MAESTRÍA EN AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN

PROPUESTA DE UN MARCO DE TRABAJO PARA LA EVALUACIÓN DE MADUREZ DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN UN RETAIL DE LA CIUDAD DE GUAYAQUIL

Propuesta de artículo presentado como requisito para la obtención del título:

Magister en Auditoría de Tecnologías de la Información

Por los estudiantes:

Juan Antonio ASTUDILLO HERRERA

Salvattore Giulliano STRACUZZI PÁSTOR

Bajo la dirección de:

Gary Xavier REYES ZAMBRANO

Universidad Espíritu Santo
Facultad de Postgrado
Guayaquil– Ecuador
2019

Propuesta de un Marco de Trabajo para la Evaluación de Madurez de la Gestión de Seguridad de la Información en un Retail de la Ciudad de Guayaquil

Proposal of a Framework for the Evaluation of Maturity of the Information Security Management in a Retail of Guayaquil City.

Juan Antonio ASTUDILLO HERRERA [1]

Salvattore Giulliano STRACUZZI PÁSTOR [2]

Gary Xavier REYES ZAMBRANO [3]

Resumen

El objetivo general de este artículo fue diseñar un marco de trabajo que permita evaluar el nivel de madurez de la gestión de seguridad de la información (GSI) en una organización especializada en la comercialización masiva de productos (RETAIL) de la ciudad de Guayaquil para proveer elementos de juicio que permitan conocer el estado de sus procesos principales de negocio con relación a la seguridad de la información (SI). El enfoque es cualitativo, con un alcance descriptivo basado en la revisión de modelos de evaluación de madurez en conjunto con normas para GSI. Los resultados obtenidos identifican un nivel bajo de madurez de los procesos principales de negocio del RETAIL.

Palabras clave:	Nivel de Madurez, GSI, Marco de TI

Abstract

The general objective of this article was to design a framework for evaluating the level of maturity of information security management (ISM) in an organization specialized in the mass commercialization of products (RETAIL) in the Guayaquil city to provide evidence that they know the status of their main business processes with relation to information security (IS). The approach is qualitative, with a descriptive scope based on the revision of maturity assessment models in conjunction with ISM standards. The results obtained identify a low level of maturity of the main business processes of the RETAIL.

Key words	Maturity level, ISM, IT framework

[1]Maestrante en Auditoría de Tecnologías de Información, Universidad Espíritu Santo - Ecuador. E-mail jastudilloh@uees.edu.ec

[2]Maestrante en Auditoría de Tecnologías de Información, Universidad Espíritu Santo - Ecuador. E-mail sstracuzzi@uees.edu.ec

[3]Magister en Administración de Empresas, Profesor Universidad Espíritu Santo - Ecuador. E-mail xreyes@uees.edu.ec

INTRODUCCIÓN

En vista de los constantes avances tecnológicos y la criticidad de la información que se procesa en la actualidad muchas organizaciones no consideran a la seguridad de la información (SI) como una barrera o un costo de tecnologías de la información (TI), sino como una herramienta para facilitar su crecimiento y construir una reputación corporativa (Villafañe, 2015), un estudio realizado por la firma PriceWaterhouseCooper (2017), demuestra como a nivel mundial el 46% de las organizaciones consideran como prioridad de inversión gestionar nuevos marcos y modelos de seguridad en relación a la evolución de los modelos de negocios, así mismo, evidencia como el 62% de las organizaciones utilizan servicios de seguridad para la administración de ciberseguridad y privacidad.

De igual manera, un estudio efectuado en Latinoamérica por la firma Deloitte (2016), demuestra que el 84% de las organizaciones cuentan con un ejecutivo responsable de gestionar los ciber-riegos y la SI, y, un 43% mantienen una estrategia contra ciber-riesgos y la SI debidamente documentada y aprobada, razón por lo cual, se torna evidente la evolución que ha tenido en los últimos años la GSI a través de marcos de trabajo para gobierno y riesgos, tanto a nivel corporativo como de TI, evidenciando la necesidad de ser precisos respecto a la manera en cómo debe llevarse a cabo dicha gestión con la finalidad de asegurar el cumplimiento de los objetivos del negocio (Arbeláez, 2008; Ardita, 2013; Cárdenas-Solano, Martínez-Ardila, & Becerra-Ardila, 2016; Mesquida, Mas, & Amengual, 2009; Montaño Arango, Corona Armenta, & Medina Marín, 2008).

Los marcos de trabajo anteriormente mencionados se amparan en buenas prácticas (best practices por su terminología en inglés) definidas por la Cambridge University Press (2019), como un método de trabajo o conjunto de métodos de trabajo que se aceptan oficialmente como el mejor uso en un negocio o industria en particular, generalmente descritos de manera formal y detallada; bajo este contexto, las buenas prácticas internacionales para la GSI contienen experiencias combinadas de muchas compañías influyentes en relación a medidas de control relevantes, procedimientos y técnicas que suministran niveles de seguridad, así mismo, proveen un marco de trabajo referencial para cubrir las bases de la SI en una organización (Ducuara Cruz & Moya Molano, 2017; Velásquez Pérez, Puentes Velásquez, & Pérez Pérez, 2015; Von-Solms, 2001, 2006).

Uno de los documentos más destacados referentes a estas buenas prácticas según la revisión bibliográfica realizada por Cárdenas-Solano et al. (2016), es la serie ISO/IEC 27000, también conocido como la familia de estándares del sistema de gestión de seguridad de la información (SGSI), estos documentos ofrecen sugerencias, plantean riesgos y controles aplicables a todas las organizaciones, independientemente de su tipo, tamaño y naturaleza (iso27000.es, 2019).

De manera similar, otro documento destacado es el estándar NIST SP 800-53 proporcionado por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el cual, es requerido por las agencias federales de Estados Unidos, y, del mismo modo, puede ser utilizado por cualquier organización para elaborar un plan de SI relativo a tecnologías (Varonis, 2018). Estos documentos anteriormente mencionados apoyan a la gestión de un profesional de seguridad en la elaboración de programas y/o marcos de trabajo para la GSI (Ducuara Cruz & Moya Molano, 2017; Granneman, 2013; Gutiérrez Beltrán & Alonso Ricardo, 2019).

Estudios previos como Hong et al. (2003), demuestran que estos programas y/o marcos de trabajo son escasos, puesto que mencionan que la ausencia de estos documentos en conjunto con una metodología aportan a la falta de conocimientos referentes a la GSI. Del mismo modo, Entrust (2004), sugiere que existen pocos marcos de trabajo referentes a la SI que permitan guiar de forma adecuada a las organizaciones con relación

a la GSI, evidenciando la necesidad de elaborar este tipo de documentos para la GSI enfocados a una organización o giro de negocio en específico.

La elaboración de estos marcos de trabajo puede ser asociada a modelos de madurez que permitan identificar de mejor manera el estado en el que se encuentra una organización con relación a la GSI, un estudio realizado por Rosmiati, Riadi, & Prayudi (2016), evidencia la utilización de un marco detallado por niveles basados en el modelo de capacidad y madurez (CMM por sus siglas en inglés), posteriormente devenido como integración de modelo de capacidad y madurez (CMMI por sus siglas en inglés), permitiendo asociar por escalas su aplicación para la GSI. Así mismo, otros estudios demuestran que la aplicación del modelo CMMI permite evaluar la GSI en todos sus aspectos, dando a conocer el estado en el que se encuentran los procesos de una organización permitiendo establecer metas para avanzar por cada nivel del modelo (Kurniawan & Riadi, 2018; Maggiore, 2014; Matrane & Talea, 2014; Van Os, 2016).

Todo lo expuesto anteriormente, permite definir como problema de esta investigación la deficiente aplicación de marcos de trabajo que permitan identificar el nivel de madurez de los procesos en una organización con relación a la GSI.

Por lo tanto, el objetivo general de este artículo consiste en diseñar un marco de trabajo que permita identificar el nivel de madurez de la GSI en un RETAIL de la ciudad de Guayaquil. El conocimiento del nivel de madurez proveerá elementos de juicio que permitirá conocer el estado de los principales procesos del negocio con relación a la GSI.

El enfoque utilizado en la metodología de investigación fue cualitativo, con un alcance descriptivo y su tipo de razonamiento es deductivo. Se elaboró un listado de puntos de atención basados en el marco de trabajo desarrollado, el cual, posee lineamientos de los estándares ISO/IEC 27000 y NIST SP 800-53. Para determinar el nivel de madurez se aplicó el modelo CMMI. La validación del marco de trabajo fue realizada por un juicio de expertos y para su aplicación se seleccionó un RETAIL de la ciudad de Guayaquil. Los procesos seleccionados de la organización fueron determinados en función de su cadena de valor, los cuales contemplan aspectos con relación a la GSI (Velásquez Pérez et al., 2015).

En este documento se realizará una revisión del concepto de la GSI, los estándares ISO/IEC 27000 y NIST SP 800-53, el modelo de madurez CMMI y sus niveles, luego se procederá a aplicar el instrumento, analizar los resultados obtenidos y formular las respectivas conclusiones y recomendaciones. Adicionalmente se cuenta con dos apartados: bibliografía con todas las fuentes que alimentaron la investigación y anexos en los que se incluyen el instrumento aplicado y los permisos obtenidos para la investigación.

