ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE SISTEMAS

UNIDAD DE TITULACIÓN

Herramienta para la evaluación del nivel de confianza de los miembros postulantes de una organización virtual basada en la ISO 27001.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN SOFTWARE

JAVIER EDUARDO CAGUANA POZO
Javier.caguana@epn.edu.ec

Director: Msc. Cindy Pamela López
cindy.lopez@epn.edu.ec

Codirector: Dr. Marco Oswaldo Santorum Gaibor
Marco.santorum@epn.edu.ec

2021

APROBACIÓN DEL DIRECTOR

Como director del trabajo de titulación “Herramienta para la evaluación del nivel de confianza de los miembros postulantes de una organización virtual basada en la ISO 27001.” desarrollado por Javier Eduardo Caguana Pozo, estudiante de la Maestría en Software mención Seguridad, habiendo supervisado la realización de este trabajo y realizado las correcciones correspondientes, doy por aprobada la redacción final del documento escrito para que prosiga con los trámites correspondientes a la sustentación de la Defensa oral.

Msc. Cindy López

DIRECTOR

APROBACIÓN DEL CODIRECTOR

Como codirector del trabajo de titulación “Herramienta para la evaluación del nivel de confianza de los miembros postulantes de una organización virtual basada en la ISO 27001.” desarrollado por Javier Eduardo Caguana Pozo, estudiante de la Maestría en Software mención Seguridad, habiendo supervisado la realización de este trabajo y realizado las correcciones correspondientes, doy por aprobada la redacción final del documento escrito para que prosiga con los trámites correspondientes a la sustentación de la Defensa oral.

Dr. Marco Santorum

CODIRECTOR

DECLARACIÓN DE AUTORÍA

Yo, Javier Eduardo Caguana Pozo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Javier Eduardo Caguana Pozo

DEDICATORIA

Dedico este logro a mi familia, aquellos que siempre han estado apoyándome en cada paso, aquellos que, con una llamada, una visita, o simplemente un mensaje han estado al tanto de mi progreso y me han incentivado a alcanzar mis objetivos, a todos ellos dedico el presente trabajo y a futuro los logros que vendrán.

AGRADECIMIENTO

Agradezco a mi familia, compañeros y maestros, que han formado parte de este ciclo, a mi familia por su apoyo incondicional, a mis compañeros por su calidad y amistad y apoyo en los momentos difíciles, a los maestros que me han guiado en el proceso y han dedicado su tiempo y esfuerzo a transmitir sus conocimientos para que los podamos asimilar y crecer profesional y personalmente. A la Escuela Politécnica Nacional que me abrió sus puertas para poder alcanzar este objetivo. A todos muchas gracias.

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

Las organizaciones virtuales son formas de organización basadas en las nuevas tecnologías, si bien el concepto no es nuevo, sí lo son las formas de interacción entre los miembros que pueden formar parte de una organización virtual y por lo tanto los riesgos asociados con la formación y operación de estas han evolucionado.

El presente trabajo pretende dar una alternativa a uno de los problemas recurrentes de gran relevancia a la hora de formar organizaciones virtuales, como es la selección de miembros y más específicamente la confianza que se puede depositar en un miembro aspirante a formar parte de una organización virtual. Lo cual se abordará desde varias perspectivas, que permitirán determinar qué criterios son más relevantes o de mayor prioridad a la hora de formar organizaciones virtuales. Esta selección se realizará empatando estos criterios con la norma ISO 27001, la misma que nos provee lineamientos y controles para asegurar la protección de los activos de información desde diversos puntos de vista. En conclusión, tanto los criterios de diversas fuentes consultadas, como los controles proporcionados por la norma ISO 27001, nos permiten elaborar una lista de sentencias que deben ser evaluadas en los socios postulantes. Finalmente, se aplican algoritmos que permitan obtener una calificación que servirá como medición del nivel de confianza en cada postulante, y como punto de partida para analizar la posible inclusión o no del postulante en la organización virtual que se está formando.

Palabras clave: Organización virtual, ISO 27001, Seguridad, Criterios de selección, Selección de socios

ABSTRACT

Virtual organizations represent modern forms of organizing based on new technologies. Even though the concept is not new, how potential members of a virtual organization interact with each other and the risks associated with the formation and operation of these organizations have evolved.

The present work intends to give alternative solutions to the recurrent challenge of selecting the members, to be more specific, to maximize the outcome of the trust invested in a certain member aspirating to be part of the organization. Which will consider various perspectives that will allow the determination of what criteria is more relevant or highly prioritized when the organization is being formed. The selection process will take place following the ISO 27001 regulations, the same framework that provides guidelines and controls to assure the protection of the active information from diverse points of view.

In conclusion, the criteria consulted with diverse sources altogether with the controls (ISO 27001) allow us to elaborate a checklist that evaluates the applicants. At last, algorithms will be applied which lead to obtaining qualifications that will serve as a reliability measurement for each candidate and as a milestone to analyze the possible acceptance of an applicant in the virtual organization which is in the formation process.

Keywords: Virtual Organization, ISO 27001, Security, Selection criteria, Partner selection

1. INTRODUCCIÓN

Actualmente la rapidez con la que se genera y transporta información, da origen a la necesidad de las organizaciones de moverse al mismo ritmo y adaptarse a nuevos modelos o demandas de los clientes. Una forma de solventar esta necesidad se conoce como Organizaciones Virtuales (OVs), según [1], una organización virtual es una coalición dinámica de recursos y usuarios geográficamente distribuidos, que se agrupan con la finalidad de alcanzar un objetivo común. Las organizaciones virtuales generalmente terminan cuando los objetivos se han alcanzado.

No obstante, esta versatilidad con la que cuentan las OVs, trae consigo algunos inconvenientes y desafíos, entre ellos uno muy importante, la seguridad. Según [2], el principal problema en las organizaciones virtuales es la seguridad, lo que también incluye la etapa de identificación de aliados óptimos. Es ahí donde se plantea la inclusión de una herramienta que permita tener una alternativa en lo referente a la selección de aliados, basados en estándares de seguridad y criterios de diversas fuentes referentes al tema de seguridad.

La información es una activo muy importante y en muchas organizaciones es la base de su modelo de negocio, por tanto, un manejo adecuado de la información compartida y generada durante el ciclo de vida de una organización virtual es de suma importancia.

Varios trabajos tratan sobre la relevancia de la seguridad y las brechas generadas en el ámbito de la industria 4.0 [3][4][5], mismo que se relacionan también con el contexto de las OVs, y cada día el número de posibles ataques crece.

Sin embargo, hoy en día existen organizaciones que por desconocimiento o falta de entendimiento acerca de los riesgos que existen pueden hacer un mal uso de la información [6], estas organizaciones pueden ser un grave problema para las OVs, ya que la seguridad de la OV dependerá de su eslabón más débil, y estas brechas pueden comprometer la información de todos los miembros participantes.

Varios estudios sobre confianza y seguridad en organizaciones virtuales [7][8][9] apuntan generalmente a la reputación o reconocimiento de marca que tengan las organizaciones virtuales en el entorno en que se mueven. Sin embargo, para organizaciones nuevas o con muy reducida trayectoria se hace imposible generar estos datos, con lo cual se requiere una herramienta de evaluación que permita determinar los niveles de seguridad implementados y la confianza que se pude depositar aun sin tener un histórico o una reputación previa como punto de partida. Según [10], la confianza de las sociedades de la información puede basarse en cálculos, información y datos que se tenga sobre cada socio, transitividad o puede basarse en el sistema social y las relacione creadas, La herramienta propuesta aborda el campo de los cálculos, permitiendo también el uso de información previa de cada socio o posible socio.

La ISO 27001 provee los controles y criterios para evaluar la seguridad de una organización[11], estos controles se van a contrastar con criterios de diferentes fuentes para determinar cuáles son los principales controles a evaluar a un socio postulante, y entre los seleccionados determinar los más relevantes o los que influyen más en la percepción y necesidades de seguridad de un miembro postulante a una OV, cada uno de estos criterios será evaluado mediante afirmaciones que tendrán una escala de cumplimiento, esto permitirá obtener mediante una serie de cálculos un valor que representa el nivel de implementación de medidas de seguridad de un postulante o en otras palabras la confianza o el grado de confianza con que se puede compartir información con un determinado postulante o miembro de la OV.

1.1. Objetivo general

Elaborar una herramienta que permita evaluar el nivel de implementación de medidas de seguridad, nivel de confianza y reputación de un posible socio en una OV con base en la ISO 2700.

1.2. Objetivos específicos

- Diseñar una herramienta de evaluación que permita emitir una valoración general en base a la evaluación de los criterios tomados en cuenta y la reputación de cada organización.
- Establecer los criterios más relevantes a ser evaluados en un posible socio de una organización virtual en base a las recomendaciones de la ISO 27001.
- Establecer una lista de verificación y un rango de evaluación de los criterios a tomar en cuenta.

1.3. Hipótesis o Alcance

Una herramienta de evaluación basada en la ISO 27001 permite valorar el nivel de implementación de prácticas de seguridad en las organizaciones postulantes a formar una OV como apoyo a la toma de decisiones en el proceso de selección inteligente de socios.

1.4. Marco Teórico

Organización Virtual:

Cuando se habla de una organización virtual se hace referencia a un equipo temporal de empresas o entidades [12], se puede decir también que consiste en un grupo de actores o instituciones definido en base a un conjunto de reglas acerca de compartición de recursos[13], con el propósito de alcanzar una meta o un objetivo en común. Por ejemplo, un producto o servicio que se desea ofrecer al consumidor[14]. Las organizaciones virtuales permiten la integración de varias organizaciones para usar sus habilidades o activos de importancia con el fin de alcanzar el o los objetivos[15].

Características:

Si bien los conceptos pueden variar de un autor a otro debido a la alta dinámica de las Organizaciones Virtuales, hay ciertas características que se pueden tomar como generales: [14].

Desmaterialización: El propio termino virtual da a entender un proceso de desmaterialización de las operaciones.

Deslocalización: Las organizaciones virtuales son potencialmente independientes del espacio y la localización.
Asíncrono: Libertad de cada entidad para organizar su tiempo y actividades diarias.
Atomización interactiva: Implica asignar a cada tarea un proveedor o socio que pueda realizarlo cumpliendo los estándares.
Temporal: Las organizaciones virtuales tienen un ciclo de vida lo cual las convierte en asociaciones temporales.
No institucionalización: Renunciando a un espacio físico o un centro de operaciones muchos aspectos tradicionales pasan a ser virtuales incluidos muchos costos de institucionalización.
Individualización: La idea es de la individualización es ofrecer producción en masa que se adapte a las nuevas necesidades y demandas de los clientes. [14].

Ciclo de vida:

Como se mencionó previamente las organizaciones virtuales cumplen con un ciclo de vida, este ciclo de vida desde diferentes perspectivas puede tener más o menos pasos en función de cómo se agrupen las actividades a realizar en cada uno de ellos. [16] divide el ciclo de vida en 5 fases que son:

Preparación para la participación en la organización virtual:

Es una fase preliminar de la organización virtual y consiste en la publicación de los recursos con los que cuenta cada posible socio, esto servirá para evaluar la posible participación de cada miembro

Identificación:

Esta fase es una de las principales en el ciclo de vida y es en la cual se identifica el objetivo de la conformación de la organización virtual, y se establecen las metas que cada integrante deberá cumplir para alcanzar el objetivo final.

Formación:

El iniciador o quien esté a cargo de la conformación de la organización virtual consulta los repositorios o la información de los postulantes que entregaron su información en la fase de preparación, Con esa información se selecciona un set de potenciales miembros que cumplan con los requisitos establecidos, luego se

envía a estos participantes una invitación para participar donde se establece los requerimientos que deben cumplir, si es aceptada la invitación estos miembros pasan a ser parte de la organización virtual.

Operación:

Una vez conformada la organización virtual, los miembros inician su cooperación de acuerdo a los requerimientos y contratos establecidos, esta fase conlleva asuntos de seguridad critica, en esta etapa los miembros seleccionados ya cuentan con acceso a información proveniente de los demás y pueden acceder a información sensible tanto de otros miembros como del proyecto que se lleva a cabo, existe la posibilidad de que uno o varios miembros no puedan o no quieran cumplir con los requerimientos contractuales, estos miembros son penalizados de acuerdo a la gravedad del incumplimiento.

Disolución:

Esta fase tiene lugar cuando los objetivos de la organización virtual han sido alcanzados, la estructura se disuelve y se finaliza cualquier contrato entre los miembros participantes.

Seguridad y Confianza.

Uno de los principales problemas de las organizaciones virtuales es la seguridad, que incluye desde la identificación de un usuario hasta como evaluar las acciones que puede realizar [2]. Debido a la gran cantidad de información que se transmite a través de los miembros de una Organización virtual, es importante poder confiar en ellos para depositar esta información.

La confianza es vista como un punto importante en la formación de organizaciones virtuales [17].

Según [10], la confianza en las sociedades de la información se puede tener de 4 formas:

Confianza basada en cálculos: Es la forma más común de confianza que generalmente se da al inicio de una relación de negocios. Este tipo de confianza requiere cálculos y aproximaciones basadas en las expectativas y posibles riesgos, todo dentro de un marco contractual.

Confianza basada en información: Esta forma de confianza se desarrolla en base a la relación entre empresas, con el tiempo cada empresa recopila información para poder predecir el comportamiento de la otra y en base a esa información establecer su nivel de confianza.

Confianza basada en transitividad o confianza transferible: En este caso se trata de añadir una tercera parte que juzgue la confianza en un determinado ente y transferir esa confianza a la relación entre entidades.

Confianza a través de un sistema social: Esta forma de confianza se basa en las interacciones dentro de un medio social, o lo que es lo mismo la aprobación de la sociedad genera la confianza en una determinada entidad.

Debido a que de inicio es muy complejo abordar los otros tipos de confianza la investigación se enfoca en la confianza basada en cálculos que es la que en primer lugar se puede generar sin un conocimiento previo ni un historial de los miembros postulantes de una Organización Virtual.

Estándares de Seguridad:

Aunque en un inicio los estándares de seguridad eran generalmente propios de cada nación, con el paso del tiempo fueron saliendo al panorama internacional ciertas metodología y estándares que se difundieron gracias a su aceptación.

Basados en 3 estándares nacionales que fueron el TCSEC (Trusted Computer System Evaluation Criteria), ITSEC (Information Technology Security Evaluation Criteria) y el CTCPEC (Canadian Trusted Computer Product Evaluation Criteria), en 1996 se codifica un estándar considerado internacional llamado ISO/IEC 15408. Posteriormente se conocería como “Comon Criteria”. Estándar que es aceptado alrededor del mundo.

