américas Torre Central-Bogota

Impacted programs:

Priority: Normal

Risk: Moderate

Impact: 3 - Low (< 20% users)

Reason for Change: Vendor Maintenance

Impact to PCI DSS 3.2:

Is Notification Required: No

Is Testing Required: Not Applicable

Opened by: Gabriel M

opened by time zone: America/Bogota

Time Zone for Change Communication: US/Eastern

Opened: 2021-05-31 16:43:24

Impact on Infosec: -- None --

Change model: Minor change

Type: Normal

State: Closed

Approval State: CAB approval

Outage:

Conflict status: Conflict

Conflict last run: 2021-06-14 12:26:45

Assignment group: IT Operations - TCB

Implementer: Hector J

Short description: Maintenance of security equipment in the data center on the 6th floor of Torre Calle 13

Description: I request your assistance to provide accompaniment to the maintenance of the data center security equipment, this would not affect the security of the data center, we will need two days from 08:00 to 17:00, please let us know which dates will work for you the best.

1. Fire detection and extinguishing system.

2. Aspiration detection

3. Intrusion system

4. Flooding system

Thanks

Post Implementation Review: Activity Completed

Figura 11. Recolección de información básica

Nota: La imagen corresponde al formulario generado para un control de cambios tecnológicos de la Organización XYZ, un formulario similar puede ser ajustado para el proceso de excepción de acceso

1. Identificador numérico
2. Muestra al usuario en qué fase del proceso está el requerimiento
3. Captura de información básica sobre el programa y la persona quien solicita, dando a conocer quién es la persona que estará a cargo del proceso
4. Descripción del requerimiento, en esta sección se puede incluir la justificación del negocio.

Fuente: Elaboración propia. Recuperado de Organización XYZ.

Planning	Schedule	Conflicts	Notes	Closure Information	CAB review
Justification	Preventive maintenance routine over the following security systems: 1. Fire detection and extinguishing system. 2. Aspiration detection 3. Intrusion system 4. Flooding system				
Implementation plan	Preventive maintenance routine over the following security systems: 1. Fire detection and extinguishing system. 2. Aspiration detection 3. Intrusion system 4. Flooding system				
Risk and impact analysis	No risk, the equipment to be verified: 1. Fire detection and extinguishing system. 2. Aspiration detection 3. Intrusion system 4. Flooding system				
Risk of not performing the change	the lack of maintenance can impact the functionalities of the security equipment				
Preimplementation Test Plan	Not Required				
Post implementation test plan	test all systems: 1. Fire detection and extinguishing system. 2. Aspiration detection 3. Intrusion system 4. Flooding system				
Backout plan	N/A				

Related Links
[Calculate Risk](#)
[Show SLA Timeline](#)
[Show Workflow](#)

Figura 12. *Justificación*

Nota: En esta sección se da a conocer la justificación y plan del cambio tecnológico, en el caso de estudio se puede modificar para que sea ajustado a la evaluación de riesgo generada por el gerente de seguridad de la información.

Fuente: Elaboración propia. Recuperado de Organización XYZ.