REVISIÓN DE LA LITERATURA

Gestión de la Seguridad de la Información

La SI en sus comienzos tuvo un abordaje netamente tecnológico puesto que era el enfoque que prevalecía respecto al uso de la información. A pesar de las regulaciones y normas emitidas respecto de la necesidad de contar con políticas, programas, procesos de evaluación de riesgos, las organizaciones no han logrado un control eficaz de diferentes escenarios que son objeto de tratamiento por parte de la GSI (Solarte Solarte, Enriquez Rosero, & Benavides Ruano, 2015).

Esta falta de control se ve reflejada cada vez que existen nuevos ataques informáticos que afectan los factores de la SI (confiabilidad, disponibilidad e integridad). Como premisa para mejorar la situación, el Instituto de Gobernabilidad de TI (ITGI por sus siglas en inglés) creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA por sus siglas en inglés) sostiene que la SI concierne a todas las personas y procesos de la información, física y electrónica, independientemente de si involucran personas y tecnología o relaciones con socios comerciales, clientes y terceras partes, de igual manera, a la protección total

en todos los puntos dentro del ciclo de vida de la información utilizada en la organización (ISACA, 2019).

Así mismo, el Equipo de Respuesta ante Emergencias Informáticas (CERT por sus siglas en inglés) perteneciente al Instituto de Ingeniería de Software (SEI por sus siglas en inglés) administrado por la Universidad Carnegie Mellon quien avala al CMMI, expresa lo siguiente: "*Gobernar para la seguridad de la empresa significa entender que la adecuada seguridad es un requerimiento del que no se puede prescindir para hacer negocios. Si la dirección de una organización no establece y no refuerza la necesidad que tienen los negocios de una efectiva seguridad de la empresa, el estado deseado de seguridad no será articulado, alcanzado ni sostenido en el tiempo. Para alcanzar una capacidad sustentable las organizaciones deben hacer responsable de la seguridad empresarial a líderes del nivel de gobierno, no a otros roles organizacionales que carecen de autoridad, responsabilidad y recursos para actuar y hacer cumplir las regulaciones*" (SEI, 2012).

De manera similar, se complementa con la propia norma ISO/IEC 27001, la cual, en su introducción define: "*Es importante que el sistema de gestión de seguridad de la información sea parte y esté integrado en los procesos organizacionales y en la estructura global, y que sea considerado en el diseño de los procesos, los sistemas de información y los controles*" (ISO, 2019b).

En consecuencia, estas publicaciones muestran que la SI debe integrarse en los procesos de negocio y está involucrada en los aspectos internos y externos de una organización, por lo cual, su adecuada gestión empieza con el compromiso de la alta gerencia en establecer lineamientos que permitan cumplir los requerimientos que conlleva su implementación.

Por otra parte, la GSI no es responsabilidad únicamente para organizaciones grandes con Tecnologías de Información y Comunicación (TIC por sus siglas en inglés) avanzadas. Se debe tener en cuenta que la SI alcanza a todo tipo y envergadura de organizaciones, por lo tanto, no es proporcional al tamaño de las mismas, sino que tiene relación con la sensibilidad y criticidad de la información de los procesos que maneja, así como cuán avanzadas se encuentran con el uso de las TIC (Maggiore, 2014).

Además, la GSI permite implementar la SI donde realmente se justifica, debido a que su ausencia pondría a la organización en una situación de riesgo cuya cristalización puede provocar un impacto económico perjudicial. De hecho, el alcance de controles establecidos por algunas normas excede lo tecnológico, puesto que existen apartados referidos a la organización, RRHH, cumplimientos regulatorios, entre otros (Westerman & Richard, 2007).

En conclusión, la GSI está inmersa en todo tipo y tamaño de organizaciones, por lo cual, es importante realizar una adecuada implementación de la SI empezando por los procesos que agreguen valor, considerando que de no ser efectiva su implementación los riesgos que podrían suscitarse ocasionarían impactos económicos negativos en la organización.

ISO/IEC 27000

La familia de estándares ISO/IEC 27000 27001, 27002, 27003, 27004, 27005, entre otros, son un conjunto de pautas desarrollados por la Organización Internacional de Estandarización (ISO por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC por sus siglas en inglés), que proporcionan un marco de gestión de la SI disponible por cualquier tipo de organización, pública o privada, de cualquier tamaño (iso27000.es, 2019).

Por tanto, el estándar ISO/IEC 27000 posee un vocabulario general para un SGSI. ISO/IEC 27001 detalla los requisitos para la implantación del SGSI, puesto que adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. ISO/IEC 27002 es código de buenas prácticas para la GSI. ISO/IEC 27003 son directrices para una implementación. ISO/IEC 27004 son métricas para la GSI. ISO/IEC 27005 refiere a la gestión de riesgos en la SI (López Armendáris, 2017).

De igual manera, el estándar ISO/IEC 27001 consiste en la conservación de la confidencialidad, integridad y disponibilidad, así como, de los sistemas implicados en su tratamiento dentro de una organización. El objetivo es que las organizaciones puedan garantizar la optimización de riesgo menor que el soportado, para preservar la confidencialidad, integridad y disponibilidad de la información. Esta norma contiene las mejores prácticas para desarrollar, implementar y mantener especificaciones para los SGSI (Fernández, Gómez, & Álvarez, 2012; ISO, 2019b).

Para concluir, el estándar ISO/IEC 27001 es aplicable a cualquier tipo de organización, la norma posee un conjunto de buenas prácticas que permite realizar una adecuada gestión de la SI.

NIST SP 800-53

La NIST es una agencia no reguladora del Departamento de Comercio de los Estados Unidos encargada de investigar y establecer estándares en todas las agencias federales. NIST SP 800-53 define los estándares y pautas para que las agencias federales diseñen y administren sus sistemas de seguridad de la información. Se estableció para proporcionar orientación para la protección de datos privados de agencias y ciudadanos (Varonis, 2018).

Otro aspecto de NIST SP 800-53 es que establece estándares básicos para las políticas de seguridad de la información para las agencias federales, se creó para mejorar la seguridad (y la política de seguridad) de los sistemas de información utilizados en el gobierno federal. Por consiguiente, ayuda a explicar qué estándares se aplican a cada objetivo, y proporciona orientación sobre cómo implementarlos, razón por la cual, puede ser utilizado por cualquier organización para construir un plan de seguridad de la información relativo a tecnologías (Cárdenas-Solano et al., 2016; Varonis, 2018).

En conclusión, NIST SP 800-53 posee un conjunto de pautas que apoyan a la GSI y son adaptables a cualquier tipo de organización.

Modelo de Madurez

CMMI

Según el SEI (2019), existen tres dimensiones críticas en las que las organizaciones se focalizan:

1. Personas.
2. Procedimientos y métodos.
3. Herramientas y equipamiento.

Sin embargo, afirma que lo que sustenta todo este conjunto son los procesos, puesto que permiten alinear las actividades estableciendo la infraestructura necesaria para hacer frente a un mundo en constante evolución, maximizando la productividad de personas y utilizando la tecnología para crecer en competitividad.

Basado en estos principios, el SEI desarrolló modelos de capacidad y madurez (CMMI por sus siglas en inglés) que proponen dos caminos: el modelo de capacidad y el modelo de madurez. La diferencia más importante entre ambos es que el modelo de capacidad puede ser usado para la mejora de un área de proceso individual o un conjunto de ellas, mientras tanto, el modelo de madurez establece que cada nivel será alcanzado cuando se mejoren las áreas de proceso pertenecientes a un subconjunto previamente definido para dicho nivel (Maggiore, 2014).

El modelo de madurez según Matrane & Talea (2014), permite aplicar:

1. Técnicas de procesos, proyectos y organizaciones.
2. Métodos de evaluación para conocer la madurez de un proceso.

Por consiguiente, el modelo CMMI posee cinco niveles que permiten demostrar el nivel de madurez de un proceso. Según el SEI (2010), estos son:

- **Nivel 1 – Inicial**: Demuestra que todas las prácticas básicas se realizan de manera informal, lo que significa que no hay documentación, no hay estándares y se realizan por separado.
- **Nivel 2 – Gestionado**: Planificado y rastreado, que indica los estándares

del proceso de planificación de compromisos.

- **Nivel 3 – Definido**: Significa que el proceso estándar se ha ejecutado acorde a su definición.
- **Nivel 4 – Gestionado Cuantitativamente:** Control cuantitativo, lo que indica una mejor calidad a través del monitoreo de cada proceso.
- **Nivel 5 – En optimización:** Mejora constante, lo que demuestra que el estándar ha sido perfecto y su enfoque permite adaptarse a los cambios.

El modelo CMMI se utiliza al dar la evaluación de la puntuación en cada área del proceso que se seleccione entre 1 y 5 (Supriyatna, 2014).

En consecuencia, el modelo CMMI puede utilizarse para medir la madurez de un proceso mediante los cinco niveles que dispone, permitiendo establecer lineamientos para mejorar el proceso analizado.

Por lo descrito anteriormente en la revisión de literatura se puede evidenciar la relevancia que tiene la SI en las organizaciones y de igual manera la importancia de realizar adecuadamente una GSI amparada en estándares como ISO/IEC 27000, NIST SP 800-53 y modelos como el CMMI, los cuales son respaldados por organismos internacionales.

METODOLOGÍA DE LA INVESTIGACIÓN

A. Desarrollo del marco de trabajo

a. Correlación de estándares

Con base en la revisión bibliográfica de la presente investigación, se seleccionaron los estándares ISO/IEC 27000 y NIST SP 800-53 para el diseño del marco.