Se puede mencionar otras metodologías que si bien son internacionales no se consideran estándares como por ejemplo ITIL (IT Infrastructure Library), que es una metodología aceptada internacionalmente, y liberada como estándar bajo el nombre de BS15000 y conocida actualmente como ISO 20000.

Pese a esto en el campo de la seguridad hoy en día se recomienda el uso de la ISO 27000. [18].

ISO 27000 es uno de los estándares más importantes a nivel de empresas en el mundo. Es un estándar que proporciona guías para la seguridad de la información abordando tanto prácticas de seguridad como físicas y procedimientos, que particularmente se incluyen en la ISO 27001 y 27002.

La ISO 27001 provee un modelo para establecer, implementar, operar, monitorear, revisar y mejorar un sistema de gestión de seguridad de la información. El estándar agrupa los requerimientos de seguridad de la información en Dominios, Objetivos de control y controles [19].

La ISO 27002 contiene un código de prácticas para la seguridad de la información e introduce cientos de controles a implementar.

Haciendo énfasis en la ISO 27001 como parte de la familia ISO 27K o ISO 27000 Se puede mencionar que provee tanto una guía para certificación como un marco de trabajo para garantizar seguridad de la información. Dependiendo de las necesidades de la empresa en específico, provee controles los cuales deben ser implementados de igual manera en función de la realidad y necesidad de la empresa que implementa los mismos.

Figura 1 Ciclo PDCA de un SGSI [20]

Priorización de controles:

La priorización de controles pasa por varias etapas, dependiendo de cada organización estas etapas pueden ser:

La priorización de activos y amenazas: dentro de la priorización de activos y amenazas cada organización debe ser capaz de identificar sus activos y los objetivos de negocio, estos activos deben ser evaluados para identificar su valor para la organización y posteriormente se debe enlazar estos activos con los objetivos de la organización a fin de determinar el impacto real que podría suponer la pérdida o daño de cada activo.

Posteriormente se deberá realizar una priorización de amenazas y riesgos, para lo cual se debe identificar las posibles amenazas y eventos de riesgo, posteriormente identificar que tan vulnerable se encuentra la organización frente a estas amenazas, determinar la probabilidad de ocurrencia y el impacto que ocasionaría la ocurrencia de cada evento. Finalmente determinar el riego, esto puede ayudar considerablemente a las organizaciones a buscar soluciones de seguridad.

Una vez determinado el riesgo y valorados los activos de la organización se puede priorizar los controles de seguridad en función del impacto y las necesidades de la organización basada en la documentación obtenida previamente.[21]

En el caso de organizaciones virtuales al ser una agrupación heterogénea de distintas organizaciones este proceso conllevaría tanto tiempo como recursos que no son objeto del modelo de organizaciones virtuales. En este caso la opinión de diversos autores puede ser una opción para llevar a cabo la priorización de los controles, en base a los criterios que distintos autores consideren relevantes en un entorno distribuido como lo son las organizaciones virtuales.

Si bien existe varios documentos que hacen referencia a entornos distribuidos y organizaciones virtuales con base en las recomendaciones del Comon Criteria [22][23], también existe documentación acerca del uso de la ISO 17799 [24], sin embargo las investigaciones que relacione la ISO 27000 con entornos distribuidos es muy escaso y prácticamente nulo en el caso específico de organizaciones virtuales.

En conclusión, las organizaciones virtuales pretenden facilitar la producción de bienes de consumo o servicios, sin embargo, su principal fortaleza la cual se relaciona con su capacidad de distribuir el trabajo y la información a distintos agentes también genera una de sus principales amenazas que es la confianza en estos agentes y la seguridad de la información que se comparte. Siendo necesario que se tome en cuenta los niveles de seguridad de cada miembro que va a formar la organización virtual a fin de garantizar los niveles de seguridad de la organización virtual en su conjunto.

2. METODOLOGÍA

Para el desarrollo del proyecto en primer lugar, se adopta un método explorativo documental, que utilice como fuente principal la Norma ISO 27001 y bibliografía enfocada en las necesidades de una OV. En este contexto, de inicio se realiza una evaluación de los requerimientos de la norma, dentro de lo cual:

Se realiza un estudio de los criterios presentados en la ISO 27001 para determinar cuáles son los más relevantes para seleccionar a los integrantes de una organización virtual, de acuerdo con el análisis que se realiza de las necesidades de una OV y entornos distribuidos para determinar esta importancia.

El análisis se realiza tomando en cuenta los controles que se encuentran en la ISO 27001, de los cuales se extrae los que sean considerados de mayor relevancia en la etapa previa.

Una vez concluido el proceso explorativo documental los pasos siguientes se desarrollan primando las necesidades de la investigación particulares del proyecto por lo tanto se realiza una comparativa de los criterios seleccionados con los requerimientos en el área de las OVs.

Para el desarrollo de la herramienta se hace uso de los criterios escogidos los cuales una vez seleccionados se adaptan a un sistema de evaluación, para el cual se propone un rango de evaluación de cada criterio, este rango de evaluación es una escala numérica cuyos valores son determinados en el desarrollo del proyecto. Los criterios seleccionados de ser el caso se agrupan para formar uno solo o se establecerá criterios individuales, en función de la relevancia del criterio seleccionado.

Posteriormente se verifica la importancia de cada criterio para lograr un nivel de confianza de la OV. Además, se establece también un algoritmo que calcule el peso relativo de la reputación de cada ente.

Se toma en cuenta el nivel de importancia de cada criterio seleccionado, a fin de desarrollar un modelo de evaluación que emita una valoración final basada tanto en los criterios antes presentados como en la reputación del ente evaluado.

Una vez evaluado se presenta el resultado de la evaluación como un valor de nivel numérico, que permita saber en conjunto el nivel de implementación de prácticas de seguridad que posee la organización evaluada, lo que se traducirá en el nivel de confianza que se puede depositar en dicha organización para compartir información.

En lo referente a implementación se toma un modelo ficticio de OV, a fin de extraer las características propias del sistema y determinar la validez tanto de los criterios seleccionados como de su importancia en el entorno distribuido de la OV.

Finalmente, se probará la herramienta aplicando diferentes entradas para determinar la validez de la evaluación realizada por la herramienta.

Al final se obtiene una herramienta que consiste en una lista de verificación con los criterios seleccionados, cada uno se podrá evaluar en una escala determinada y tendrá un peso relativo en la valoración final, además se crea el algoritmo que permita en base a dichas entradas calcular una valoración a modo de evaluación que ayude a determinar el nivel de confianza basado en el nivel de implementación de controles de seguridad de los postulantes a conformar una organización virtual, este resultado será un valor único en una escala determinada lo que facilitará su interpretación.

2.1. Revisión bibliográfica de criterios

Se realizó una exploración documental y bibliográfica, en la cual se priorizó la búsqueda de fuentes que permitan determinar los aspectos de seguridad de la información más relevantes considerados por los autores a la hora de conformar una organización virtual o en entornos distribuidos en general. Luego de la recopilación de información para lograr una mejor comprensión de los resultados obtenidos, se tabuló la información en la Tabla 1 de resumen donde se ubican de

manera horizontal los criterios o características descritos por cada autor y de manera vertical los autores de los cuales se recopilo la información, al final se realiza la sumatoria para determinar qué criterios o características aparecen o son tomados en cuenta con mayor frecuencia en entornos distribuidos y más específicamente en organizaciones virtuales.

Tabla 1- Selección de criterios por autor

	Calidad	Tiempo	Costos de insumos	Fiabilidad	Puntualidad	Autenticación	Permisos (control)de acceso	Integridad del contenido	Privacidad	Encripción	Comunicación	Protección de datos	Utilización de recursos	Canales seguros	Auditoria	Operación segura	Seguridad física	Seguridad de red	Sistema operativo	Aplicaciones	Limitar exposición	Detección de intrusos	Restauración	Políticas
A[25]	x	x	x	x	x																			
B[26]	x			x		x	x	x	x	x														
C[27]						x																		
D[28]																								
E[29]						x				x														
F[22]						x			x	x	x	x	x	x	x									
G[30]						x	x			x					x	x	x	x	x	x				
H[23]					x	x	x		x					x							x	x	x	
I[31]						x			x	x	x	x	x	x	x						x		x	
J[32]						x	x																	x
K[33]																								x
L[34]						x	x		x															
M[35]						x	x																	
N[36]						x				x				x										

Valoración de criterios.

Como se puede observar hay una marcada inclinación por ciertos criterios de seguridad, estos se consideran de relevancia con mayor frecuencia dentro de lo que se refiere a entornos distribuidos.

En la Tabla 2 se observa los resultados de la contabilización de las coincidencias respecto a cada criterio por los distintos autores, en este punto se observa claramente ciertos criterios que se tienen en cuenta con mayor frecuencia a la hora de buscar seguridad.

Tabla 2- Contabilización de resultados obtenidos para cada criterio.

CONTEO DE CRITERIOS SEGÚN DIVERSOS AUTORES.					
Calidad	2	Privacidad	4	Seguridad física	1
Tiempo	1	Encripción	7	Seguridad de red	1
Costos	1	Comunicación	2	Sistema operativo	1
Fiabilidad	2	Protección de datos	2	Aplicaciones	1
Puntualidad	1	Utilización de recursos	2	Limitar exposición	2
Autenticación	11	Canales seguros	3	Detección de intrusos	1
Control de acceso	6	Auditoria	4	Restauración	2
Integridad	2	Operación segura	1	Políticas	2

Mapeo respecto a la ISO 27001

Con los datos recopilados y resumidos en las tablas anteriores se puede realizar un mapeo respecto de los criterios que presenta la ISO 27001 lo que permitirá realizar una selección de los criterios más relevantes a la hora de formar una organización virtual.

En la Tabla 3 se puede evidenciar este mapeo, cabe recalcar que solo se incluyeron los dominios que tenían por lo menos una concordancia con los criterios encontrados. Hay criterios que debido a su naturaleza pueden ser tomados en cuenta o son válidos para más de un dominio.

Tabla 3- Mapeo de criterios vs dominios de la ISO 27K

	Calidad	Tiempo	Costos de insumos	Fiabilidad	Puntualidad	Autenticación	Permisos (control)de acceso	Integridad del contenido	Privacidad	Encripción	Comunicación	Protección de datos	Utilización de recursos	Canales seguros	Auditoria	Operación segura	Seguridad física	Seguridad de red	Sistema operativo	Aplicaciones	Limitar exposición	Detección de intrusos	Restauración	Políticas
Políticas de seguridad de la información																								x
Gestión de activos								x				x	x								x			
Control de acceso						x	x		x												x			
Cifrado									x	x														
Seguridad física y del ambiente																	x							
Seguridad en la operativa																x			x	x			x	
Seguridad en las telecomunicaciones											x			x				x			x	x		
Adquisición desarrollo y mantenimiento de los sistemas de información																			x	x				
Relaciones con proveedores																					x			
Gestión de Incidentes en la seguridad de la información															x							x		
Aspectos de seguridad de la información en la gestión de la continuidad del negocio															x									
Cumplimiento.				x					x															

Luego de realizado el mapeo se procede a empatar los datos de la Tabla 2 con lo tabulado en la Tabla 3 para obtener los valores definitivos de relevancia de los criterios de la norma ISO 27001 que serán analizados e incluidos en la herramienta. Los resultados se pueden observar en la Tabla 4 para cada dominio de la ISO 27001 que tuvo por lo menos una coincidencia.

Tabla 4- Valoración general de los dominios de la ISO 27K con respecto a los criterios de diversos autores.

Valoración general	
DOMINIOS	**VALORACIÓN**
Políticas de seguridad de la información	2
Gestión de activos	8
Control de acceso	23
Cifrado	11
Seguridad física y del ambiente	1
Seguridad en la operativa	5
Seguridad en las telecomunicaciones	9
Adquisición desarrollo y mantenimiento de los sistemas de información	2
Relaciones con proveedores	2
Gestión de Incidentes en la seguridad de la información	5
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	4
Cumplimiento.	6

2.2. Selección de criterios

Dominios

Luego de analizar la Tabla 4 es claro que el dominio de mayor peso en la investigación será el control de acceso dentro del cual se tienen 4 objetivos de control y 14 controles. Para el caso del trabajo desarrollado se toma en cuenta una valoración mayor o igual a 8 puntos para incluir los dominios en la herramienta. Esta selección se hace ponderando un peso porcentual igual o mayor al 10 % en relación con los demás dominios, un peso porcentual menor al 10 % se supone no relevante tanto para el presente estudio como para la comunidad. Este análisis previo también sirve de punto de partida para establecer un peso relativo de cada uno de los aspectos que será objeto de evaluación con la herramienta.

En general se usan diversos métodos de priorización que generalmente se basan en decisiones subjetivas de un individuo o un grupo pequeño de individuos relacionado con la organización, en el presente trabajo se propone una priorización basada en criterios de varios autores donde se toma en cuenta la recurrencia y

atención de cada criterio para posteriormente ser empatado con los controles de la ISO 27001 dejando de lado el sesgo que pueda ocasionar la priorización basado en el criterio de un solo autor.[37]

A continuación, se realiza la revisión a detalle de los 4 dominios seleccionados mediante la valoración individual. Los cuatro dominios seleccionados son:

- Gestión de activos.
- Control de acceso
- Cifrado
- Seguridad en las telecomunicaciones.

Cada uno de los cuales es desglosado en el Anexo 1 de la ISO27001: 2013 en uno o más objetivos de control dentro de los cuales existen varios controles que se pueden implementar. [38]

Desglose de dominios.

La Tabla 5 muestra cada uno de los dominios seleccionados con sus respectivos objetivos de control y controles, para los cuales se realizarán las afirmaciones que permitan evaluar su cumplimiento.

Tabla 5- Desglose de dominios seleccionados

Dominios seleccionados, objetivos de control y controles.	
GESTIÓN DE ACTIVOS.	**CONTROL DE ACCESO.**
1 Responsabilidad sobre los activos. 1.1 Inventario de activos. 1.2 Propiedad de los activos. 1.3 Uso aceptable de los activos. 1.4 Devolución de activos. **2 Clasificación de la información.** 2.1 Directrices de clasificación. 2.2 Etiquetado y manipulado de la información. 2.3 Manipulación de activos. **3 Manejo de los soportes de almacenamiento.** 3.1 Gestión de soportes extraíbles. 3.2 Eliminación de soportes.	**1 Requisitos de negocio para el control de accesos.** 1.1 Política de control de accesos. 1.2 Control de acceso a las redes y servicios asociados. **2 Gestión de acceso de usuario**. 2.1 Gestión de altas/bajas en el registro de usuarios. 2.2 Gestión de los derechos de acceso asignados a usuarios. 2.3 Gestión de los derechos de acceso con privilegios especiales. 2.4 Gestión de información confidencial de autenticación de usuarios.