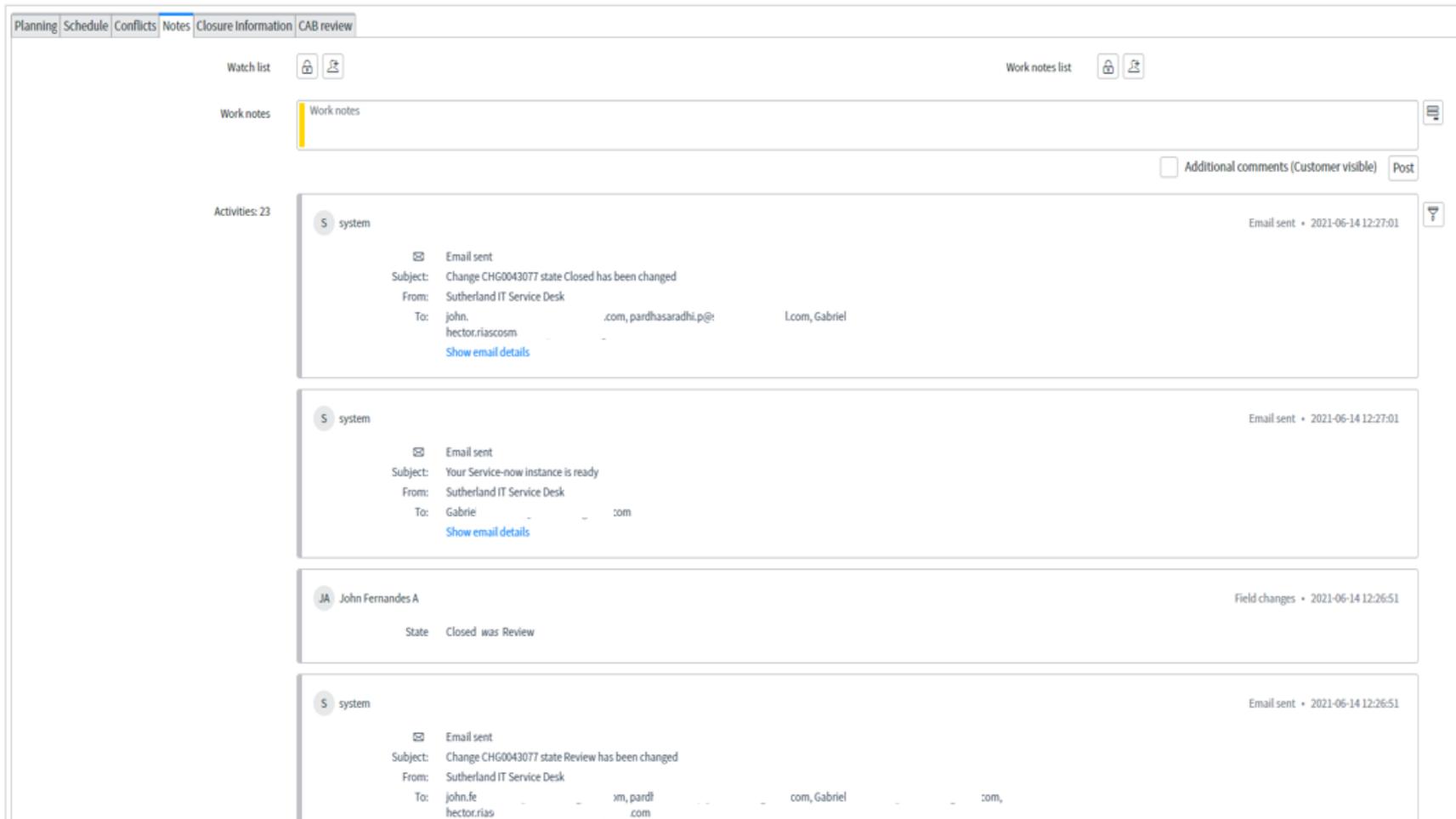


Figura 13. Interfaz para actualizar notas.

Nota: Esta sección permite al usuario que creo el requerimiento intercambiar información, al igual que al evaluador del riesgo, la información queda documentada y se puede evidenciar quien realizó el aporte, por otro lado, si se adjuntan documentos se puede ver quién y cuándo se agregó, con el fin de tener al máximo la documentación.

Elaboración propia. Recuperado de Organización XYZ.

State	Approver	Comments	Approving	Group
Approved	Jason Cont		Change Request: CHG0043077	(empty)
Approved	Rahu		Change Request: CHG0043077	GAPRV0048683
Approved	Pardh		Change Request: CHG0043077	GAPRV0048679
No Longer Required	Johr		Change Request: CHG0043077	GAPRV0048679
Approved	Dura	2021-06-02 11:59:18 - Durai Murugan (Com	Change Request: CHG0043077	(empty)
Approved	Ron		Change Request: CHG0043077	(empty)

Figura 14. Grupo de aprobadores.

Nota: Se muestra la lista de aprobadores requeridos para aprobar la implementación del cambio tecnológico, para el proceso de excepción de acceso se pueden listar los aprobadores, en base al programa y/o geografía a que corresponde el programa.

Elaboración propia. Recuperado de Organización XYZ.

	Number	Location	Approval	Assignment group	Assigned to	State	Opened by	Due date	Description	Resolve time	Resolved
<input type="checkbox"/>	INC1890947	Americas Torre Central-Bogota	Not Yet Requested	RIM_Suj	(empty)	On Hold		2021-03-16 11:41:40			(empty)
<input type="checkbox"/>	INC1891230	Americas Torre Central-Bogota	Not Yet Requested	RIM_Suj	(empty)	On Hold		2021-03-16 13:14:49			(empty)
<input type="checkbox"/>	INC1892564	Americas Torre Central-Bogota	Not Yet Requested	RIM_Suj	(empty)	On Hold		2021-03-17 07:04:14			(empty)
<input type="checkbox"/>	INC1900653	Americas Torre Central-Bogota	Not Yet Requested	Infosec	(empty)	In Progress		2021-03-20 13:48:56			(empty)
<input type="checkbox"/>	INC1909355	Americas Torre Central-Bogota	Not Yet Requested	IT Oper	Hector Javier RiascosMalaver	On Hold		2021-03-25 07:50:11			(empty)
<input type="checkbox"/>	INC1912299	Americas Torre Central-Bogota	Not Yet Requested	RIM_Suj	(empty)	On Hold		2021-03-26 11:38:39			(empty)
<input type="checkbox"/>	INC1912323	Americas Torre Central-Bogota	Not Yet Requested	RIM_Suj	(empty)	On Hold		2021-03-26 11:48:22			(empty)
<input type="checkbox"/>	INC1912329	Americas Torre Central-Bogota	Not Yet Requested	RIM_Suj	(empty)	On Hold		2021-03-26 11:51:04			(empty)
<input type="checkbox"/>	INC1918410	Americas Torre Central-Bogota	Not Yet Requested	Networ	(empty)	On Hold		2021-04-01 07:26:17			(empty)
<input type="checkbox"/>	INC1954607	Americas Torre Central-Bogota	Not Yet Requested	Infosec	(empty)	In Progress		2021-04-17 17:21:05			(empty)
<input type="checkbox"/>	INC1965291	Americas Torre Central-Bogota	Not Yet Requested	LMS Ad	(empty)	In Progress		2021-04-23 11:59:03			(empty)
<input type="checkbox"/>	INC2014503	Americas Torre Central-Bogota	Not Yet Requested	Global	(empty)	On Hold		2021-05-18 15:36:15			(empty)
<input type="checkbox"/>	INC2017379	Americas Torre Central-Bogota	Not Yet Requested	Infosec	(empty)	In Progress		2021-05-19 17:18:18			(empty)
<input type="checkbox"/>	INC2021673	Americas Torre Central-Bogota	Not Yet Requested	Networ	(empty)	In Progress		2021-05-21 12:08:26			(empty)
<input type="checkbox"/>	INC2024225	Americas Torre Central-Bogota	Not Yet Requested	IT Oper	(empty)	On Hold		2021-05-22 15:08:21			(empty)

Figura 15 Lista de requerimientos.

Nota: se muestra la lista de requerimientos, en nuestro caso de estudio cada requerimiento puede ser una excepción de acceso, la cual queda almacenada en la nube.

Elaboración propia. Recuperado de Organización XYZ.