Respecto al estándar ISO/IEC 27000 se escogió la norma ISO/IEC 27001:2013 por ser la versión más actual según su sitio oficial, con relación a los dominios que posee la norma se consideran los 14 dominios aplicables en una implementación de SGSI, estos son del A5 al A18 los cuales se describen en la tabla 1 (ISO, 2019a).

Tabla 1. Dominios ISO/IEC 27001:2013

Dominio	Descripción
A5	Políticas de seguridad de la información
A6	Organización de la seguridad de la información
A7	Seguridad relativa a los recursos humanos
A8	Gestión de activos
A9	Control de acceso
A10	Criptografía
A11	Seguridad física y del entorno
A12	Seguridad de las operaciones
A13	Seguridad de las comunicaciones
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información
A15	Relación con proveedores
A16	Gestión de incidentes de seguridad de la información
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio
A18	Cumplimiento

Fuente: (ISO, 2019a)

De manera similar, para el estándar NIST SP 800-53 se utilizó el marco para la mejora de seguridad cibernética en infraestructuras críticas en su versión 1.1 la cual según el sitio oficial de NIST es la más actualizada, del marco indicado se consideran todas sus funciones, mismas que se describen en la tabla 2 (NIST, 2018).

Tabla 2. Identificadores únicos de función NIST SP 800-53

Identificador	Función
ID	Identificar
PR	Proteger
DE	Detectar
RS	Responder
RC	Recuperar

Fuente: (NIST, 2018)

Como análisis inicial se realizó una correlación entre los estándares descritos anteriormente asociando los dominios correspondientes a la norma ISO/IEC 27001:2013 con las funciones del estándar NIST SP 800-53 (Anexo 1).

Seguidamente, como resultado de la correlación de los estándares se elaboraron 342 puntos de atención que permiten identificar la GSI en una organización (Anexo 2).

b. Modelo de madurez

Se realizó la selección del modelo de madurez CMMI para la gestión y control de los procesos de la organización, que puedan evaluarse desde el nivel 1 (inicial) hasta el nivel 5 (en optimización). Permitiendo identificar la existencia de problemas y cómo determinar la prioridad de mejora (Rosmiati et al., 2016).

Para obtener los resultados del valor del nivel de madurez se tomó como referencia el índice de madurez según lo especificado en la Tabla 3 (Gusti Ayu, I Made, & Agung B, 2005).

Tabla 3. Criterios de evaluación del nivel de madurez

Índice de madurez	Nivel de Madurez
1.00 – 1.50	1 – Inicial
1.51 – 2.50	2 – Gestionado
2.51 – 3.50	3 – Definido
3.51 – 4.50	4 – Gestionado Cuantitativamente
4.51 – 5.00	5 – En Optimización

Con relación a las técnicas de medición descriptivas, estas se realizan según el tamaño nominal para ordenar los objetos desde el más bajo al más alto, puesto que sólo dan el rango de orden. Las mediciones se llevaron a cabo directamente a partir de datos que hacen referencia a los valores del modelo de madurez en orden de salida tal como se muestran en la Tabla 4 (Erniwati & Hikmawati, 2015).

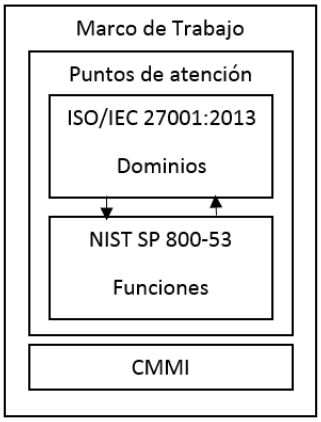
Tabla 4. Nivel de madurez

Nivel de Madurez	Descripción
1 – Inicial	La organización tiene un enfoque ad-hoc o desestructurado en esta práctica o estándar.
2 – Gestionado	La organización tiene un enfoque consistente, pero en su mayoría no está documentado.
3 – Definido	La organización aplica un enfoque detallado, documentado. Pero no medido ni reforzado.
4 – Gestionado Cuantitativamente	La organización regularmente mide su cumplimiento y hace mejoras al proceso de forma regular.
5 – En Optimización	La organización ha refinado su cumplimiento a un nivel de buena práctica.

c. Instrumento

Se procedió a elaborar el marco de trabajo uniendo la correlación de los estándares realizada en el literal a, especificando por cada punto de atención propuesto el modelo CMMI indicado en el literal b, permitiendo describir en cada punto su respectiva valoración (Anexo 3). La imagen descrita a continuación representa el marco de trabajo elaborado.

Imagen 1. Marco de trabajo elaborado



Fuente propia

B. Validación del marco de trabajo

La técnica aplicada para realizar la validación del marco de trabajo propuesto se efectuó mediante el método Delphi, el cual, permite obtener la opinión de un grupo de expertos a través de una consulta reiterada, por lo tanto, su evaluación es de carácter cualitativo. Previo a la aplicación del método descrito se debe realizar la selección de expertos en los temas concernientes a la presente investigación, a los cuales se les determinará un coeficiente de competencia que permita corroborar dichos conocimientos. (Torrado-fonseca, 2016).

a. Selección de expertos

Según la Universitat de Barcelona (2019), el coeficiente de competencia presenta las siguientes variables:

- kc = Coeficiente de conocimiento.
- ka = Coeficiente de argumentación.
- k = Coeficiente de competencia.

Por consiguiente, para determinar el coeficiente de competencia se debe aplicar la siguiente condición:

- 0,8 < k < 1,0: Coeficiente de Competencia Alto.
- 0,5 < k < 0,8: Coeficiente de Competencia Medio.
- k < 0,5: Coeficiente de Competencia Bajo.

A continuación, se presentan los resultados obtenidos en la Tabla 5 del coeficiente de competencia realizado a seis expertos con experiencia en las áreas de: SI, Ciberseguridad y Modelos de Madurez (Anexo 4).

Tabla 5. Coeficiente de competencia aplicado a expertos seleccionados

Experto	kc	ka	k	Competencia
Catania Játiva	0.9	1	0.95	Alta
Susan Noboa	0.93	1	0.97	Alta
Jaime De La Cuadra	0.67	0.8	0.74	Media
Jorge Romero	0.93	0.9	0.92	Alta
Javier Baquero	0.87	1	0.94	Alta
María Elena Ríos	0.67	0.8	0.74	Media

Fuente propia

En conclusión, los resultados obtenidos del coeficiente de competencia reflejan que de los seis expertos seleccionados, cuatro presentan un nivel alto de competencia en las áreas de conocimiento de la presente investigación, razón por lo cual, procedieron a validar el marco propuesto mediante la aplicación del método Delphi.

b. Validación del marco de trabajo – Método Delphi

Se elaboró la versión inicial de un cuestionario para ratificar el marco de trabajo propuesto, el cual, fue sometido a la revisión del grupo de expertos seleccionados en el paso previo, lo que arrojó el listado de ítems a considerar para la validación del marco de trabajo.

Tabla 6. Ítems para validación del marco de trabajo

No.	Ítem
1	¿El Marco de trabajo cubre la integridad, confidencialidad y disponibilidad de la información?
2	¿El marco de trabajo define correctamente el nivel de madurez de la Empresa?
3	¿El marco de trabajo asocia correctamente las normas de

	ciberseguridad con las normas de Seguridad de la Información?
4	¿El marco es claro en sus preguntas para conocer la madurez de los procesos?
5	¿Está de acuerdo con el nivel de madurez definido?
6	¿Considera que las preguntas apuntan a mejoras dentro del proceso de Seguridad de la Información?

Fuente propia

Una vez modificado el cuestionario a partir de las consideraciones obtenidas como resultado de la primera ronda, se sometió el mismo a una segunda ronda de consulta al grupo de expertos seleccionados cuyos resultados cuantitativos de las valoraciones pueden variar en una escala de 1 (inadecuado) a 5 (muy adecuado). Los datos se procesaron mediante análisis estadístico aplicando las técnicas descritas en el método (Blasco Mira, López Padrón, & Mengual Andrés, 2010).

Tabla 7. Valoraciones de Ítems

Ítem	Valoración				
	MA	BA	A	PA	I
1	4				
2	4				
3	4				
4	4				
5	4				
6	4				

Leyenda:
MA = Muy adecuado, BA = Bastante adecuado, A = Adecuado, PA = Poco adecuado, I = Inadecuado

Fuente: Tabulación de resultados (Anexo 5)

En conclusión, los resultados obtenidos del método Delphi reflejan que los cuatro expertos seleccionados concuerdan al 100% en los seis ítems del cuestionario elaborado, obteniendo una valoración de "*muy adecuado*" en referencia del marco de trabajo propuesto, expresando su conformidad con lo realizado (Anexo 5).

C. Selección de organización y procesos de negocio

Para la aplicación del marco propuesto, se seleccionó un RETAIL domiciliado en la ciudad de Guayaquil debido a la apertura de la organización para su ejecución. Los procesos seleccionados fueron determinados en función de su cadena de valor, la cual, según Porter (1985), permite identificar las actividades que la organización realiza de forma exclusiva o con mayor eficiencia que la competencia, y que son percibidas como importantes por los clientes.