3.3 Soportes físicos en tránsito.	2.5 Revisión de los derechos de acceso de los usuarios. 2.6 Retirada o adaptación de los derechos de acceso **3 Responsabilidades del usuario.** 3.1 Uso de información confidencial para la autenticación. **4 Control de acceso a sistemas y aplicaciones.** 4.1 Restricción del acceso a la información. 4.2 Procedimientos seguros de inicio de sesión. 4.3 Gestión de contraseñas de usuario. 4.4 Uso de herramientas de administración de sistemas. 4.5 Control de acceso al código fuente de los programas.
CIFRADO.	**SEGURIDAD EN LAS TELECOMUNICACIONES.**
1 Controles criptográficos. 1.1 Política de uso de los controles criptográficos. 1.2 Gestión de claves.	**1 Gestión de la seguridad en las redes.** 1.1 Controles de red. 1.2 Mecanismos de seguridad asociados a servicios en red. 1.3 Segregación de redes. **2 Intercambio de información con partes externas.** 2.1 Políticas y procedimientos de intercambio de información. 2.2 Acuerdos de intercambio. 2.3 Mensajería electrónica. 2.4 Acuerdos de confidencialidad y secreto.

2.3. Check list.

Cada uno de los controles debe ser evaluado, para lo cual se elabora un check list con una o más afirmaciones derivadas de cada control, las mismas que permitan medir el cumplimiento del control. E l número y tipo de afirmaciones se establecen tomando en cuenta que permitan evaluar el control seleccionado. A continuación, se establecen las afirmaciones a ser evaluadas para cada control de la Tabla 5.

Se describe una tabla para cada conjunto de afirmaciones correspondiente a cada uno de los dominios seleccionados.

La Tabla 6 Muestra las afirmaciones a ser evaluadas en cada uno de los controles de la Gestión de activos de la ISO 27K.

Tabla 6- Afirmaciones Evaluación de Gestión de Activos

GESTIÓN DE ACTIVOS.
1 Responsabilidad sobre los activos.
1.1 Inventario de activos.
• *Existe un inventario de activos de la información.*
• *El inventario es lo suficientemente completo, preciso, detallado y se mantiene actualizado correctamente.*
1.2 Propiedad de los activos.
• *Los activos de información tienen un propietario y un responsable técnico*
• *Existe un sistema de asignación, etiquetado e información de incidentes para los activos de información.*
1.3 Uso aceptable de los activos.
• *Existe una política que norma el uso apropiado de recursos tecnológicos como correo electrónico, mensajería, FTP, incluyendo el comportamiento del usuario en internet y redes sociales, y que además establece responsabilidades por parte del usuario.*
• *Se ha socializado correctamente lo que constituye un uso inapropiado de activos a todos los miembros de la empresa.*
1.4 Devolución de activos.
• *Existe un procedimiento para recuperación de activos de información tras una baja o despido que garantiza el correcto tratamiento de estos.*
• *Existe un procedimiento a seguir para abordar el caso de activos de información que no han sido devueltos.*
2 Clasificación de la información.
2.1 Directrices de clasificación.

• *Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados a la clasificación de la información. Y estas se ligan a obligaciones contractuales o legales.*
• *La clasificación se basa en los requisitos de seguridad de la información (confidencialidad, integridad, disponibilidad), y el personal está consciente de ellos.*
2.2 Etiquetado y manipulado de la información.
• *Existe un proceso de etiquetado de la información tanto física como electrónica, sincronizado con las políticas de clasificación de la información que garantiza una correcta manipulación de la información.*
• *Existen niveles de clasificación y se garantiza el acceso únicamente a aquellos con permisos de acceso aprobados.*
2.3 Manipulación de activos.
• *Para la manipulación de activos se tiene en consideración: Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios físicos y electrónicos, divulgación, intercambio, intercambio con terceros, traslado, etc.*
3 Manejo de los soportes de almacenamiento.
3.1 Gestión de soportes extraíbles.
• *Existe un registro detallado de medios extraíbles como CD/DVD, almacenamiento USB y demás medios extraíbles.*
• *Los medios extraíbles están correctamente etiquetados, manejados y almacenados garantizando que no exista acceso no autorizado a la información almacenada.*
3.2 Eliminación de soportes.
• *Existe una política orientada a la eliminación de activos de información ligada a obligaciones legales y contractuales de los responsables, que permita además realizar un seguimiento del proceso de eliminación.*
• *Se tiene en cuenta la criticidad de la información para el proceso de eliminación: Respaldo de información, periodos de retención y eliminación segura (borrado criptográfico, desmagnetización, destrucción física),*

3.3 Soportes físicos en tránsito.
• *Se utiliza servicios de transporte confiables y mecanismos adecuados de cifrado para las transferencias de información.*
• *Se verifica la recepción en el lugar de destino de la información.*

La Tabla 7 contiene las afirmaciones a ser evaluadas en cada uno de los controles de Control de acceso.

Tabla 7- Afirmaciones evaluación de Control de acceso.

CONTROL DE ACCESOS.
1 Requisitos de negocio para el control de accesos.
1.1 Política de control de accesos.
• *Existe una política de control de acceso que contempla una asignación adecuada de deberes y un proceso documentado de control de acceso.*
• *El proceso de aprobación de acceso requiere la participación del propietario del sistema o de la información.*
1.2 Control de acceso a las redes y servicios asociados.
• *El acceso VPN e inalámbrico esta correctamente supervisado, controlado y autorizado.*
• *Se utiliza una autenticación multi factor para acceso a redes sistemas y aplicaciones críticas.*
• *Existe un proceso de monitoreo y pruebas constante para detectar accesos no autorizados, tiempos de respuesta a incidentes, entre otros.*
2 Gestión de acceso de usuario.
2.1 Gestión de altas/bajas en el registro de usuarios.
• *El alta de un usuario por solicitud pasa por un proceso adecuado de aprobación y registro, y genera un ID único para cada usuario.*
• *Existe un proceso para la baja de los ID de usuario de forma inmediata tras el cese o despido o si ya no son necesarios previa confirmación.*
2.2 Gestión de los derechos de acceso asignados a usuarios.

• *Cada acceso a sistemas está basado en las necesidades del negocio y se corresponde con las políticas de control de acceso y segregación de funciones.*
• *Se documenta adecuadamente las solicitudes y aprobaciones de acceso.*
2.3 Gestión de los derechos de acceso con privilegios especiales.
• *Existe un proceso periódico de revisión de cuentas con privilegios especiales que contemple, asignación y eliminación de privilegios en base a necesidades.*
• *Existe una diferenciación de usuarios con privilegios especiales, tanto en ID, caducidad de cuentas y controles más estrictos de actividades.*
2.4 Gestión de información confidencial de autenticación de usuarios.
• *Hay restricciones técnicas como: longitud mínima de contraseña, reglas de complejidad, cambio forzado de contraseña, autenticación en múltiples factores, etc.*
• *El utiliza cifrado en almacenamiento y manipulación de contraseñas en dispositivos, sistemas y aplicaciones.*
• *Se verifica la identidad del usuario antes de proporcionar contraseña temporal nueva y esta contraseña es suficientemente fuerte.*
2.5 Revisión de los derechos de acceso de los usuarios.
• *Se revisa periódicamente los derechos de acceso de los usuarios y se lleva un registro documental de las revisiones.*
• *Las revisiones se realizan en presencia de los propietarios para verificar cambios en las funcionas para los usuarios.*
2.6 Retirada o adaptación de los derechos de acceso
• *Existe un proceso estructurado de reasignación o eliminación de derechos de acceso en el cual se contempla el acceso tanto físico como lógico a los sistemas.*
• *Las contraseñas se eliminan o cambian inmediatamente en caso de finalización de contrato, cambio de rol etc.*
3 Responsabilidades del usuario.
3.1 Uso de información confidencial para la autenticación.

• *Existe medidas que aseguran la confidencialidad de las credenciales de autenticación y cambios de contraseña en caso de que esta se vea comprometida.*
• *Existen controles de seguridad aplicables a cuentas compartidas.*
4 Control de acceso a sistemas y aplicaciones.
4.1 Restricción del acceso a la información.
• *Existen controles adecuados e identificación individual de cada usuario.*
• *Existe un procedimiento para definir, autorizar, asignar, revisar, gestionar y retirar los derechos de acceso y permisos asignados.*
4.2 Procedimientos seguros de inicio de sesión.
• *Existen formas de disuadir el acceso no autorizado a los sistemas como por ejemplo: pantallas de advertencia, demoras en el sistema, bloqueos, alarmas, registros y alertas.*
• *Existen procedimientos claros para identificar la identidad del usuario que ingresa al sistema, así como autenticación multi factor para sistemas, servicios o conexiones críticas.*
4.3 Gestión de contraseñas de usuario.
• *La fortaleza de las contraseñas está establecida en estándares y políticas de la organización, y se toma en cuenta longitud mínima, restringir la reutilización de contraseñas, nivel de complejidad, cambios forzados de contraseñas, ocultamiento de la contraseña durante el tipeo.*
• *Las contraseñas se transmiten por canales seguros y cifrados.*
4.4 Uso de herramientas de administración de sistemas.
• *Esta claramente definido el responsable de las herramientas de administración.*
• *Se tiene claramente identificado quien, porque, para que, y en que condiciones se puede acceder a las herramientas de administración.*
• *El proceso es auditable y se genera un registro detallado de su uso.*
4.5 Control de acceso al código fuente de los programas.
• *Se cuenta con un entorno de almacenaje del código fuente seguro, con limitación de acceso, monitoreo, control de versiones, registros, etc.*

• *Se tienen procesos claramente establecidos y documentados para realizar modificaciones, publicaciones y compilaciones.*
• *Se generan, almacenan y revisan los registros de acceso y cambios.*

La Tabla 8 contiene las afirmaciones que se evalúan en cada control de Cifrado

Tabla 8- Afirmaciones evaluación de Cifrado.

CIFRADO.
1 Controles criptográficos.
1.1 Política de uso de los controles criptográficos.
• *Existen políticas que cubren el uso de controles criptográficos y estas se cumplen.*
• *Las políticas cubren: Casos de información que debe ser protegida con criptografía, normas que deben aplicarse, proceso basado en el riesgo para identificar la protección necesaria, cifrado para información almacenada y transferida, cumplimiento de normas y leyes aplicables, efectos del cifrado en la inspección de contenidos de software.*
1.2 Gestión de claves.
• *Hay un proceso claro para abarcar todo el ciclo de vida de la gestión de claves incluida la protección del equipo utilizado para generar, almacenar y archivar las claves criptográficas.*
• *Existe un procedimiento para evitar claves débiles o repetidas.*
• *Existen reglas establecidas sobre cambio y actualización de claves.*

Finalmente, en la Tabla 9 se ubican las afirmaciones a ser evaluadas en el apartado Seguridad en las telecomunicaciones.

Tabla 9- Afirmaciones evaluación de Seguridad en las telecomunicaciones.

SEGURIDAD EN LAS TELECOMUNICACIONES.
1 Gestión de la seguridad en las redes.
1.1 Controles de red.

• *Existen políticas que norman las conexiones físicas e inalámbricas.*
• *Existe un sistema adecuado de autenticación para el acceso a la red y se limita el acceso de personas autorizadas a servicios y aplicaciones legitimas.*
• *Existe un control de seguridad de red tanto a nivel de sistemas como a nivel de infraestructura.*
1.2 Mecanismos de seguridad asociados a servicios en red.
• *Existe una gestión, clasificación y protección adecuada de los servicios de red propios y un derecho de auditoría de servicios de red de terceros.*
• *Existe un monitoreo y revisión periódica de los servicios de red y configuraciones de cortafuegos, IDS/IPS, DAM, WAF.*
1.3 Segregación de redes.
• *Existe una política de segmentación de redes y está basada en la clasificación, nivel de confianza, dominios, etc.*
• *Existe una segregación adecuada y clara incluyendo redes de invitados y la segmentación de proveedores y clientes, la cual es controlada y monitoreada a fin de mitigar los riesgos conforme a las políticas de la organización.*
2 Intercambio de información con partes externas.
2.1 Políticas y procedimientos de intercambio de información.
• *Existen políticas enfocadas en la transmisión segura de información en diferentes herramientas de comunicación como son: Wifi, bluetooth, almacenamientos externos mensajería, correo electrónico, FTP, foros, servicios en la nube y similares; basados en la clasificación de información.*
• *Existe un programa de capacitación concientización y cumplimiento, siguiendo el principio de confidencialidad y privacidad.*
2.2 Acuerdos de intercambio.
• *Las responsabilidades sobre la perdida, corrupción o divulgación de datos están claramente definidas.*

• *Se mantiene una cadena de custodia para la información y existe sincronía de los niveles de clasificación de la información por parte de todos los involucrados.*
2.3 Mensajería electrónica.
• *Se tiene controles de seguridad adecuados para mensajería como, por ejemplo: cifrado de correo electrónico, autenticidad, confidencialidad e irrenunciabilidad de mensajes.*
2.4 Acuerdos de confidencialidad y secreto.
• *Existen acuerdos de confidencialidad y estos están revisados y aprobados por el departamento legal, y firmados por las personas adecuadas.*
• *Existen sanciones adecuadas para el caso de incumplimiento y/o beneficios para el cumplimiento de los acuerdos.*

Las afirmaciones de cada uno de los controles de la ISO 27001 seleccionados fueron redactadas en base a los criterios de cumplimiento de cada control, el Workbook de ISO 27K obtenido en [39] que provee una guía de todos los controles para llevar a cabo una verificación de cumplimiento, y las características de las organizaciones virtuales planteadas en [40] donde se puede apreciar la caracterización de una organización virtual en base a varios criterios.

Se buscó obtener un resultado adecuado con el mínimo de afirmaciones a evaluar, esto a fin de reducir la carga, en este punto, a los miembros postulantes de una organización virtual y su representante de TI, quien a fin de cuentas es quien debería completar el check list en base a su situación actual.

Sin embargo, no se ha dejado de lado el abordar cada control con el detalle adecuado para permitir una evaluación adecuada del nivel de implementación de medidas de seguridad por parte de las organizaciones postulantes.

2.4. Evaluación

En la evaluación se describe como se establecen los rangos tanto de evaluación y criticidad y como estos valores una vez asignados son usados para obtener un valor de cada una de las sentencias evaluadas. Además, se explica cómo se obtiene la evaluación final en base a cada uno de los resultados obtenidos.

Relevancia o criticidad

Se debe establecer el nivel de relevancia de cada una de las afirmaciones. Esta información es interna de la herramienta y no necesita ser conocida por la organización evaluada.

Los criterios de evaluación se dividen en una escala de 4 niveles de acuerdo con la criticidad del criterio a ser evaluado. Los niveles seleccionados se muestran en la Tabla 10

Tabla 10 Escala de criticidad

Criticidad de los criterios	
Criticidad Baja	1
Criticidad Media-Baja	2
Criticidad Media-Alta	3
Criticidad Alta	4

Estos niveles de criticidad se asignarán a cada ítem de acuerdo con la evaluación previa de relevancia, donde para cada uno de los dominios se determinó un nivel de relevancia, misma que está dada en función del criterio de varios autores. Para la asignación del nivel de criticidad en cada ítem se asigna en primer lugar un rango para cada dominio, la valoración de cada ítem se hará dentro de este rango y en función de que tan crítico se considere en general se dará el valor correspondiente, esta subvaluación de criticidad dentro de cada rango se hace en base a la apreciación de la frecuencia con la cual puede suscitarse o necesitarse un determinado control. Esto es beneficioso ya que la apreciación de criticidad es

altamente subjetiva, la determinación de un rango en base a diversas opiniones hace que la asignación de estos valores tenga mayor relevancia a nivel general.

Estos niveles de relevancia son muy importantes ya que influyen en gran medida en la valoración final de una organización que se evalúa en la herramienta. Por tanto, influyen directamente en el resultado final del nivel de seguridad de cada organización.

Escala de nivel de implementación

La calificación individual de cada ítem es la valoración que le da cada uno de los entes u organizaciones evaluadas en función del nivel de implementación si es que lo tiene implementado. Esta escala es de conocimiento del evaluado y debe estar claramente entendido, ya que debe ser respondido con total seguridad y honestidad por parte del evaluado. Para facilitar la evaluación y evitar subjetividades a la hora de responder a cada una de las afirmaciones presentadas se ha dividido la escala de respuestas en 3 niveles. Los niveles y su interpretación se muestran en la Tabla 11.

Tabla 11 Métricas de evaluación

Métricas	
Inexistente	0
Parcialmente implementado	1
Completamente implementado	2

A continuación, se describe brevemente en que consiste cada una de las métricas.

- **Inexistente:** La afirmación presentada no se lleva a cabo o no existe dentro de la organización.
- **Parcialmente implementado:** Una parte de la afirmación es verdadera para la empresa mas no se cumple totalmente, la afirmación se ha implementado parcialmente o se está implementando.

- **Completamente implementado:** La afirmación es verdadera en su totalidad, se han implementado todos los requerimientos de la afirmación o los necesarios para cumplir con el objetivo.

El sujeto u organización evaluada debe llenar completamente el check list para acceder a la calificación final de la evaluación y solo se permite una de las 3 respuestas a cada una de las afirmaciones, en ningún caso se permitirá una valoración que no se haya detallado en la Tabla 11.

Cálculos

Se verifica que la totalidad de las respuestas sean válidas, las respuestas en blanco se consideran nulos o ceros para el cálculo del nivel de confianza.

Se separa por grupos de respuestas dependiendo de la criticidad establecida, así se forma por ejemplo un grupo con todas las sentencias con un nivel de criticidad 4.

Dentro de cada grupo se establece un promedio, que servirá para el cálculo de la ponderación total una vez se compute con su peso dentro del puntaje general.

Para cada nivel de criticidad se tiene un peso dentro de la calificación final como se muestra en la Tabla 12.

Tabla 12 Porcentaje de relevancia de las respuestas en base a criticidad

Peso general en base a criticidad	
Valor de Criticidad	**Peso en la valoración general**
4	40%
3	30%
2	20%
1	10%

El peso porcentual derivado de la criticidad establecida para cada sentencia no solo busca alcanzar un 100% sino también se deriva de la investigación previa donde se determina la relevancia para diversos autores, en base a esto, los objetivos de control con mayor calificación superan ligeramente el 40% del total de puntos obtenidos por todos los dominios seleccionados, mientras que el segundo lugar

logra alcanzar una puntuación superior al 20%, dejando una suma cercana al 30% para los dos más bajos de puntuación, siguiendo ese criterio se otorgó valores de 40% al más alto nivel de criticidad, un valor de 30% al segundo nivel de criticidad y un valor conjunto de 30 % a los dos últimos niveles. Estos valores representan el peso que tienen en la calificación final.

Una vez se tenga los promedios en cada nivel de criticidad se puede obtener la valoración general sumando los valores que aporta cada grupo en la calificación final, en este caso la valoración final se presentará sobre 5 puntos, aun así, se presenta un modelo con el cual se puede modificar el puntaje de referencia para la valoración final. Los valores que cada grupo aporta se pueden obtener mediante la Ecuación 1. Para el presente trabajo la ecuación se debe hacer particular con una valoración general de 5, por lo cual se reduce la ecuación a continuación.

Ecuación 1 Valoración final del nivel de criticidad i

$$Vi = P(i) * \Pr(i) * \frac{Vg}{2}$$

Donde:
i: nivel de criticidad del grupo (1, 2, 3 o 4)
Vi: valoración final del nivel i.
P(i): Peso en la valoración general del nivel i.
Pr(i): Promedio calculado del nivel i.
Vg: Valoración general requerida para la evaluación.

En el caso particular se establece una valoración final sobre 5 puntos por lo cual la Ecuación 1 se simplifica, y tenemos como resultado luego de hacer operaciones la Ecuación 2:

$$Vi = \frac{5}{2} * P(i) * \Pr(i)$$

Ecuación 2 Caso particular de la Ecuación 1 para un rango de evaluación de 0 a 5 puntos

$$Vi = 2.5 * P(i) * \Pr(i)$$

La valoración total como se mencionó previamente se obtendrá de la sumatoria de las valoraciones individuales.

Ecuación 3 Valoración total de la herramienta basado en la implementación de seguridad

$$Vt = V1 + V2 + V3 + V4$$

El resultado de la Ecuación 3 nos da el nivel de confianza de la organización virtual en una escala de 0 a 5 puntos, donde 0 representa una absoluta falta de implementación de los criterios evaluados y 5 una implementación completa de los criterios evaluados. La aplicación de la ecuación 3 se ve reflejado en la descripción del caso de estudio y se utiliza para obtener la calificación final de cada una de las organizaciones evaluadas.

El proceso se puede ver resumido en la Figura 2 y el proceso de cálculo se puede ver detallado en la Figura 3.

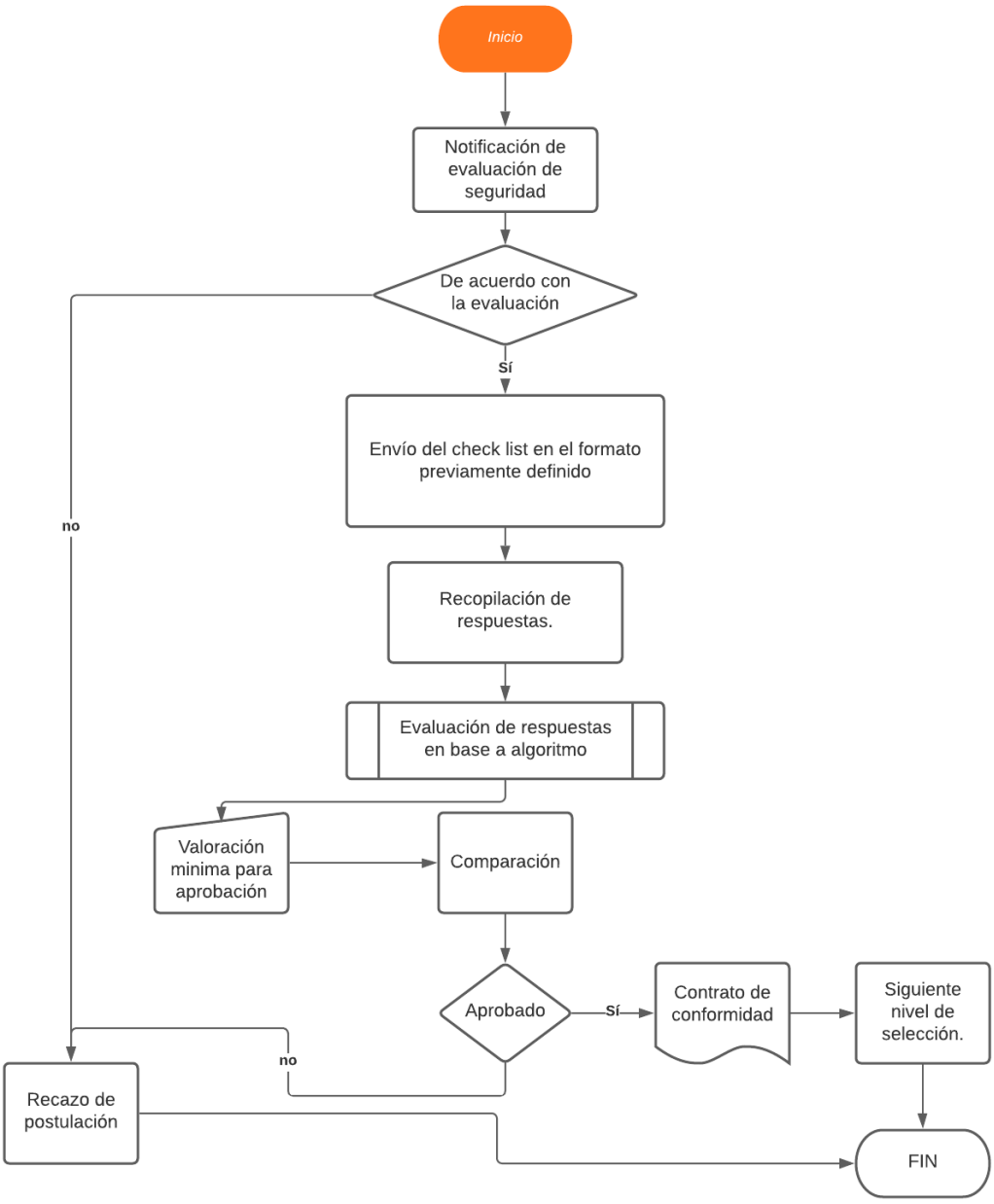


Figura 2 Proceso de selección en base a la herramienta

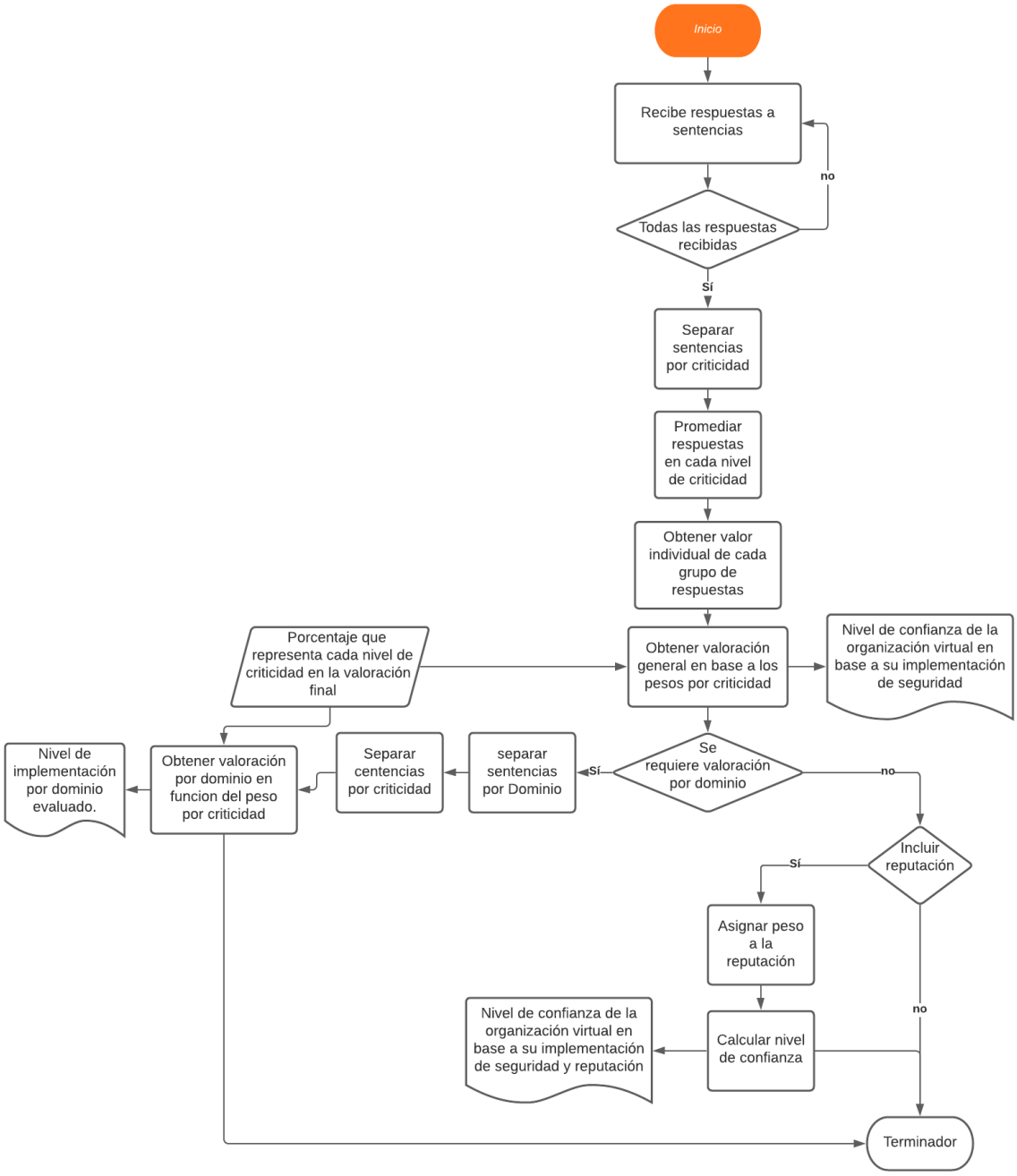


Figura 3 Proceso de evaluación de la herramienta

El nivel requerido para acceder a la organización virtual en formación se determinará en función de los criterios y la necesidad de cada organización virtual formada, si bien una organización virtual que pretenda manejar información sumamente confidencial podría requerir un nivel de confianza superior al 4 o muy cercano a 5 puntos para este caso. Otra organización virtual que no pretende difundir información confidencial o cuya información en general sea de baja confidencialidad podría establecer un nivel de confianza requerido en niveles más

bajos. En cualquier caso, la herramienta permite hacer una selección dependiendo de las necesidades de la organización virtual que se está conformando.