En base a lo expuesto, los procesos determinados como principales según la cadena de valor de la organización y a los cuales se les requirió determinar el análisis de la SI son los siguientes:

Tabla 8. Procesos principales de la organización

Identificador	Descripción
P1	Compras locales
P2	Ventas RETAIL
P3	Crédito y Cobranzas

Fuente: Cadena de Valor (Anexo 6)

ANÁLISIS DE LOS RESULTADOS

Se ejecutó el marco elaborado a los 3 procesos seleccionados para determinar su nivel de madurez, validando cada uno de los puntos de atención con relación a la información proporcionada por la organización, como resultante, se estableció un valor promedio de los 3 procesos previamente mencionados por cada uno de los dominios que posee el marco, obteniendo un total de 25.8, este valor fue dividido por 14, que es el total de dominios que posee el marco, con lo cual, se evidencia un nivel de madurez de 1.8 con relación a la GSI en sus 3 procesos mencionados.

A continuación, la Tabla 9 e Imagen 2 presentan el detalle del promedio obtenido del nivel de madurez de los 3 procesos seleccionados por cada dominio del marco propuesto.

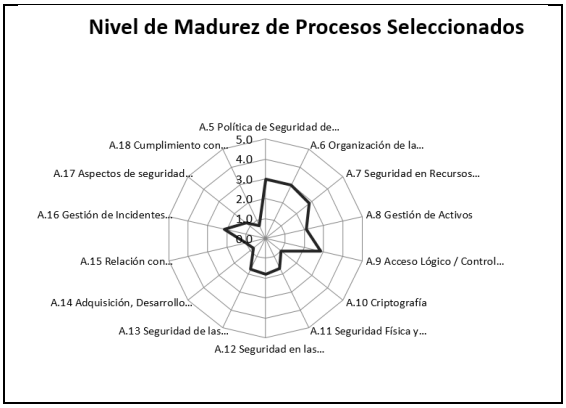
Tabla 9. Nivel de madurez por dominio del marco propuesto

Dominio	Nivel de madurez
A5. Políticas de seguridad de la información.	3.0
A6. Organización de la seguridad de la información.	3.0
A7. Seguridad relativa a los	2.8

recursos humanos.	
A8. Gestión de activos.	2.1
A9. Control de acceso.	2.9
A10. Criptografía.	1.0
A11. Seguridad física y del entorno.	1.7
A12. Seguridad de las operaciones.	1.8
A13. Seguridad de las comunicaciones.	1.7
A14. Adquisición, desarrollo y mantenimiento de los sistemas de información.	0.8
A15. Relación con proveedores.	1.0
A16. Gestión de incidentes de seguridad de la información.	2.1
A17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio.	1.3
A18. Cumplimiento.	0.7
Total	**25.8**
Promedio	**1.85**

Fuente propia

Imagen 2. Nivel de madurez por dominio del marco propuesto



Fuente propia

Los resultados presentados evidencian que la organización posee un nivel 2 (Gestionado) de madurez con relación a la GSI en sus procesos seleccionados, por lo cual, se puede concluir que tiene un enfoque consistente, pero en su mayoría no está documentado.

CONCLUSIONES

El presente trabajo de investigación proporcionó elementos de juicio que permitieron conocer el estado de los procesos principales de negocio en la organización seleccionada con relación a la SI, para esto se utilizó el marco propuesto amparado en la GSI como referencia para la validación de información por medio de puntos de atención.

Los puntos de atención definidos en el marco fueron producto de la correlación de las normas ISO/IEC 27001:2013 y NIST SP 800-53, y, a su vez, se pudieron combinar mediante la aplicación de niveles de madurez en función del modelo CMMI. La confiabilidad de los resultados obtenidos en el marco a partir de su validación por un grupo de expertos mediante el método Delphi es alta, puesto que mediante la aplicación del coeficiente de competencia se pudo constatar un alto nivel de experiencia de las personas seleccionadas en los temas tratados.

Los resultados obtenidos del nivel de madurez presentados en esta investigación soportan y certifican que las organizaciones requieren elaborar marcos de trabajo que permitan establecer lineamientos para la administración, control y seguimiento de la GSI, y, del mismo modo, demuestran que es conveniente relacionar estos marcos con modelos de madurez para identificar de una forma clara y precisa el estado en el que se encuentran cada uno de sus procesos de negocio, dejando la posibilidad de establecer compromisos para su mejoramiento.

FORTALEZAS Y LIMITACIONES

La principal fortaleza de la presente investigación fue la apertura de la organización y las facilidades que se brindaron para la ejecución del marco y la obtención de información de soporte para los puntos de atención. Así mismo, fue importante la predisposición e interés que demostraron los jefes de las áreas involucradas en conocer los resultados del estudio para establecer hitos de mejoramiento en relación a la GSI.

Una de las principales limitaciones es que la ejecución del marco fue realizada a una sola organización con un giro de negocio en específico, y, de igual manera, a un número limitado de procesos, lo cual impidió conocer el nivel de madurez de toda la organización con relación a la GSI.

FUTURAS LÍNEAS DE INVESTIGACIÓN

Para futuros estudios que surgen de la presente investigación se puede tomar como referencia el marco planteado para ser ejecutado a todos los procesos de una organización que posea el mismo giro de negocio que la organización seleccionada, o, a su vez, direccionar la investigación hacia otros negocios, pudiéndose realizar una comparación de niveles de madurez por giros de negocio para determinar en qué nichos la GSI se presenta con mayor vulnerabilidad.

Otro punto importante a considerar y que sería de gran aporte, es referenciar el marco con otros estándares aplicables a la GSI, con la finalidad de identificar puntos de atención que no hayan sido identificados por el marco propuesto en esta investigación.

RECOMENDACIONES

Según lo mencionado y analizado anteriormente se recomienda:

- Elaborar marcos de trabajo para la GSI alineados a una organización o giro de negocio en específico, que posean una combinación con modelos de madurez para identificar de una mejor manera el estado de los procesos de negocios.
- Fomentar líneas de investigación que permitían cuantificar los beneficios que adquiere una organización al implementar marcos de trabajo que apoyen a la administración, control y seguimiento de la GSI.
- Aplicar el estudio adicionando hitos que permitan identificar por punto de atención las mejoras que la organización debería implementar para incrementar su nivel de madurez.

BIBLIOGRAFÍA

Arbeláez, R. (2008). *Modelos de Madurez de Seguridad de la Información: cómo debe evolucionar la seguridad en las organizaciones*. Colombia.

Ardita, J. C. (2013). Nivel de madurez de seguridad en las Instituciones Financieras. *CYBSEC Security Systems*. Paraguay.

Blasco Mira, J. E., López Padrón, A., & Mengual Andrés, S. (2010). Validación Mediante Método Delphi De Un Cuestionario Para Conocer Las Experiencias E Interés Hacia Las Actividades Acuáticas Con Especial Atención Al Windsurf. *Ágora Para La Educación Física Y El Deporte*, *12*(1), 75–96.

Cambridge University Press. (2019). Cambridge Dictionary. Retrieved from https://dictionary.cambridge.org/dictionary/english/best-practice

Cárdenas-Solano, L.-J., Martínez-Ardila, H., & Becerra-Ardila, L.-E. (2016). Gestión de seguridad de la información: revisión bibliográfica. *El Profesional de La Información*, *25*(6), 931–948. https://doi.org/10.3145/epi.2016.nov.10

Deloitte. (2016). *La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte 2016 Cyber Risk Information Security Study - Latinoamérica - Resultados Generales vf (Perú).pdf

Ducuara Cruz, A. Y., & Moya Molano, J. A. (2017). MANUAL DE BUENAS PRACTICAS SOBRE LA SEGURIDAD DE LA INFORMACIÓN SENSIBLE DE LA ENTIDAD DEL DANE. *INSTITUCIÓN UNIVERSITARIA POLITECNICO GRANCOLOMBIANO, FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS, ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN*, (6), 67–72.

Entrust. (2004). Information security governance (ISG). An essential element of corporate governance. Retrieved from Entrust securing digital identities & information website: https://www.entrust.com/wp-content/uploads/2013/05/wp_entrust_isg_april04.pdf

Erniwati, S., & Hikmawati, N. K. (2015). An Analysis of Information Technology on Data Processing by using Cobit Framework. *(IJACSA) Intermasional Journal of Advanced Computer Science and Application*, *6*(9), 151 – 157.

Fernández, Gómez, L., & Álvarez, A. A. (2012). *Guía de aplicación de la Norma UNE - ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. España.

Granneman, J. (2013). IT security frameworks and standards: Choosing the right one. Retrieved from TechTarget search se- curity, Sept website: http://searchsecurity.techtarget.com/tip/IT-security- frameworks-and-standards-Choosing-the-right-one

Gusti Ayu, T., I Made, S., & Agung B, I. P. (2005). Governance Audit of Application Procurement Using Cobit Framework. *Journal of Theoretical and Applied Information Technology (JATIT)*, *59*(2), 342 – 351. https://doi.org/1992-8645.2005

Gutiérrez Beltrán, D. P., & Alonso Ricardo, C. A. (2019). ELABORACIÓN DE UN INSTRUMENTO BASADO EN LA UNIFICACIÓN DE LOS ESTÁNDARES PCI DSS 3.2, FRAMEWORK DE CIBERSEGURIDAD VERSIÓN 1.1 Y NTC-ISO-IEC 27001:2013 ESTABLECIENDO EL ESTADO ACTUAL Y PROPONIENDO MEDIDAS PARA EL FORTALECIMIENTO DE LA SEGURIDAD DE LA INFOR. *UNIVERSIDAD PILOTO DE COLOMBIA, FACULTAD DE INGENIERÍA, ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA*.