Finalmente se puede o no incluir en la valoración la reputación previa de las organizaciones, claramente este último punto únicamente aplica en el caso de que se tenga un valor de reputación previo para la organización, y esta calificación de la reputación tendrá un peso relativo a la importancia o relevancia que tenga su reputación, no es lo mismo una organización con apenas una o dos calificaciones previas a una Organización con un extenso historial de participación, en el primer caso la reputación deberá tener una influencia mínima respecto al segundo caso en el cual la reputación debe ser considerada con un peso mayor. Esto depende de si se desea o no incluir la reputación previa de las organizaciones en el cálculo del nivel de confianza.

En caso de requerir incluir la reputación, el proceso se hará de la siguiente manera. La reputación debe estar evaluada en la misma escala en la cual se evaluó la implementación de medidas de seguridad calculada previamente.

En el caso particular se estableció una valoración de 5 puntos por lo cual la reputación debe estar valorada sobre 5 puntos.

El peso de la reputación se dará bajo consideración del organizador y puede tener un valor entre 0 y 0.4. Para calcular la valoración de la organización virtual incluyendo la reputación se utiliza la Ecuación 4

Ecuación 4 Valoración total incluido la reputación de la organización.

$$VT = R * pe + Vt * (1 - pe)$$

Donde:

VT = Valoración final basado en reputación.

pe = Peso considerado para la reputación, valoración entre 0 y 0.4.

Vt = Valoración total en base a la implementación de seguridad (Ecuación 3).

R = Reputación de la organización virtual.

2.5. Caso de estudio.

Para ilustrar el funcionamiento de la herramienta detallada en las secciones previas, se utiliza un proceso simulado de formación de organización virtual, donde se proponen 5 candidatos aspirantes a formar parte de la organización virtual, los candidatos son reales sin embargo no se dará a conocer sus nombres ni ningún detalle que permita identificarlos debido a que las organizaciones que participaron de este estudio han solicitado se guarde sigilo en su información, si bien es cierto las respuestas de dos de los candidatos se realizan en base a una situación anterior y no en base a su situación actual a la cual no se tiene acceso, sin embargo se mantienen privados para proteger la imagen y la información privada de los mismos. Se supone un escenario en el cual se requiere 2 organizaciones que se sumen a la cadena productiva con dos actividades claramente definidas, obteniendo una organización virtual conformada por 3 miembros.
Las actividades a realizar se dividen en actividad “A” y actividad “B”, se plantea 3 aspirantes a unirse para colaborar en la actividad “A” y 2 aspirantes para el caso de la actividad “B”.

El resultado de la aplicación de la herramienta, en primer lugar con el check list y en segundo lugar con los cálculos descritos para obtener la valoración del nivel de confianza que se puede depositar en cada organización, permitirá seleccionar un aspirante para cada actividad basados únicamente en la implementación de seguridad de cada organización, si bien es cierto el proceso de selección conlleva el análisis de un mayor número de características de cada socio aspirante, en el presente trabajo se enfoca el punto de vista de la seguridad y el nivel de confianza que en teoría se puede depositar en un aspirante basado únicamente en la herramienta previamente detallada.
La Figura 4 muestra el posible escenario donde se tiene en la parte central a la organización o ente que lidera u organiza la formación de la OV, rodeado de los 5 aspirantes a ser parte de esta OV, 3 de ellos en un rubro o actividad y 2 en el otro. Para el caso particular de estudio se considera establecido el objetivo de la organización virtual y el interés de las organizaciones por participar se da por

sentado, estos pasos son previos a la aplicación de la herramienta por lo cual se asumen cumplidos.

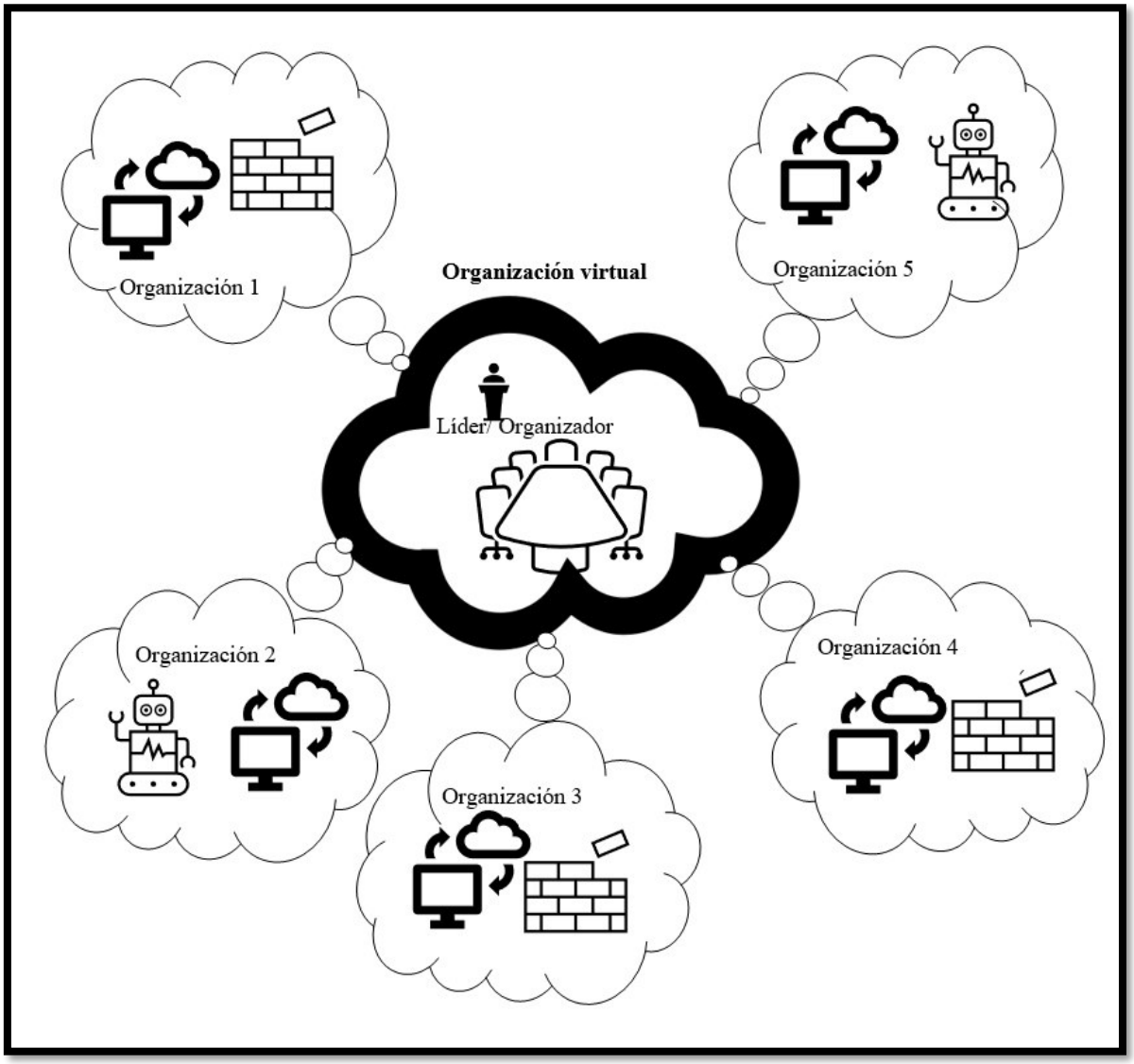


Figura 4 Modelo de aspirantes a conformar una OV

Para iniciar el caso de estudio con la herramienta se envía el check list a las organizaciones aspirantes junto con las indicaciones para su correcto uso, y se espera recibir todas las respuestas completas, como se mencionó en la descripción de cálculos las respuestas vacías se rellenan con 0, en el Anexo II – Respuestas de la evaluación realizada a la organización 1 (O1), se puede ver las respuestas obtenidas para la organización 1.

Una vez son recibidas las respuestas se procede a tabular los resultados para obtener los promedios de cada nivel de criticidad, a continuación, se muestran los resultados obtenidos.

Para cada una de las organizaciones evaluadas se realiza el mismo procedimiento por lo cual solo se muestra uno de los procesos, los resultados finales se muestran de las 5 organizaciones a fin de realizar una comparación.

Con las respuestas obtenidas de cada uno de los ítems evaluados se obtiene los promedios para cada nivel de criticidad los cuales se tabulan en la Tabla 13.

Tabla 13 Promedios por nivel de criticidad obtenidos O1

Resultados de las respuestas obtenidas	
Nivel de criticidad	Promedio obtenido.
4	1
3	0,93333333
2	0,68421053
1	0,66666667

A continuación, se realiza el cálculo de cada uno de los valores en la calificación general con ayuda de la Ecuación 2.
Vamos a obtener la valoración final para cada nivel de criticidad.

$$Vi = 2.5 * P(i) * \Pr(i)$$

Para nivel de criticidad 1

$$V1 = 2.5 * P(1) * \Pr(1)$$
$$V1 = 2.5 * 0.1 * 0.667$$
$$V1 = 0.1667$$

Para nivel de criticidad 2.

$$V2 = 2.5 * P(2) * \Pr(2)$$
$$V2 = 2.5 * 0.2 * 0.6842$$
$$V2 = 3421$$

Para nivel de criticidad 3.

$$V3 = 2.5 * P(3) * \Pr(3)$$
$$V3 = 2.5 * 0.3 * 0.9333$$
$$V3 = 0.7$$

Para nivel de criticidad 4.

$$V4 = 2.5 * P(4) * \Pr(4)$$
$$V4 = 2.5 * 0.4 * 1$$
$$V4 = 1$$

Luego de realizar el cálculo para cada nivel de criticidad se obtienen los datos mostrados en la Tabla 14.

Tabla 14 Valoración final por nivel de criticidad

Valoración final por nivel de criticidad	
Nivel de criticidad	Valoración final.
4	1
3	0,7
2	0,34210526
1	0,16666667

Finalmente, con los valores obtenidos se puede obtener la calificación final del nivel de confianza sobre 5 puntos para la organización evaluada, en este caso particular la valoración final obtenida mediante la Ecuación 3 es:

$$Vt = 2.21/5$$

Como se mencionó previamente el proceso detallado para las otras 4 organizaciones no se muestra sin embargo si se muestran los resultados finales obtenidos para cada una de las organizaciones.

Para verificar el funcionamiento de la herramienta se muestran de cada organización la valoración final en base a los valores obtenidos con la herramienta.

Organización 2:

$$Vt = 3.36$$

Organización 3:

$$Vt = 2.98$$

Organización 4:

$$Vt = 2.84$$

Organización 5:

$$Vt = 3.97$$

Con los datos obtenidos se puede organizar los resultados y determinar el uso y ayuda que representa el contar con una herramienta para medir el nivel de confianza que se puede depositar en una organización postulante a ser miembro de una organización virtual.

No se incluye la valoración en base a la reputación previa ya que se considera que es la primera vez que forman parte de la organización virtual y el organizador no tiene datos previos para realizar el cálculo, caso contrario se puede utilizar la Ecuación 4 para calcular la valoración final en base a la implementación de medidas de seguridad y la reputación previa que se tenga de las organizaciones evaluadas.

Concluyendo con la posible selección de las organizaciones 3 y 5, cada una alcanza la mayor calificación en su rubro para continuar con el proceso, recalcando que esta selección está basada únicamente en el tema de seguridad.

3. RESULTADOS Y DISCUSIÓN

En esta sección se muestra los resultados obtenidos al aplicar la herramienta y se discute los aspectos que diferencian el presente trabajo.

3.1. Resultados

A continuación, se presenta un resumen de los resultados obtenidos por cada una de las organizaciones evaluadas con la herramienta propuesta. La Tabla 15 muestra los resultados obtenidos, los valores que se obtienen para cada organización son resultado directo de la evaluación realizada a las prácticas de seguridad que han implementado mediante la herramienta propuesta, se ha establecido una escala de 0 a 5 para dar esta calificación, siendo 0 una ausencia total de implementación de los criterios evaluados y 5 una completa implementación de los criterios evaluados.

Tabla 15- Resultados obtenidos por las organizaciones 0 a 5

Resultados obtenidos	
Organización	Valor obtenido/5
Organización 1	2.21
Organización 2	3.36
Organización 3	2.98
Organización 4	2.84
Organización 5	3.97

En base a los resultados obtenidos por cada organización el determinar qué organización puede brindar un mayor nivel de confianza a la organización virtual que se está conformando se simplifica considerablemente, para este caso tenemos que las organizaciones de la actividad “A” son 3, O1, O3 y O4, de las 3 la Organización 3 (O3) es la que posee una mayor calificación en cuanto a su implementación de medidas de seguridad, por tanto es la organización en la cual teóricamente se puede depositar un mayor nivel de confianza.

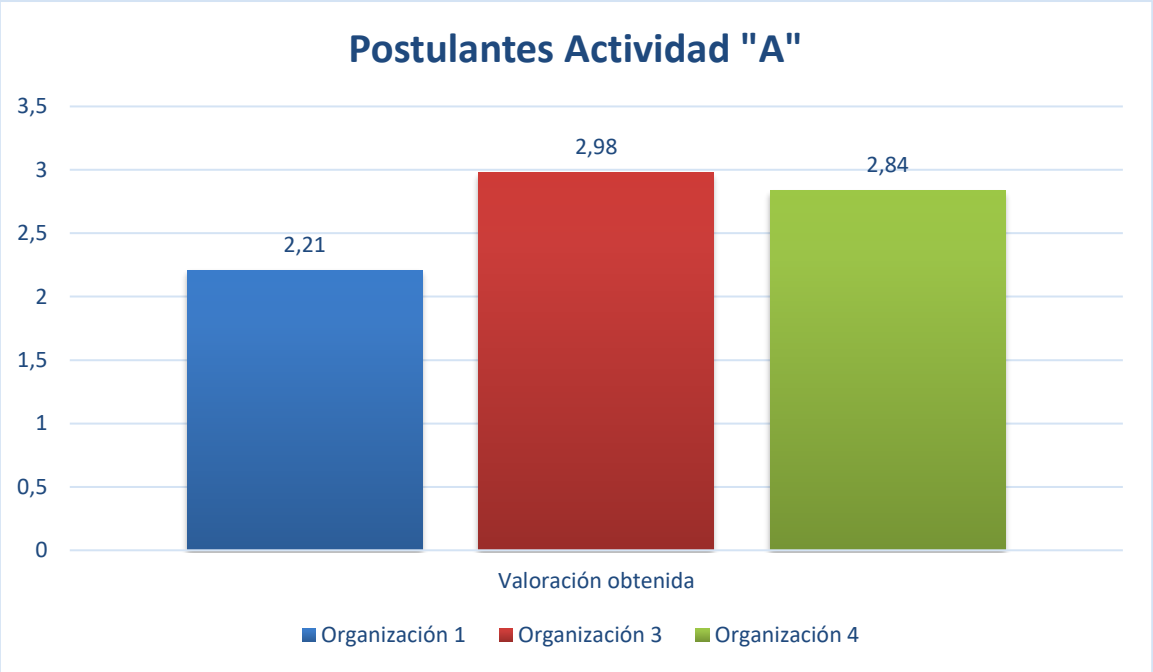


Figura 5 Comparativa postulantes actividad "A"

Para el caso de la actividad “B” entre las 2 organizaciones postulante que son la O2 y O5, se tiene que la mayor calificación es la obtenida por la organización 5 (O5),

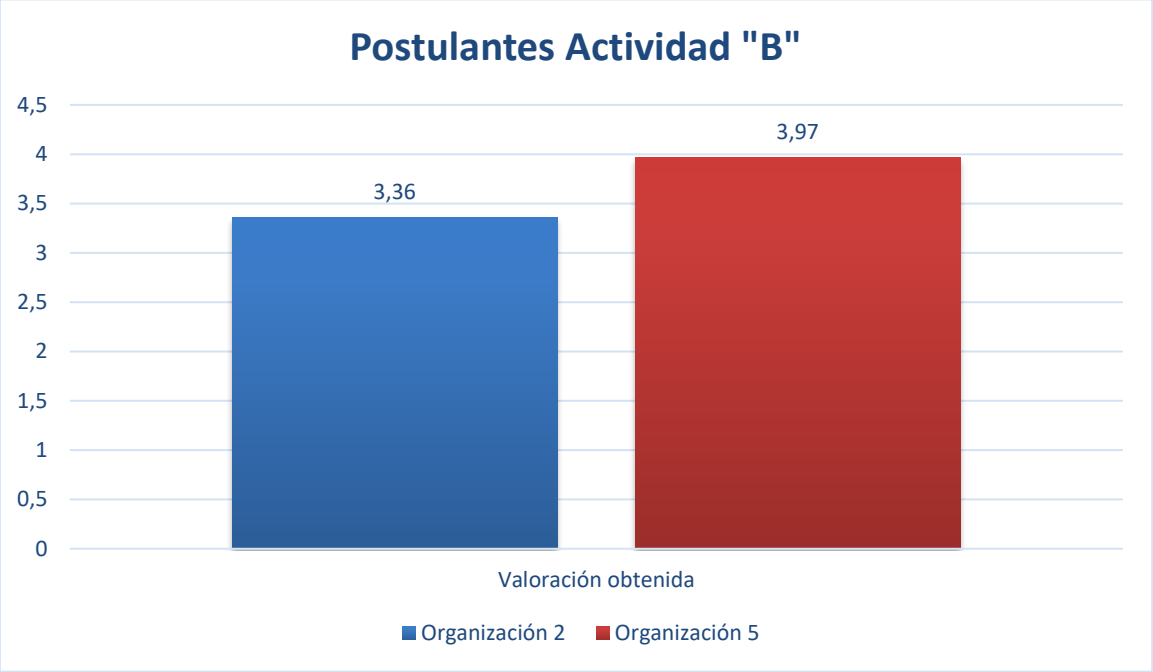


Figura 6 Comparativa postulantes actividad "B"

En este caso basados únicamente en los resultados de la herramienta se puede formar la Organización virtual con las organizaciones 3 y 5, como se mencionó previamente la selección no solo depende de un factor sino de una serie de factores, la herramienta como tal permite tener una valoración de implementación de seguridad que se pueda utilizar en la selección.

Los resultados obtenidos son concordantes con la estimación de las organizaciones evaluadas así vemos que las organizaciones 2 y 5 son organizaciones relacionadas a temas tecnológicos por lo que les son más familiares los temas de protección de la información, la herramienta obtuvo una calificación más alta para estas dos organizaciones, sobre las otras tres que si bien es cierto mantienen ciertos controles de seguridad al no estar directamente enfocadas en rubros tecnológicos, su calificación es más baja que las anteriores. Este fenómeno se puede evidenciar claramente en la Figura 7, donde se observa por encima de la franja naranja a las 2 organizaciones cuyas actividades o rubros principales son los tecnológicos.

Figura 7 valores obtenidos por las organizaciones 0 a 5

Selección de miembros

Cada organización virtual puede establecer su nivel de seguridad requerido mínimo para formar parte de la misma, en ese sentido posiblemente la organización con el mayor puntaje obtenido no siempre sea la organización seleccionada, pero si se puede discriminar de inicio las organizaciones con niveles por debajo de la valoración requerida.

Por ejemplo, si para el caso estudia se propone una valoración mínima de 2.75/5 para cualquier miembro que quiera forma parte de la Organización virtual, inmediatamente se puede descartar la organización 1, antes de cualquier análisis de fatores adicionales. Lo cual reduce el tiempo y el esfuerzo necesario para la selección de miembros.

3.2. Discusión

La herramienta permite determinar la confianza que se puede depositar en una organización postulante a formar parte de una organización virtual, basada en objetivos de control de la ISO 27001, seleccionados en base a los criterios que son más relevantes de acuerdo con varios autores, lo que hace la herramienta confiable y útil para establecer una calificación de la implementación de medidas de

seguridad. Sin embargo, se requiere establecer contratos y acuerdos de servicio para garantizar que los resultados obtenidos sean asumidos con responsabilidades directas a cada uno de los miembros postulantes una vez elegidos para formar parte de la OV.

La herramienta a diferencia de otras como se verá adelante no se basa en criterios seleccionado en base a una sola opinión o percepción de importancia, sino que toma en cuenta diversos criterios a fin de formar una herramienta que sea aplicable a la mayor parte de casos, salvo ciertas aplicaciones donde se requiera un tipo de criterio particular ya sea por la naturaleza u objetivo de la aplicación.

A continuación, se presenta una comparación entre algunos aspectos tomados en cuenta por otras herramientas orientadas ya sea a la selección de miembros o a la evaluación de seguridad en organizaciones virtuales.
Las características más significativas de la herramienta y el proceso propuestos son:

1. Basado en distintos puntos de vista.
2. Determinación de criticidad en base a relevancia.
3. Posibilidad de incluir o no reputación previa.
4. Calificación de nivel de confianza en base a implementaciones de seguridad.
5. En base a estándares de seguridad.
6. Evaluación sencilla.
7. Evaluación independiente de terceros

Tabla 16 Comparativa de trabajos previos

	1	**2**	**3**	**4**	**5**	**6**	**7**
[7]	✗	✗	✗	✗	✗	✓	✗
[24]	✗	✓	✗	✓	✓	✗	✓
[9]	✓	✗	✗	✗	✗	✓	✓

[6]	✗	✓	✗	✓	✗	✓	✓
Este trabajo	✓	✓	✓	✓	✓	✓	✓

La Tabla 16 muestra las características destacadas de la herramienta y como algunos trabajos previos relacionados a la temática no llegan a cumplir todas las características destacadas en el trabajo realizado. La herramienta también utiliza este análisis de criterios para establecer una relevancia de cada uno de los dominios y de los ítems evaluados, dejando de lado la apreciación personal en cada uno de los ítems que se contabilizan en esta herramienta. El cálculo final está orientado a servir en cualquier escala de acuerdo a las necesidades de granularidad que se necesiten, si en determinadas circunstancias con el valor sugerido se tiene varias organizaciones con puntajes similares y no se puede realizar una correcta discriminación se puede optar por utilizar una escala mayor que permita diferenciar claramente los resultados obtenidos.

Como valor adicional la herramienta permite incluir la reputación en los cálculos realizados para obtener una valoración final más completa si hay data relacionada a la reputación previa de las organizaciones postulantes, de no ser el caso la herramienta funciona perfectamente sin el uso de data previa.

Por los motivos descritos la herramienta es apropiada para su uso en el proceso de formación de organizaciones virtuales y permite tener una valoración inicial de confianza que se puede depositar en cada uno de los aspirantes.

La herramienta basada en la ISO 27001 permite dar una valoración del nivel de confianza o de implementación de medidas de seguridad en organizaciones postulantes a pertenecer a una OV, y estos datos como se ha mencionado sirven de apoyo para que el o los organizadores puedan tomar decisiones inteligentes en el proceso de conformación de OVs permitiendo descartar tempranamente postulantes con niveles de implementación de seguridad por debajo del mínimo

requerido, por tanto, podemos concluir que la hipótesis planteada al inicio del proyecto es verdadera.

En conclusión se tiene una herramienta desarrollada y diseñada en función de la búsqueda de criterios de diversos autores en cuanto a aspectos de seguridad y los controles de la norma ISO27001 que actualmente es la norma recomendada para aspectos relacionados a seguridad de la información en organizaciones, otra herramienta permite dar una valoración inicial del nivel de confianza que se puede depositar en una organización virtual previo a que se continue con el proceso de selección, esto permite descartar tempranamente organizaciones con estándares de seguridad bajos y aliviar la carga de las siguientes etapas del proceso de selección a la vez que permite discriminar las organizaciones que por su nivel de seguridad pueden formar parte de la organización y se les puede depositar con confianza la información que se pretende compartir.

4. CONCLUSIONES

Se elaboró una herramienta que permite evaluar el nivel de implementación de medidas de seguridad de una organización aspirante a formar parte de una organización virtual con base en los dominios objetivos de control y controles que plantea la ISO 27001. La herramienta emite una valoración de 0 a 5 para el nivel de confianza, sin embargo, este rango de evaluación se puede variar y ajustarlo a las necesidades particulares de cada organizador o caso de estudio individual, lo cual brinda una mayor versatilidad y adaptabilidad de la herramienta.

Se establecieron los criterios más relevantes en función de diversos puntos de vista y se valoró su relevancia para tener un modelo de evaluación que se ajuste a las principales necesidades de seguridad de organizaciones virtuales y entornos distribuidos.

Se desarrollo una lista de verificación o check list con los criterios seleccionados para su evaluación a la vez que se asignó un rango de evaluación de 3 niveles para cada sentencia considerada en el check list.

Los resultados obtenidos se apegan a la realidad de las empresas evaluadas las cuales son de diversos entornos, lo cual nos da la confianza de poder utilizarla con en el análisis de cualquier tipo de organización aspirante. Para el caso de estudio se utilizó organizaciones de dos ramas diferentes con diferentes enfoques lo cual nos dio como resultado una clara diferencia de puntajes en sus niveles de confianza.

El trabajo desarrollado presenta varias características que son y serán útiles para cualquier organización virtual en proceso de selección de miembros, ya que permite obtener una valoración de seguridad y confianza como un punto de partida para tomar decisiones con datos reales, también permite la inclusión de la reputación previa lo que incrementa el poder de la herramienta al tomar en cuenta datos de interacciones anteriores para la calificación general.

La herramienta permite emitir una valoración general de confianza basada en la implementación de seguridad de cada organización, tomando en cuenta criterios de diversos autores para determinar los aspectos más significativos a evaluar, además permite incluir la reputación previa de cada organización y asignarle un porcentaje de influencia en el puntaje final.

El proceso es adaptable a cualquier organización y se requiere un conocimiento mínimo de TI, lo que si requiere es un conocimiento del estado actual de la organización y los procesos que se siguen para poder responder adecuadamente las sentencias que se evaluarán.

5. RECOMENDACIONES.

Para el uso de la herramienta es necesario que se establezcan acuerdos claros de participación donde cada uno de los postulantes asuma su responsabilidad sobre el uso de la herramienta y la calificación obtenida, para tener una base sobre la cual reaccionar en caso de incumplimiento o ingreso de información falsa o engañosa.
A futuro se pueden desarrollar mecanismos de análisis de datos que permitan en base a datos previos, conocidos o generados en tiempo real, determinar si las respuestas obtenidas son consecuentes con la situación actual de cada postulante.
Se puede establecer mecanismos futuros que permitan determinar de acuerdo al objetivo u orientación que tenga la conformación de la organización virtual determinar un valor mínimo por dominio para el proceso de selección.

6. REFERENCIAS BIBLIOGRÁFICAS

[1] J. Li, J. Huai, C. Hu, and Y. Zhu, “A secure collaboration service for dynamic virtual organizations,” *Inf. Sci. (Ny).*, vol. 180, no. 17, pp. 3086–3107, 2010, doi: 10.1016/j.ins.2010.05.014.

[2] J. Cao, W. Yu, and Y. Qu, “A new complex network model and convergence dynamics for reputation computation in virtual organizations,” *Phys. Lett. Sect. A.*, vol. 356, no. 6, pp. 414–425, 2006, doi: 10.1016/j.physleta.2006.04.005.

[3] I. Jamai, L. Ben Azzouz, and L. A. Saidane, “Security issues in Industry 4.0,” *2020 Int. Wirel. Commun. Mob. Comput. IWCMC 2020*, vol. 0, pp. 481–488, 2020, doi: 10.1109/IWCMC48107.2020.9148447.

[4] M. Waidner and M. Kasper, “Security in industrie 4.0 - Challenges and solutions for the fourth industrial revolution,” *Proc. 2016 Des. Autom. Test Eur. Conf. Exhib.*, pp. 1303–1308, 2016, doi: 10.3850/9783981537079_1005.

[5] M. M. Alani and M. Alloghani, “Security Challenges in the Industry 4.0 Era,” *Ind. 4.0 Eng. a Sustain. Futur.*, pp. 117–136, 2019, doi: 10.1007/978-3-030-12953-8.

[6] X. Ni and J. Luo, “A clustering analysis based trust model in grid environment supporting virtual organizations,” *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 100–105, 2008, doi: 10.1109/WAINA.2008.162.

[7] L. Kagal, T. W. Finin, and A. Joshi, “Moving from Security to Distributed Trust in Ubiquitous Computing Environments,” *IEEE Comput.*, vol. 34, no. 12, pp. 154–157, 2001.

[8] R. Toro, J. E. Correa, and P. M. Ferreira, “A Cloud-Monitoring Service for Manufacturing Environments,” *Procedia Manuf.*, vol. 26, pp. 1330–1339, 2018, doi: 10.1016/j.promfg.2018.07.128.

[9] E. C. Kasper-Fuehrer and N. M. Ashkanasy, “Communicating trustworthiness and building trust in interorganizational virtual organizations,” *J. Manage.*, vol. 27, no. 3, pp. 235–254, 2001, doi: 10.1016/S0149-2063(01)00090-3.

[10] D. Lekkas, “Establishing and managing trust within the public key infrastructure,” *Comput. Commun.*, vol. 26, no. 16 SPEC., pp. 1815–1825, 2003, doi: 10.1016/S0140-3664(03)00077-X.