Hong, Kwo-Shing; Chi, Yen-Ping; Chao, Louis R.; Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243–248. https://doi.org/10.1108/09685220310500153

ISACA. (2019). ITGI. Retrieved from http://www.isaca.org/ITGI/Pages/default.aspx

ISO. (2019a). ISO/IEC 27001:2013. Retrieved from https://www.iso.org/standard/54534.html

ISO. (2019b). *ISO 27001*. Retrieved from http://www.iso.org/iso/iso27001

iso27000.es. (2019). ISO 27000. Retrieved from http://www.iso27000.es/download/doc_iso27000_all.pdf

Kurniawan, E., & Riadi, I. (2018). Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *2*(1), 12. https://doi.org/10.29407/intensif.v2i1.11830

López Armendáris, D. N. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica ESPOL – RTE*, *30*(Mayo), 51–69. Retrieved from http://rte.espol.edu.ec/index.php/tecnologica/article/view/581/356

Maggiore, M. L. (2014). *Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio*. Universidad de Buenos Aires.

Matrane, O., & Talea, M. (2014). A Maturity Model for Information Security Management in Small and Medium-Sized Moroccan Enterprises: An Empirical Investigation. *International Journal of Advanced Research in Computer Science*, *5*(6), 206–210. https://doi.org/0976-5697

Mesquida, A. L., Mas, A., & Amengual, E. (2009). La madurez de los servicios TI. *Revista Española de Innovación, Calidad e Ingenieria Del Software*, *5*(2), 77–87. https://doi.org/1885-4486

Montaño Arango, O., Corona Armenta, J. R., & Medina Marín, J. (2008). MODELO QUE IDENTIFICA EL NIVEL DE MADUREZ DE LOS PROCESOS DE LAS PEQUEÑAS EMPRESAS DEL SECTOR INDUSTRIAL. *XII CONGRESO INTERNACIONAL DE LA ACADEMIA DE CIENCIAS ADMINISTRATIVAS A. C. (ACACIA)*, (01771). Retrieved from https://www.uaeh.edu.mx/investigacion/productos/5692/prod_06.pdf

NIST. (2018). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas*. https://doi.org/10.6028/NIST.CSWP.04162018

Porter, M. (1985). *Competitive Advantage: Creating and Sustaining Superior Performance*.

PriceWaterhouseCooper. (2017). *Encuesta Global de Seguridad de la Información*. Retrieved from https://www.pwc.com.ar/es/publicaciones/assets/encuesta-global-seg-inf2017.pdf

Rosmiati, Riadi, I., & Prayudi, Y. (2016). A Maturity Level Framework for Measurement of Information Security Performance. *International Journal of Computer Applications*, *141*(8), 1–6. https://doi.org/10.5120/ijca2016907930

SEI. (2010). CMMI ® para Desarrollo, Versión 1.3. *CMMI Para Dsarrolo, Version 1.3*, 555. https://doi.org/CMU/SEI-2010-TR-033 ESC-TR-2010-033

SEI. (2012). Governing for Enterprise Security. Retrieved from http://www.cert.org/governance/

SEI. (2019). Software Engineering Institute. Retrieved from https://www.sei.cmu.edu/

Solarte Solarte, F. N. J., Enriquez Rosero, E. R., & Benavides Ruano, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO / IEC 27001. *Revista Tecnológica ESPOL – RTE*, *28*(Diciembre), 492–507.

Supriyatna, A. (2014). Analysis of the academic information system security level by combining Standard BS-7799 with SSE-CMM. *Seminar Nasional Aplikasi Sains & Teknologi (SNAST)*. https://doi.org/1979-911X

Torrado-fonseca, M. R.-álvarez M. (2016). El método Delphi. *REIRE. Revista d'Innovació i Recerca En Educació*, *9*(1), 87–102. https://doi.org/10.1344/reire2016.9.1916

Universitat de Barcelona. (2019). CRITERIO DE EXPERTOS. SU PROCESAMIENTO A TRAVÉS DEL MÉTODO DELPHY. Retrieved from METODOLOGÍA Y EPISTEMOLOGÍA website: http://www.ub.edu/histodidactica/index.php?option=com_content&view=article&id=21:criterio-de-expertos-su-procesamiento-a-traves-del-metodo-delphy&catid=11:metodologia-y-epistemologia&Itemid=103

Van Os, R. (2016). *SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers* (Luleå University of Technology). Retrieved from http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1033727&dswid=1307

Varonis. (2018). NIST 800-53: Definition and Tips for Compliance. Retrieved from https://www.varonis.com/blog/nist-800-53/

Velásquez Pérez, T., Puentes Velásquez, A. M., & Pérez Pérez, Y. M. (2015). Un enfoque de buenas prácticas de gobierno corporativo de TI. *Tecnura*, 159–169. https://doi.org/10.14483/udistrital.jour.tecnu-ra.2015.SE1.a14

Villafañe, J. (2015). *La comunicación empresarial y la gestión de los intangibles en España y Latinoamérica*. https://doi.org/9788497848732

Von-Solms, B. (2001). Information security. A multidi- mensional discipline. *Computers & Security*, *20*(6), 504–508. https://doi.org/10.1016/S0167-4048(01)00608-3

Von-Solms, B. (2006). Information security. The fourth wave. *Computers & Security*, *25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

Westerman, G., & Richard, H. (2007). IT Risk – Turnig Business Threats into Competitive Advantage. *Harvard Business School Press*, 2–7.

ANEXOS.

Anexo 1. Correlación entre los estándares ISO/IEC 27001:2013 / NIST SP 800-53

	ISO 27001:2013	NIST SP 800-53		
Sección	**Dominio / Subdominio**	**Función**	**Categoría**	**Subcategoría**
A5	**Políticas de seguridad de la información**			
A5.1	**Directrices de gestión de la seguridad de la información**			
A5.1.1	Políticas para la seguridad de la información	Identificar (ID)	**Gobierno (ID.GV):** Las políticas, procedimientos y procesos para manejar y monitorear los requerimientos regulatorios, legales, riesgos, ambientales y operacionales de la organización son entendidos e informados a la Gerencia de riesgo de Ciberseguridad	**ID.GV-1:** La Política de Seguridad de la Información se encuentra establecida
A5.1.2	Revisión de las políticas para la seguridad de la información			
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			

A6.1.1	Roles y responsabilidades en seguridad de la información	Identificar (ID)	**Gobierno (ID.GV):** Las políticas, procedimientos y procesos para manejar y monitorear los requerimientos regulatorios, legales, riesgos, ambientales y operacionales de la organización son entendidos e informados a la Gerencia de riesgo de Ciberseguridad	**ID.GV-2:** Los roles y responsabilidades de la Seguridad de la Información son coordinados y alineados con las funciones internas y proveedores externos
			Gestión de activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-6:** Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados
		Proteger (PR)	**Concienciación y capacitación (PR.AT):** El personal y los socios de	**PR.AT-2:** Los usuarios privilegiados comprenden sus roles y responsabilidades **PR.AT-3:** Los terceros interesados (por ejemplo,

			la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	proveedores, clientes, socios) comprenden sus roles y responsabilidades **PR.AT-4:** Los ejecutivos superiores comprenden sus roles y responsabilidades. **PR.AT-5:** El personal de seguridad física y cibernética comprende sus roles y responsabilidades.
		Detectar (DE)	**Procesos de Detección (DE.DP):** Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	**DE.DP-1:** Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.

		Responder (RS)	**Comunicaciones (RS.CO):** Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	**RS.CO-1:** El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.
A6.1.2	Segregación de tareas	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-4:** Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
			Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.

			organización para proteger la confidencialidad, integridad y disponibilidad de la información.	
A6.1.3	Contacto con las autoridades	Responder (RS)	**Comunicaciones (RS.CO):** Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	**RS.CO-2:** Los incidentes se informan de acuerdo con los criterios establecidos.
A.6.1.4	Contacto con grupos de interés especial	Identificar (ID)	**Evaluación de riesgos (ID.RA):** La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	**ID.RA-2:** La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.

A6.1.5	Seguridad de la información en la gestión de proyectos	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-3:** Se encuentran establecidos procesos de control de cambio de la configuración.
A6.2	**Los dispositivos móviles y el teletrabajo**			
A6.2.1	Política de dispositivos móviles			
A6.2.2	Teletrabajo	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones	**PR.AC-3:** Se gestiona el acceso remoto

			asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	
A7	**Seguridad relativa a los recursos humanos**			
A7.1	**Antes del empleo**			
A7.1.1	Investigación de antecedentes	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
			Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las	**PR.IP-11:** La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)

			responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	
A7.1.2	Términos y condiciones del empleo	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
A7.2	**Durante el empleo**			
A7.2.1	Responsabilidades de gestión	Identificar (ID)	**Gobierno (ID.GV):** Las políticas, procedimientos y procesos para manejar y monitorear los requerimientos regulatorios, legales, riesgos, ambientales y operacionales de la organización son entendidos e informados a la Gerencia de riesgo de	**ID.GV-2:** Los roles y responsabilidades de la Seguridad de la Información son coordinados y alineados con las funciones internas y proveedores externos

			Ciberseguridad	
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Proteger (PR)	**Concienciación y capacitación (PR.AT):** El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-1:** Todos los usuarios están informados y capacitados.
				PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.
				PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.
				PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.
				PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.
A7.2.3	Proceso disciplinario			
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**			

A7.3.1	Responsabilidades ante la finalización o cambio	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
			Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-11:** La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)

A8	**Gestión de activos**			
A8.1	**Responsabilidad sobre los activos**			
A8.1.1	Inventario de activos	Identificar (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados.
				ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.
A8.1.2	Propiedad de los activos	Identificar (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados.
				ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.

			organización.	
A8.1.3	Uso aceptable de los activos			
A8.1.4	Devolución de activos	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-11:** La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)
A8.2	**Clasificación de la información**			
A8.2.1	Clasificación de la información	Identificar (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las	**ID.AM-5:** Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.

			instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	
A8.2.2	Etiquetado de la información	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.

			Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-2:** Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.
A8.2.3	Manipulado de la información	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-1:** Los datos en reposo están protegidos. **PR.DS-2:** Los datos en tránsito están protegidos **PR.DS-3:** Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.

			Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-6:** Los datos son eliminados de acuerdo con las políticas.
A8.3	**Manipulación de los soportes**			

A8.3.1	Gestión de soportes extraíbles	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-3:** Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.

			Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-6:** Los datos son eliminados de acuerdo con las políticas.
			Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-2:** Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.

A8.3.2	Eliminación de soportes	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-3:** Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.

			Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-6:** Los datos son eliminados de acuerdo con las políticas.
			Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-2:** Los medios extraíbles están protegidos y su uso se encuentra registrido de acuerdo con la política.

A8.3.3	Soportes físicos en tránsito	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-3:** Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
			Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-2:** Los medios extraíbles están protegidos y su uso se encuentra registrido de acuerdo con la política.
A9	**Control de acceso**			
A9.1	**Requisitos de negocio para el control de acceso**			
A9.1.1	Política de control de acceso	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.

			la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	
A9.1.2	Acceso a las redes y a los servicios de red	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-4:** Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.

			Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
			Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-3:** Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.
A9.2	**Gestión de acceso de usuario**			
A9.2.1	Registro y baja de usuario	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

			asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	
A.9.2.2	Provisión de acceso a usuario	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

A9.2.3	Gestión de privilegios de acceso	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-4:** Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
		Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso**	**PR.AC-4:** Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación

			(PR.AC): El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	de funciones.
A9.2.5	Revisión de los derechos de acceso de usuario			
A9.2.6	Retirada o reasignación de los derechos de acceso			
A9.3	**Responsabilidades del usuario**			
A.9.3.1	Uso de información secreta de autenticación	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

			usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	
A9.4	**Control de acceso a sistemas y aplicaciones**			
A9.4.1	Restricción del acceso a la información	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-4:** Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones. **PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
A9.4.2	Procedimientos seguros de inicio de sesión	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

			asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	
A9.4.3	Sistema de gestión de contraseñas	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

A.9.4.4	Uso de utilidades con privilegios del sistema	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC)**: El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-4:** Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
			Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
A9.4.5	Control de acceso al código	Proteger (PR)	**Seguridad de los datos**	**PR.DS-5:** Se implementan protecciones

	fuente de los programas		**(PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	contra las filtraciones de datos.
A10	**Criptografía**			
A10.1	**Controles criptográficos**			
A10.1.1	Política de uso de los controles criptográficos			
A10.1.2	Gestión de claves			
A11	**Seguridad física y del entorno**			
A11.1	**Áreas seguras**			
A11.1.1	Perímetro de seguridad física	Identificar (ID)	**Entorno empresarial (ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes	**ID.BE-5:** Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).

			interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	
A11.1.2	Controles físicos de entrada	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-2:** Se gestiona y se protege el acceso físico a los activos.
		Proteger (PR)	**Mantenimiento (PR.MA):** El mantenimiento y la reparación de los componentes del sistema de	**PR.MA-1:** El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.

			información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.	
A11.1.3	Seguridad de oficinas, despachos y recursos			
A11.1.4	Protección contra amenazas externas y ambientales	Identificar (ID)	**Entorno empresarial (ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	**ID.BE-5:** Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).
A11.1.5	El trabajo en áreas seguras			
A11.1.6	Áreas de carga y descarga	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan	**PR.IP-5:** Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.

			el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	
A11.2	**Seguridad de los equipos**			
A11.2.1	Emplazamiento y protección de equipos	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los	**PR.IP-5:** Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.

			activos.	
A11.2.2	Instalaciones de suministro	Identificar (ID)	**Entorno empresarial (ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética	**ID.BE-4:** Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.
		Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y	**PR.IP-5:** Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.

			los activos.	
A11.2.3	Seguridad del cableado	Identificar (ID)	**Entorno empresarial (ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética	**ID.BE-4:** Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.
		Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de	**PR.IP-5:** Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.

			los sistemas de información y los activos.	
A11.2.4	Mantenimiento de los equipos	Proteger (PR)	**Mantenimiento (PR.MA):** El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos	**PR.MA-1:** El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.
				PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.
A11.2.5	Retirada de materiales propiedad de la empresa			
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Identificar (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización	**ID.AM-4:** Los sistemas de información externos están catalogados.

			alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	
A11.2.7	Reutilización o eliminación segura de equipos	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-6:** Los datos son eliminados de acuerdo con las políticas.
A11.2.8	Equipo de usuario desatendido			

A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Proteger (PR)	**Tecnología de protección (PR.PT):** Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-2:** Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política
A12	**Seguridad de las operaciones**			
A12.1	**Procedimientos y responsabilidades operacionales**			
A12.1.1	Documentación de procedimientos operacionales			
A12.1.2	Gestión de cambios	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).

			entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	
A12.1.3	Gestión de capacidades	Identificar (ID)	**Entorno empresarial (ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	**ID.BE-4:** Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-7:** Los entornos de desarrollo y prueba(s) están separados del entorno de producción.

A12.2	**Protección contra el software malicioso (malware)**			
A12.2.1	Controles contra el código malicioso	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-6:** Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
		Detectar (DE)	**Monitoreo Continuo de la Seguridad (DE.CM):** El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas y protección	**DE.CM-4:** Se detecta el código malicioso.
		Responder (RS)	**Mitigación (RS.MI):** Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	**RS.MI-2:** Los incidentes son mitigados.
A12.3	**Copias de seguridad**			
A12.3.1	Copias de seguridad de la información	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de	**PR.DS-4:** Se mantiene una capacidad adecuada para asegurar la disponibilidad.

			la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	
			Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-4:** Se realizan, se mantienen y se prueban copias de seguridad de la información.
A12.4	**Registros y supervisión**			

A12.4.1	Registro de eventos	Detectar (DE)	**Monitoreo Continuo de la Seguridad (DE.CM):** El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas y protección	**DE.CM-3:** Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.
		Responder (RS)	**Análisis (RS.AN):** Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	**RS.AN-1:** sSe investigan las notificaciones de los sistemas de detección.
A12.4.2	Protección de la información del registro			

A12.4.3	Registros de administración y operación	Proteger (PR)	**Tecnología de protección (PR.PT):** Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-1:** Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
A12.4.4	Sincronización del reloj	Proteger (PR)	**Tecnología de protección (PR.PT):** Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-1:** Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
A12.5	**Control del software en explotación**			

A12.5.1	Instalación del software en explotación	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-7:** Los entornos de desarrollo y prueba(s) están separados del entorno de producción.

			Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
		Detectar (DE)	**Monitoreo Continuo de la Seguridad (DE.CM):** El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas y protección	**DE.CM-5:** Se detecta el código móvil no autorizado.
A12.6	**Gestión de la vulnerabilidad técnica**			

A12.6.1	Gestión de las vulnerabilidades técnicas	Identificar (ID)	**Evaluación de riesgos (ID.RA):** La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.

		Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-12:** Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.

		Detectar (DE)	**Monitoreo Continuo de la Seguridad (DE.CM):** El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas y protección	**DE.CM-5:** Se detecta el código móvil no autorizado.
		Responder (RS)	**Mitigación (RS.MI):** Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	**RS.MI-3:** Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.
A12.6.2	Restricción en la instalación de software	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).

			gestionar la protección de los sistemas de información y los activos.	
A12.7	**Consideraciones sobre la auditoria de sistemas de información**			
A12.7.1	Controles de auditoría de sistemas de información	Proteger (PR)	**Tecnología de protección (PR.PT):** Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-1:** Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
A13	**Seguridad de las comunicaciones**			
A13.1	**Gestión de la seguridad de las redes**			
A13.1.1	Controles de red	Proteger (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo	**PR.AC-3:** Se gestiona el acceso remoto

			evaluado de acceso no autorizado a actividades autorizadas y transacciones.	
			Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-5:** El personal de seguridad física y cibernética comprende sus roles y responsabilidades.
			Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-2:** Los datos en tránsito están protegidos

			Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-4:** Las redes de comunicaciones y control están protegidas.
A13.1.2	Seguridad de los servicios de red			

A13.1.3	Segregación en redes	Proteger (PR)	**Concienciación y capacitación (PR.AT):** El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-5:** El personal de seguridad física y cibernética comprende sus roles y responsabilidades.
			Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.

A13.2	Intercambio de información			
A13.2.1	Políticas y procedimientos de intercambio de información	Identificar (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-3:** La comunicación organizacional y los flujos de datos están mapeados.

		Proteger (PR)	**Concienciación y capacitación (PR.AT):** El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-5:** El personal de seguridad física y cibernética comprende sus roles y responsabilidades.
			Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.