[11] ISO, “INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and,” *ACM Work. Form. Methods Secur. Eng. DC, USA*, vol. 34, no. 19, pp. 45–55, 2018, [Online]. Available: http://www.worldcat.org/title/service-

operation/oclc/254028066&referer=brief_results%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf%0Ahttp://k504.kh.

[12] Q. Zheng and X. Zhang, “Study of virtual organizations using multi-agent system,” *Proc. Int. Conf. Auton. Agents*, pp. 1257–1258, 2005, doi: 10.1145/1082473.1082666.

[13] R. Deitos, F. Kerschbaum, and P. Robinson, “A comprehensive security architecture for dynamic, web service based Virtual Organizations for businesses,” *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 103–104, 2006, doi: 10.1145/1180367.1180386.

[14] L. M. Camarinha-Matos, H. Afsarmanesh, and M. Ollus, *Virtual Organizations Systems and Practices*. Springer, 2005.

[15] C.-P. Lopez, M. Santórum, and J. Aguilar, “Autonomous Cycles of Collaborative Processes for Integration Based on Industry 4.0,” *Inf. Technol. Syst.*, 2019.

[16] A. C. Squicciarini, F. Paci, and E. Bertino, “Trust establishment in the formation of Virtual Organizations,” *Comput. Stand. Interfaces*, vol. 33, no. 1, pp. 13–23, 2011, doi: 10.1016/j.csi.2010.03.003.

[17] L. M. Camarinha-Matos and H. Afsarmanesh, “Creation of virtual organizations in a breeding environment,” *IFAC Proc. Vol.*, vol. 12, no. PART 1, 2006, doi: 10.3182/20060517-3-fr-2903.00304.

[18] G. Breda and M. Kiss, “Overview of information security standards in the field of special protected industry 4.0 areas & industrial security,” *Procedia Manuf.*, vol. 46, no. 2019, pp. 580–590, 2020, doi: 10.1016/j.promfg.2020.03.084.

[19] I. Meriah and L. B. A. Rabai, “Comparative study of ontologies based iso 27000 series security standards,” *Procedia Comput. Sci.*, vol. 160, pp. 85–92, 2019, doi: 10.1016/j.procs.2019.09.447.

[20] G. Disterer, “ISO/IEC 27000, 27001 and 27002 for information security mangement,” *J. Inf. Secur. 2013*, p. 9, 2013, doi: 10.5555/uri:pii:0022214357900999.

[21] M. M. Alani, “Prioritizing cloud security controls,” *ACM Int. Conf. Proceeding Ser.*, 2017, doi: 10.1145/3231830.3231831.

[22] S. Morimoto, S. Shigematsu, Y. Goto, and J. Cheng, “Formal verification of security specifications with common criteria,” *Proc. ACM Symp. Appl. Comput.*, pp. 1506–1512, 2007, doi: 10.1145/1244002.1244325.

[23] C. Preschern, “Catalog of Security Tactics linked to Common Criteria Requirements,” vol. 17, pp. 1–17, 2012, [Online]. Available:

https://dl.acm.org/doi/10.5555/2821679.2831277.

[24] M. Kamel, A. Benzekri, F. Barrere, and R. Laborde, “Evaluating the conformity of an access control architecture for virtual organizations with ISO/IEC 17799,” *2007 1st Int. Glob. Inf. Infrastruct. Symp. GIIS 2007 - "Closing Digit. Divid.*, pp. 173–180, 2007, doi: 10.1109/GIIS.2007.4404185.

[25] N. Lavrač, P. Ljubič, T. Urbanič, G. Papa, M. Jermol, and S. Bollhalter, “Trust modeling for networked organizations using reputation and collaboration estimates,” *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 37, no. 3, pp. 429–439, 2007, doi: 10.1109/TSMCC.2006.889531.

[26] S. D. Ramchurn, D. Huynh, and N. R. Jennings, “Trust in multi-agent systems,” *Knowl. Eng. Rev.*, vol. 19, no. 1, pp. 1–25, 2004, doi: 10.1017/S0269888904000116.

[27] Y. Zuo and B. Panda, “Component based trust management in the context of a virtual organization,” *Proc. ACM Symp. Appl. Comput.*, vol. 2, pp. 1582–1588, 2005, doi: 10.1145/1066677.1067035.

[28] M. Gschwandtner, L. Demetz, M. Gander, and R. Maier, “Integrating threat intelligence to enhance an organization’s information security management,” *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3230833.3232797.

[29] K. Kwak, K. Lee, D. Won, and S. Kim, “Analysis and countermeasures of security vulnerability on portal sites,” *Proc. 5th Int. Conf. Ubiquitous Inf. Manag. Commun. ICUIMC 2011*, 2011, doi: 10.1145/1968613.1968728.

[30] A. Uta, I. Ivan, M. Popa, C. Ciurea, and M. Doinea, “Security of virtual entities,” *ACM Int. Conf. Proceeding Ser.*, vol. 883, pp. 278–285, 2014, doi: 10.1145/2659532.2659634.

[31] Common Criteria, “Common Criteria for Information Technology Security Evaluation - Part 2 : Security functional components,” *Common Criteria*, vol. 3.1, no. April, pp. 1–321, 2017, [Online]. Available: https://www.commoncriteriaportal.org/cc/.

[32] M. P. Cristescu, E. A. Stoica, and L. V. Ciovică, “Web Services Specific Security Standards,” *Sci. Direct*, vol. 16, no. May, pp. 597–602, 2014, doi: 10.1016/s2212-5671(14)00846-6.

[33] M. Zaydi and B. Nassereddine, “A new comprehensive solution to handle information security governance in organizations,” *ACM Int. Conf. Proceeding Ser.*, vol. Part F1481, pp. 1–5, 2019, doi: 10.1145/3320326.3320382.

[34] P. J. Chuang and M. Y. Ni, “Efficient and secure trust negotiation over the internet,” *Proc. - Int. Symp. Parallel Archit. Algorithms Program. PAAP*, pp. 19–24, 2012, doi: 10.1109/PAAP.2012.11.

[35] M. Niinimaki and V. Sivunen, “Applying Grid security and virtual organization tools in

distributed publication databases," *Proc. 1st Int. Symp. Inf. Commun. Technol.*, pp. 543–548, 2003.

[36] I. Constandache, A. Yumerefendi, and J. Chase, "Secure control of portable images in a virtual computing utility," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 1–8, 2008, doi: 10.1145/1456482.1456484.

[37] S. Aly, J. Tyrychtr, R. Kvasnicka, and I. Vrana, "Novel methodology for developing a safety standard based on clustering of experts' assessments of safety requirements," *Saf. Sci.*, vol. 140, p. 105292, 2021, doi: 10.1016/j.ssci.2021.105292.

[38] INB, "Information technology – Security techniques – Information security management systems – Requirements," p. 44, 2013.

[39] "ISO27k infosec management standards." https://www.iso27001security.com/ (accessed Aug. 25, 2021).

[40] T. M. Guamushig, C. P. Lopez, M. Santorum, and J. Aguilar, "Characterization of a fourth generation virtual organization based on industry 4.0," *Proc. - 2019 Int. Conf. Inf. Syst. Softw. Technol. ICI2ST 2019*, pp. 182–186, 2019, doi: 10.1109/ICI2ST.2019.00033.

ANEXOS

Anexo I – Nivel de criticidad para cada afirmación a ser evaluada.

Criticidad	Dominios y sentencias
	1 Responsabilidad sobre los activos.
	1.1 Inventario de activos.
3	· Existe un inventario de activos de la información.
2	· El inventario es lo suficientemente completo, preciso, detallado y se mantiene actualizado correctamente.
	1.2 Propiedad de los activos.
2	· Los activos de información tienen un propietario y un responsable técnico
1	· Existe un sistema de asignación, etiquetado e información de incidentes para los activos de información.
	1.3 Uso aceptable de los activos.
2	· Existe una política que norma el uso apropiado de recursos tecnológicos como correo electrónico, mensajería, FTP, incluyendo el comportamiento del usuario en internet y redes sociales, y que además establece responsabilidades por parte del usuario.
3	· Se ha socializado correctamente lo que constituye un uso inapropiado de activos a todos los miembros de la empresa.
	1.4 Devolución de activos.
3	· Existe un procedimiento para recuperación de activos de información tras una baja o despido que garantiza el correcto tratamiento de los mismos.
2	· Existe un procedimiento a seguir para abordar el caso de activos de información que no han sido devueltos.
	2 Clasificación de la información.
	2.1 Directrices de clasificación.
2	· Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados a la clasificación de la información. Y estas se ligan a obligaciones contractuales o legales.
2	· La clasificación se basa en los requisitos de seguridad de la información (confidencialidad, integridad, disponibilidad), y el personal está consciente de ellos.
	2.2 Etiquetado y manipulado de la información.
1	· Existe un proceso de etiquetado de la información tanto física como electrónica, sincronizado con las políticas de clasificación de la información que garantiza una correcta manipulación de la información.
3	· Existen niveles de clasificación y se garantiza el acceso únicamente a aquellos con permisos de acceso aprobados.
	2.3 Manipulación de activos.
2	· Para la manipulación de activos se tiene en consideración: Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios físicos y electrónicos, divulgación, intercambio, intercambio con terceros, traslado, etc.
	3 Manejo de los soportes de almacenamiento.
	3.1 Gestión de soportes extraíbles.

2	· Existe un registro detallado de medios extraíbles como CD/DVD, almacenamiento USB y demás medios extraíbles.
2	· Los medios extraíbles están correctamente etiquetados, manejados y almacenados garantizando que no exista acceso no autorizado a la información almacenada.
	3.2 Eliminación de soportes.
2	· Existe una política orientada a la eliminación de activos de información ligada a obligaciones legales y contractuales de los responsables, que permita además realizar un seguimiento del proceso de eliminación.
3	· Se tiene en cuenta la criticidad de la información para el proceso de eliminación: Respaldo de información, periodos de retención y eliminación segura (borrado criptográfico, desmagnetización, destrucción física),
	3.3 Soportes físicos en tránsito.
3	· Se utiliza servicios de transporte confiables y mecanismos adecuados de cifrado para las transferencias de información.
1	· Se verifica la recepción en el lugar de destino de la información.
	CONTROL DE ACCESOS.
	1 Requisitos de negocio para el control de accesos.
	1.1 Política de control de accesos.
4	· Existe una política de control de acceso que contempla una asignación adecuada de deberes y un proceso documentado de control de acceso.
3	· El proceso de aprobación de acceso requiere la participación del propietario del sistema o de la información.
	1.2 Control de acceso a las redes y servicios asociados.
4	· El acceso VPN e inalámbrico esta correctamente supervisado, controlado y autorizado.
3	· Se utiliza una autenticación multi factor para acceso a redes sistemas y aplicaciones criticas.
3	· Existe un proceso de monitoreo y pruebas constante para detectar accesos no autorizados, tiempos de respuesta a incidentes, entre otros.
	2 Gestión de acceso de usuario.
	2.1 Gestión de altas/bajas en el registro de usuarios.
3	· El alta de un usuario por solicitud pasa por un proceso adecuado de aprobación y registro, y genera un ID único para cada usuario.
4	· Existe un proceso para la baja de los ID de usuario de forma inmediata tras el cese o despido o si ya no son necesarios previa confirmación.
	2.2 Gestión de los derechos de acceso asignados a usuarios.
3	· Cada acceso a sistemas está basado en las necesidades del negocio y se corresponde con las políticas de control de acceso y segregación de funciones.
3	· Se documenta adecuadamente las solicitudes y aprobaciones de acceso.
	2.3 Gestión de los derechos de acceso con privilegios especiales.
4	· Existe un proceso periódico de revisión de cuentas con privilegios especiales que contemple, asignación y eliminación de privilegios en base a necesidades.

4	· Existe una diferenciación de usuarios con privilegios especiales, tanto en ID, caducidad de cuentas y controles más estrictos de actividades.
	2.4 Gestión de información confidencial de autenticación de usuarios.
4	· Hay restricciones técnicas como: longitud mínima de contraseña, reglas de complejidad, cambio forzado de contraseña, autenticación en múltiples factores, etc.
4	· El utiliza cifrado en almacenamiento y manipulación de contraseñas en dispositivos, sistemas y aplicaciones.
4	· Se verifica la identidad del usuario antes de proporcionar contraseña temporal nueva y esta contraseña es suficientemente fuerte.
	2.5 Revisión de los derechos de acceso de los usuarios.
3	· Se revisa periódicamente los derechos de acceso de los usuarios y se lleva un registro documental de las revisiones.
3	· Las revisiones se realizan en presencia de los propietarios para verificar cambios en las funcionas para los usuarios.
	2.6 Retirada o adaptación de los derechos de acceso
3	· Existe un proceso estructurado de reasignación o eliminación de derechos de acceso en el cual se contempla el acceso tanto físico como lógico a los sistemas.
4	· Las contraseñas se eliminan o cambian inmediatamente en caso de finalización de contrato, cambio de rol etc.
	3 Responsabilidades del usuario.
	3.1 Uso de información confidencial para la autenticación.
4	· Existe medidas que aseguran la confidencialidad de las credenciales de autenticación y cambios de contraseña en caso de que esta se vea comprometida.
3	· Existen controles de seguridad aplicables a cuentas compartidas.
	4 Control de acceso a sistemas y aplicaciones.
	4.1 Restricción del acceso a la información.
4	· Existen controles adecuados e identificación individual de cada usuario.
3	· Existe un procedimiento para definir, autorizar, asignar, revisar, gestionar y retirar los derechos de acceso y permisos asignados.
	4.2 Procedimientos seguros de inicio de sesión.
4	· Existen formas de disuadir el acceso no autorizado a los sistemas como por ejemplo: pantallas de advertencia, demoras en el sistema, bloqueos, alarmas, registros y alertas.
4	· Existen procedimientos claros para identificar la identidad del usuario que ingresa al sistema, así como autenticación multi factor para sistemas, servicios o conexiones críticas.
	4.3 Gestión de contraseñas de usuario.
3	· La fortaleza de las contraseñas está establecida en estándares y políticas de la organización, y se toma en cuenta longitud mínima, restringir la reutilización de contraseñas, nivel de complejidad, cambios forzados de contraseñas, ocultamiento de la contraseña durante el tipeo.
4	· Las contraseñas se transmiten por canales seguros y cifrados.
	4.4 Uso de herramientas de administración de sistemas.
4	· Esta claramente definido el responsable de las herramientas de administración.