A13.2.2	Acuerdos de intercambio de información			
A13.2.3	Mensajería electrónica	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-2:** Los datos en tránsito están protegidos. **PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
A13.2.4	Acuerdos de confidencialidad o no revelación	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
A14.1	**Requisitos de seguridad en los sistemas de información**			
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se	**PR.IP-2:** Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.

			utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-3:** Se encuentran establecidos procesos de control de cambio de la configuración.
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-2:** Los datos en tránsito están protegidos. **PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	Proteger (PR)	**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan en función de	**PR.DS-5:** Se implementan protecciones contra las filtraciones de datos.

			la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-6:** Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**			
A14.2.1	Política de desarrollo seguro	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-2:** Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.
A14.2.2	Procedimiento de control de cambios en sistemas	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).

			políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	

A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
A14.2.4	Restricciones a los cambios en los paquetes de software	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).

			entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	
A14.2.5	Principios de ingeniería de sistemas seguros	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-2:** Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.
A14.2.6	Entorno de desarrollo seguro			

A14.2.7	Externalización del desarrollo de software	Detectar (DE)	**Monitoreo Continuo de la Seguridad (DE.CM):** El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia	**DE.CM-4:** Se detecta el código malicioso.
A14.2.8	Pruebas funcionales de seguridad de sistemas	Detectar (DE)	**Procesos de Detección (DE.DP):** Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	**DE.DP-3:** Se prueban los procesos de detección.
A14.2.9	Pruebas de aceptación de sistemas			
A14.3	**Datos de prueba**			
A14.3.1	Protección de los datos de prueba			
A15	**Relación con proveedores**			
A15.1	**Seguridad en las relaciones con proveedores**			

A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Proteger (PR)	**Mantenimiento (PR.MA):** El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.	**PR.MA-2:** El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.
A15.1.2	Requisitos de seguridad en contratos con terceros			
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Identificar (ID)	**Entorno empresarial (ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética	**ID.BE-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.
A15.2	**Gestión de la provisión de servicios del proveedor**			

A15.2.1	Control y revisión de la provisión de servicios del proveedor	Identificar (ID)	**Entorno empresarial (ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética	**ID.BE-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Identificar (ID)		**ID.BE-2:** Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.
A16	**Gestión de incidentes de seguridad de la información**			
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**			

A16.1.1	Responsabilidades y procedimientos	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-9:** Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).
		Detectar (DE)	**Anomalías y Eventos (DE.AE):** se detecta actividad anómala y se comprende el impacto potencial de los eventos.	**DE.AE-2:** Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.

		Responder (RS)	**Comunicaciones (RS.CO):** Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	**RS.CO-1:** El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.
A16.1.2	Notificación de los eventos de seguridad de la información	Detectar (DE)	**Procesos de Detección (DE.DP):** Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	**DE.DP-4:** Se comunica la información de la detección de eventos.
		Responder (RS)	**Comunicaciones (RS.CO):** Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley)	**RS.CO-2:** Los incidentes se informan de acuerdo con los criterios establecidos.
A16.1.3	Notificación de puntos			

	débiles de la seguridad			
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Detectar (DE)	**Anomalías y Eventos (DE.AE):** se detecta actividad anómala y se comprende el impacto potencial de los eventos.	**DE.AE-2:** Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.
A16.1.5	Respuesta a incidentes de seguridad de la información	Recuperar (RC)	**Planificación de la recuperación (RC.RP):** Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad cibernética.	**RC.RP-1:** El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.
		Responder (RS)	**Análisis (RS.AN):** Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	**RS.AN-4:** Los incidentes se clasifican de acuerdo con los planes de respuesta

			Mitigación (RS.MI): Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	**RS.MI-2:** Los incidentes son mitigados.
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-8:** Se comparte la efectividad de las tecnologías de protección.

A16.1.7	Recopilación de evidencias	Responder (RS)	**Análisis (RS.AN):** Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	**RS.AN-3:** Se realizan análisis forenses.
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**			
A17.1	**Continuidad de la seguridad de la información**			
A17.1.1	Planificación de la continuidad de la seguridad de la información	Identificar (ID)	**Entorno empresarial (ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética	**ID.BE-5:** Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).

A17.1.2	Implementar la continuidad de la seguridad de la información	Identificar (ID)	**Entorno empresarial (ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	**ID.BE-5:** Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).
		Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y	**PR.IP-4:** Se realizan, se mantienen y se prueban copias de seguridad de la información.
				PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).

			los activos.	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-4:** Se realizan, se mantienen y se prueban copias de seguridad de la información. **PR.IP-10:** Se prueban los planes de respuesta y recuperación.
A17.2	**Redundancias**			
A17.2.1	Disponibilidad de los	Identificar (ID)	**Entorno empresarial**	**ID.BE-5:** Los requisitos de resiliencia para

	recursos de tratamiento de la información		**(ID.BE):** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética	respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).
A18	**Cumplimiento**			
A18.1	**Cumplimiento de los requisitos legales y contractuales**			
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Identificar (ID)	**Gobernanza (ID.GV):** Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de ciberseguridad	**ID.GV-3:** Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.

A18.1.2	Derechos de Propiedad Intelectual (DPI)	Identificar (ID)	**Gobernanza (ID.GV):** Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de ciberseguridad	**ID.GV-3:** Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.
A18.1.3	Protección de los registros de la organización	Identificar (ID)	**Gobernanza (ID.GV):** Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de ciberseguridad	**ID.GV-3:** Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.
		Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan	**PR.IP-4:** Se realizan, se mantienen y se prueban copias de seguridad de la información.

			políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	
A18.1.4	Protección y privacidad de la información de carácter personal	Identificar (ID)	**Gobernanza (ID.GV):** Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de ciberseguridad	**ID.GV-3:** Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.
A18.1.5	Regulación de los controles criptográficos	Identificar (ID)	**Evaluación de riesgos (ID.RA):** La organización comprende el riesgo de seguridad	**ID.RA-1:** Se identifican y se documentan las vulnerabilidades de los activos.

			cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas	
A18.2	**Revisiones de la seguridad de la información**			
A18.2.1	Revisión independiente de la seguridad de la información			
A18.2.2	Comprobación del cumplimiento técnico	Proteger (PR)	**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-12:** Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.

Anexo 2. Puntos de atención

No.	Puntos de atención (ISO + NIST)
1	Nivel de evidencia de una estructura de Seguridad de la Información razonablemente diseñada y administrada
2	Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes
3	Existen mecanismos de autorización, comunicación, comprensión y aceptación de las políticas
4	Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores
5	Incorporan controles adecuados y suficientes
6	Cubren todos los activos de información esenciales: sistemas y servicios
7	Se refuerzan las políticas de seguridad de la información
8	Se hacen revisiones periódicas de las políticas
9	Sus revisiones han sido aprobadas y socializadas
10	El nivel de énfasis que se da a la seguridad y al riesgo de la información
11	Existe participación de la alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad
12	Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas
13	Cada rol tiene responsabilidad específica con respecto al riesgo y la seguridad de la información
14	Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información
15	Hay coordinación dentro de la organización entre las unidades de negocio
16	Existe apoyo de la alta gerencia para la estructura de riesgo y seguridad de la información
17	Los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas
18	Existe una matriz tipo RACI (Responsable, Aprobador, Consultado, Informado) para mantener la identificación para cada tarea
19	Existe una política que cubra la segregación de deberes
20	Las decisiones respecto a segregación de funciones se encuentran asignadas
21	Se realiza un seguimiento regular de las actividades y los registros de auditoría

22	Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias
23	Está definido el responsable de contactar a las autoridades y en qué punto de un incidente / evento se realiza este contacto y cómo
24	La lista se encuentra actualizada
25	Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches a grupos de Seguridad de la Información
26	Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes
27	La política incluye temas de control de seguridad relacionado con usuarios móviles
28	Se distinguen los dispositivos personales de los empresariales
29	Los sistemas portátiles se mantienen y controlan para garantizar que estén actualizados sobre las definiciones de antivirus y los parches de seguridad
30	Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina
31	Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (ALWAYS-ON-VPN), antivirus, copias de seguridad, parches, registro de seguridad y monitoreo, encriptación y continuidad del negocio
32	El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo
33	En caso de haber contratado a un tercero para la evaluación previa al empleo, se lo revisa sus procesos y se lo considera aceptable
34	Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección
35	Existen procesos de selección mejorados para los trabajadores en roles críticos
36	Existe un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH para la verificación de antecedentes
37	Están claramente definidos los términos y condiciones de empleo

38	Se puede distinguir entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general
39	Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles
40	Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información
41	Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia
42	El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados
43	Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad
44	Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización
45	Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente
46	Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores
47	Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos
48	Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos
49	Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas
50	Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento de Seguridad de Información
51	Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas
52	Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores
53	Se informa a los trabajadores sobre el proceso, incluidas las expectativas de la organización y sus derechos

54	Se actualiza el proceso disciplinario de forma regular
55	Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización
56	Las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos son consideradas dentro de la seguridad de información
57	Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso
58	Existe un inventario de activos de la información con sus responsables identificados que contiene lo siguiente: • Datos digitales • Información impresa • Software • Infraestructura • Servicios de información y proveedores de servicios • Seguridad física • Relaciones comerciales • Las personas
59	Se mantiene el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI
60	Los activos tienen propietario de riesgo
61	Los activos tienen responsable técnico
62	Existe un proceso de asignación de propiedad poco después de crear o adquirir los activos críticos
63	Existe un proceso de etiquetación de activos
64	Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.
65	El acceso a información personal por parte de los empleados se encuentra identificada y documentada
66	Existe un procedimiento para recuperar los activos tras una baja o despido
67	Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información
68	La clasificación de activos se basa en los requisitos de confidencialidad, integridad y

	disponibilidad
69	Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen
70	El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados
71	Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica
72	Se revisan los niveles de clasificación en intervalos predefinidos
73	Los niveles de clasificación están adecuadamente asignados a los activos
74	Se incluye: Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios electrónicos y físicos, divulgación, intercambio, intercambio con terceros, etc.
75	Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles
76	Los medios extraíbles están debidamente etiquetados y clasificados
77	Los medios se mantienen y almacenan de forma adecuada
78	Hay controles apropiados para mantener la confidencialidad de los datos almacenados
79	Existe una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios
80	Se documenta la aprobación en cada etapa para la eliminación de los medios
81	Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación
82	Los datos particularmente confidenciales se eliminan de forma segura (borrado criptográfico, desmagnetización o destrucción física)
83	Se utiliza un transporte o servicio de mensajería confiable
84	Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia
85	Se verifica la recepción por el destino
86	Existe una política de control de acceso
87	Es consistente con la política de clasificación
88	Hay una segregación de deberes apropiada
89	Existe un proceso documentado de aprobación de acceso