4	· Se tiene claramente identificado quien, porque, para que, y en que condiciones se puede acceder a las herramientas de administración.
3	· El proceso es auditable y se genera un registro detallado de su uso.
	4.5 Control de acceso al código fuente de los programas.
4	· Se cuenta con un entorno de almacenaje del código fuente seguro, con limitación de acceso, monitoreo, control de versiones, registros, etc.
3	· Se tienen procesos claramente establecidos y documentados para realizar modificaciones, publicaciones y compilaciones.
4	· Se generan, almacenan y revisan los registros de acceso y cambios.
	CIFRADO.
	1 Controles criptográficos.
	1.1 Política de uso de los controles criptográficos.
3	· Existen políticas que cubren el uso de controles criptográficos y estas se cumplen.
2	· Las políticas cubren: Casos de información que debe ser protegida con criptografía, normas que deben aplicarse, proceso basado en el riesgo para identificar la protección necesaria, cifrado para información almacenada y transferida, cumplimiento de normas y leyes aplicables, efectos del cifrado en la inspección de contenidos de software.
	1.2 Gestión de claves.
3	· Hay un proceso claro para abarcar todo el ciclo de vida de la gestión de claves incluida la protección del equipo utilizado para generar, almacenar y archivar las claves criptográficas.
3	· Existe un procedimiento para evitar claves débiles o repetidas.
2	· Existen reglas establecidas sobre cambio y actualización de claves.
	SEGURIDAD EN LAS TELECOMUNICACIONES.
	1 Gestión de la seguridad en las redes.
	1.1 Controles de red.
3	· Existen políticas que norman las conexiones físicas e inalámbricas.
2	· Existe un sistema adecuado de autenticación para el acceso a la red y se limita el acceso de personas autorizadas a servicios y aplicaciones legitimas.
3	· Existe un control de seguridad de red tanto a nivel de sistemas como a nivel de infraestructura.
	1.2 Mecanismos de seguridad asociados a servicios en red.
3	· Existe una gestión, clasificación y protección adecuada de los servicios de red propios y un derecho de auditoria de servicios de red de terceros.
3	· Existe un monitoreo y revisión periódica de los servicios de red y configuraciones de cortafuegos, IDS/IPS, DAM, WAF.
	1.3 Segregación de redes.
2	· Existe una política de segmentación de redes y está basada en la clasificación, nivel de confianza, dominios, etc.
2	· Existe una segregación adecuada y clara incluyendo redes de invitados y la segmentación de proveedores y clientes, la cual es controlada y monitoreada a fin de mitigar los riesgos conforme a las políticas de la organización.
	2 Intercambio de información con partes externas.

	2.1 Políticas y procedimientos de intercambio de información.
2	· Existen políticas enfocadas en la transmisión segura de información en diferentes herramientas de comunicación como son: Wifi, bluetooth, almacenamientos externos mensajería, correo electrónico, FTP, foros, servicios en la nube y similares; basados en la clasificación de información.
3	· Existe un programa de capacitación concientización y cumplimiento, siguiendo el principio de confidencialidad y privacidad.
	2.2 Acuerdos de intercambio.
3	· Las responsabilidades sobre la perdida, corrupción o divulgación de datos están claramente definidas.
2	· Se mantiene una cadena de custodia para la información y existe sincronía de los niveles de clasificación de la información por parte de todos los involucrados.
	2.3 Mensajería electrónica.
2	· Se tiene controles de seguridad adecuados para mensajería como, por ejemplo: cifrado de correo electrónico, autenticidad, confidencialidad e irrenunciabilidad de mensajes.
	2.4 Acuerdos de confidencialidad y secreto.
3	· Existen acuerdos de confidencialidad y estos están revisados y aprobados por el departamento legal, y firmados por las personas adecuadas.
2	· Existen sanciones adecuadas para el caso de incumplimiento y/o beneficios para el cumplimiento de los acuerdos.

Anexo II – Respuestas de la evaluación realizada a la organización 1 (O1)

Sentencias evaluadas	Puntuación
· Existe un inventario de activos de la información.	1
· El inventario es lo suficientemente completo, preciso, detallado y se mantiene actualizado correctamente.	1
· Los activos de información tienen un propietario y un responsable técnico	1
· Existe un sistema de asignación, etiquetado e información de incidentes para los activos de información.	0
· Existe una política que norma el uso apropiado de recursos tecnológicos como correo electrónico, mensajería, FTP, incluyendo el comportamiento del usuario en internet y redes sociales, y que además establece responsabilidades por parte del usuario.	1
· Se ha socializado correctamente lo que constituye un uso inapropiado de activos a todos los miembros de la empresa.	2
· Existe un procedimiento para recuperación de activos de información tras una baja o despido que garantiza el correcto tratamiento de los mismos.	1
· Existe un procedimiento a seguir para abordar el caso de activos de información que no han sido devueltos.	0
· Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados a la clasificación de la información. Y estas se ligan a obligaciones contractuales o legales.	2
· La clasificación se basa en los requisitos de seguridad de la información (confidencialidad, integridad, disponibilidad), y el personal está consciente de ellos.	1
· Existe un proceso de etiquetado de la información tanto física como electrónica, sincronizado con las políticas de clasificación de la información que garantiza una correcta manipulación de la información.	0
· Existen niveles de clasificación y se garantiza el acceso únicamente a aquellos con permisos de acceso aprobados.	2
· Para la manipulación de activos se tiene en consideración: Método de etiquetado, transferencia, almacenamiento, manejo de medios	1

extraíbles, eliminación de medios físicos y electrónicos, divulgación, intercambio, intercambio con terceros, traslado, etc.	
· Existe un registro detallado de medios extraíbles como CD/DVD, almacenamiento USB y demás medios extraíbles.	1
· Los medios extraíbles están correctamente etiquetados, manejados y almacenados garantizando que no exista acceso no autorizado a la información almacenada.	1
· Existe una política orientada a la eliminación de activos de información ligada a obligaciones legales y contractuales de los responsables, que permita además realizar un seguimiento del proceso de eliminación.	1
· Se tiene en cuenta la criticidad de la información para el proceso de eliminación: Respaldo de información, periodos de retención y eliminación segura (borrado criptográfico, desmagnetización, destrucción física),	1
· Se utiliza servicios de transporte confiables y mecanismos adecuados de cifrado para las transferencias de información.	2
· Se verifica la recepción en el lugar de destino de la información.	2
· Existe una política de control de acceso que contempla una asignación adecuada de deberes y un proceso documentado de control de acceso.	2
· El proceso de aprobación de acceso requiere la participación del propietario del sistema o de la información.	2
· El acceso VPN e inalámbrico esta correctamente supervisado, controlado y autorizado.	0
· Se utiliza una autenticación multi factor para acceso a redes sistemas y aplicaciones criticas.	1
· Existe un proceso de monitoreo y pruebas constante para detectar accesos no autorizados, tiempos de respuesta a incidentes, entre otros.	1
· El alta de un usuario por solicitud pasa por un proceso adecuado de aprobación y registro, y genera un ID único para cada usuario.	2
· Existe un proceso para la baja de los ID de usuario de forma inmediata tras el cese o despido o si ya no son necesarios previa confirmación.	1

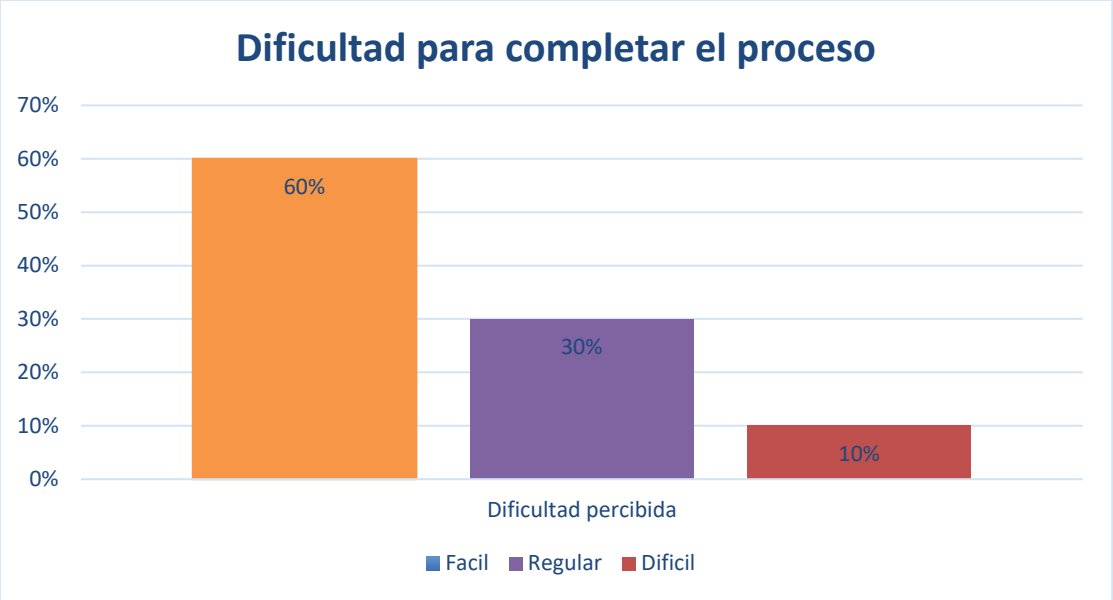
· Cada acceso a sistemas está basado en las necesidades del negocio y se corresponde con las políticas de control de acceso y segregación de funciones.	1
· Se documenta adecuadamente las solicitudes y aprobaciones de acceso.	0
· Existe un proceso periódico de revisión de cuentas con privilegios especiales que contemple, asignación y eliminación de privilegios en base a necesidades.	1
· Existe una diferenciación de usuarios con privilegios especiales, tanto en ID, caducidad de cuentas y controles más estrictos de actividades.	1
· Hay restricciones técnicas como: longitud mínima de contraseña, reglas de complejidad, cambio forzado de contraseña, autenticación en múltiples factores, etc.	1
· El utiliza cifrado en almacenamiento y manipulación de contraseñas en dispositivos, sistemas y aplicaciones.	1
· Se verifica la identidad del usuario antes de proporcionar contraseña temporal nueva y esta contraseña es suficientemente fuerte.	2
· Se revisa periódicamente los derechos de acceso de los usuarios y se lleva un registro documental de las revisiones.	0
· Las revisiones se realizan en presencia de los propietarios para verificar cambios en las funcionas para los usuarios.	1
· Existe un proceso estructurado de reasignación o eliminación de derechos de acceso en el cual se contempla el acceso tanto físico como lógico a los sistemas.	1
· Las contraseñas se eliminan o cambian inmediatamente en caso de finalización de contrato, cambio de rol etc.	1
· Existe medidas que aseguran la confidencialidad de las credenciales de autenticación y cambios de contraseña en caso de que esta se vea comprometida.	1
· Existen controles de seguridad aplicables a cuentas compartidas.	0
· Existen controles adecuados e identificación individual de cada usuario.	2
· Existe un procedimiento para definir, autorizar, asignar, revisar, gestionar y retirar los derechos de acceso y permisos asignados.	1

· Existen formas de disuadir el acceso no autorizado a los sistemas como por ejemplo: pantallas de advertencia, demoras en el sistema, bloqueos, alarmas, registros y alertas.	0
· Existen procedimientos claros para identificar la identidad del usuario que ingresa al sistema, así como autenticación multi factor para sistemas, servicios o conexiones críticas.	1
· La fortaleza de las contraseñas está establecida en estándares y políticas de la organización, y se toma en cuenta longitud mínima, restringir la reutilización de contraseñas, nivel de complejidad, cambios forzados de contraseñas, ocultamiento de la contraseña durante el tipeo.	0
· Las contraseñas se transmiten por canales seguros y cifrados.	1
· Esta claramente definido el responsable de las herramientas de administración.	2
· Se tiene claramente identificado quien, porque, para que, y en que condiciones se puede acceder a las herramientas de administración.	1
· El proceso es auditable y se genera un registro detallado de su uso.	0
· Se cuenta con un entorno de almacenaje del código fuente seguro, con limitación de acceso, monitoreo, control de versiones, registros, etc.	0
· Se tienen procesos claramente establecidos y documentados para realizar modificaciones, publicaciones y compilaciones.	1
· Se generan, almacenan y revisan los registros de acceso y cambios.	0
· Existen políticas que cubren el uso de controles criptográficos y estas se cumplen.	1
· Las políticas cubren: Casos de información que debe ser protegida con criptografía, normas que deben aplicarse, proceso basado en el riesgo para identificar la protección necesaria, cifrado para información almacenada y transferida, cumplimiento de normas y leyes aplicables, efectos del cifrado en la inspección de contenidos de software.	1
· Hay un proceso claro para abarcar todo el ciclo de vida de la gestión de claves incluida la protección del equipo utilizado para generar, almacenar y archivar las claves criptográficas.	0
· Existe un procedimiento para evitar claves débiles o repetidas.	1

· Existen reglas establecidas sobre cambio y actualización de claves.	0
· Existen políticas que norman las conexiones físicas e inalámbricas.	1
· Existe un sistema adecuado de autenticación para el acceso a la red y se limita el acceso de personas autorizadas a servicios y aplicaciones legitimas.	1
· Existe un control de seguridad de red tanto a nivel de sistemas como a nivel de infraestructura.	1
· Existe una gestión, clasificación y protección adecuada de los servicios de red propios y un derecho de auditoria de servicios de red de terceros.	0
· Existe un monitoreo y revisión periódica de los servicios de red y configuraciones de cortafuegos, IDS/IPS, DAM, WAF.	1
· Existe una política de segmentación de redes y está basada en la clasificación, nivel de confianza, dominios, etc.	0
· Existe una segregación adecuada y clara incluyendo redes de invitados y la segmentación de proveedores y clientes, la cual es controlada y monitoreada a fin de mitigar los riesgos conforme a las políticas de la organización.	0
· Existen políticas enfocadas en la transmisión segura de información en diferentes herramientas de comunicación como son: Wifi, bluetooth, almacenamientos externos mensajería, correo electrónico, FTP, foros, servicios en la nube y similares; basados en la clasificación de información.	1
· Existe un programa de capacitación concientización y cumplimiento, siguiendo el principio de confidencialidad y privacidad.	2
· Las responsabilidades sobre la perdida, corrupción o divulgación de datos están claramente definidas.	1
· Se mantiene una cadena de custodia para la información y existe sincronía de los niveles de clasificación de la información por parte de todos los involucrados.	0
· Se tiene controles de seguridad adecuados para mensajería como, por ejemplo: cifrado de correo electrónico, autenticidad, confidencialidad e irrenunciabilidad de mensajes.	0

· Existen acuerdos de confidencialidad y estos están revisados y aprobados por el departamento legal, y firmados por las personas adecuadas.	0
· Existen sanciones adecuadas para el caso de incumplimiento y/o beneficios para el cumplimiento de los acuerdos.	0

Anexo III – Resultados de encuesta de dificultad realizada a los participantes.



Normativa N° CD-03-2016, julio 2016.