90	El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión
91	Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado?
92	Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados
93	Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)
94	La organización mide la identificación y los tiempos de respuesta ante incidentes
95	Se utiliza un ID de usuario únicos para cada usuario
96	Se genera en función a una solicitud con aprobaciones y registros apropiados
97	Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido
98	Existen una comunicación eficiente entre la Administración de Seguridad y Recursos Humanos
99	Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes
100	Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios
101	Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones
102	Existe un registro documental de la solicitud y aprobación de acceso
103	Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios
104	Se genera un ID de usuario separado para otorgar privilegios elevados
105	Se ha establecido una caducidad para los ID de usuario con privilegios
106	Se controlan las actividades de los usuarios privilegiados de forma más detallada
107	Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.
108	Los Sistemas cuentan con configuraciones de contraseñas robustas
109	Se generan contraseñas temporales suficientemente fuertes
110	Se cambian las contraseñas por defecto de los fabricantes
111	Se recomienda a los usuarios usar el software adecuado de protección de contraseñas
112	Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones

113	Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones
114	Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios
115	Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente
116	Existe un proceso de ajuste de derechos de acceso
117	Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo
118	Incluye el acceso físico a las instalaciones y el acceso lógico a la red
119	En casos en los que se usan credenciales compartidas, Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan
120	Existe un proceso de cambio de contraseñas en caso de ser comprometida
121	Existen controles de seguridad relativas a las cuentas compartidas
122	Existen controles de acceso adecuados
123	Se identifican los usuarios de forma individual individuales
124	Existe una definición, autorización, asignación, revisión, gestión y retiro de los derechos de acceso, los permisos y las reglas asociadas
125	Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado
126	Se utiliza autenticación multifactor para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.
127	La información de inicio de sesión solo se valida una vez imputadas las credenciales
128	Las contraseñas no válidas desencadenan demoras o bloqueos, entradas de registro y alertas / alarmas
129	Se registran los inicios de sesión exitosos
130	Se transmiten las contraseñas de modo seguro mediante el uso de cifrado
131	Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos

132	Las reglas tienen en cuenta lo siguiente • Longitud mínima de la contraseña • Evitan la reutilización de un número específico de contraseñas • Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.) • Requiere el cambio forzado de contraseñas en el primer inicio de sesión • Esconde la contraseña durante la imputación
133	Se almacenan y transmiten de forma segura (cifrado)
134	Se verifica que estas personas necesidad comercial para otorgar el acceso según su roles y responsabilidades
135	Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado
136	El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios
137	El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.
138	Se almacenan y revisan los registros de acceso y cambios
139	Existe una política de uso de controles criptográficos que cubre lo siguiente: • Los casos en los que información debe ser protegida a través de la criptografía • Normas que deben aplicarse para la aplicación efectiva • Un proceso basado en el riesgo para determinar y especificar la protección requerida • Uso de cifrado para información almacenada o transferida • Los efectos de cifrado en la inspección de contenidos de software • Cumplimiento de las leyes y normativas aplicables
140	La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)
141	Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas
142	Se generan claves diferentes para sistemas y aplicaciones
143	Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)
144	Se hacen copias de respaldo de las claves
145	Se registran las actividades clave de gestión
146	Las instalaciones se encuentran en una zona de riesgo
147	Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)
148	Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado

149	Se monitorea los puntos de acceso con cámaras
150	Existe un sistema de detección de intrusos y se prueba periódicamente
151	Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)
152	Hay procedimientos que cubran las siguientes áreas • Cambio regular código de acceso • Inspecciones de las guardias de seguridad • Visitantes siempre acompañados y registrados en el libro de visitantes • Registro de movimiento de material • Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas)
153	Se utiliza autenticación multifactor (ej. Biométrico más el código PIN)
154	Existe un registro de todas las entradas y salidas
155	Los accesos (entrada y salida) están físicamente controladas (ej. Detectores de proximidad, CCTV)
156	Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos
157	Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones
158	Existe un procedimiento de recuperación de desastres
159	Se hace un análisis para evaluar que los controles adecuados están implementados Controles de acceso físico Alarmas de intrusión Monitoreo de CCTV (verificar la retención y frecuencia de revisión)
160	Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado
161	Se verifica que el material recibido coincide con un número de pedido autorizado
162	Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad
163	Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas
164	Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada

165	Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales • Agua / inundación • Fuego y humo • Temperatura, humedad y suministro eléctrico • Polvo • Rayos, electricidad estática y seguridad del personal
166	El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad
167	Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente
168	Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante
169	Son probados con regularidad
170	Hay una red de suministro eléctrico redundante
171	Se realizan pruebas de cambio
172	Se ven afectados los sistemas y servicios
173	Hay sistemas de aire acondicionado para controlar entornos con equipos críticos
174	Están ubicados apropiadamente
175	Hay una capacidad adecuada de A / C para soportar la carga de calor
176	Hay unidades redundantes, de repuesto o portátiles disponibles
177	Hay detectores de temperatura con alarmas de temperatura
178	Hay protección física adecuada para cables externos, cajas de conexiones
179	Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias
180	Se controla el acceso a los paneles de conexión y las salas de cableado
181	Existen procedimientos adecuados para todo ello
182	Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)
183	Hay programas de mantenimiento y registros / informes actualizados
184	Existen procedimiento relativos al traslado de activos de información
185	Hay aprobaciones o autorizaciones documentadas en los niveles apropiados

186	Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo
187	Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo
188	Existe una “política de uso aceptable” que cubra los requisitos de seguridad y “obligaciones” con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas
189	Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras
190	Se utiliza cifrado fuerte o borrado seguro
191	Se mantienen registros adecuados de todos los medios que se eliminan
192	La política y el proceso cubren todos los dispositivos y medios de TIC
193	Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción
194	Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado
195	Se protegen los bloqueos de pantalla con contraseña
196	Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas
197	Se mantienen las impresoras, fotocopiadoras, escáneres despejados
198	Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.
199	Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez
200	Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)
201	Existe una política de gestión de cambios
202	Se planifican y gestionan los cambios
203	Los cambios están debidamente documentados, justificados y autorizados por la administración
204	Existe una política de gestión de capacidad
205	Las prioridades se basan en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos

206	Se segregan entornos de TIC de desarrollo, prueba y operacionales
207	Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)
208	Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos
209	Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección
210	Existen políticas y procedimientos asociados a controles antimalware
211	Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado
212	Hay controles de antivirus de “escaneado en acceso” y “escaneo programático” en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT
213	Se actualiza el software antivirus de forma automática
214	Se genera alertas accionables tras una detección y se toma acción rápida y apropiada para minimizar sus efectos
215	Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte
216	Existen políticas y procedimientos asociados a las copias de seguridad
217	Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.
218	Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales y almacenados en ubicaciones adecuadas, protegiendo contra desastres físicos y de acceso indebido.
219	Se mantienen copias off-line para evitar una propagación de ransomware catastrófica
220	Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar
221	Existen políticas y procedimientos para el registro de eventos

222	Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí, incluyendo lo siguiente: • cambios en los ID de usuario • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web
223	Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable
224	Existen copias de seguridad de los registros
225	Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)
226	Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión
227	El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales
228	Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.
229	Existe una política acerca de la instalación de software donde se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción.
230	Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)
231	Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados
232	Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas
233	Existe un control de cambio y aprobación adecuado para la aprobación de software

234	Existe una política la gestión de vulnerabilidades técnicas
235	Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes
236	Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución
237	Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? Los procesos para implementar parches urgentes son adecuados
238	Se emplea una administración automatizada de parches
239	La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados
240	Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos
241	Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.
242	Existe una política que requiera auditorias de seguridad de la información
243	Existe un programa definido y procedimientos para auditoría
244	Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales
245	Se define el alcance de la auditoría en coordinación con la administración
246	El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado
247	Existen políticas de redes físicas e inalámbricas
248	Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red
249	Se registra y monitorea la red y los dispositivos que se conectan ella
250	Hay un sistema de autenticación para todos los accesos a la red de la organización
251	El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos
252	Los usuarios se autentican adecuadamente al inicio de sesión
253	Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.
254	Se controlan los puertos y servicios utilizados para funciones de administración de sistemas
255	Se gestionan, clasifican y protegen los servicios de red de forma adecuada
256	Existe un monitoreo de servicios de red

257	Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)
258	Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red
259	Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM
260	Existe una política de segmentación de red que incluya la red inalámbrica y física
261	
262	Existen políticas y procedimientos relacionados con la transmisión segura de información que contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.
263	Existen controles de acceso adecuados para esos mecanismos
264	
265	Existen comunicaciones donde está implementada la firma digital.
266	Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas
267	Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.
268	Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos
269	Existen acuerdos de confidencialidad y se encuentran revisados por el Departamento Legal
270	Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)
271	Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software
272	Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo
273	Se aplican estos controles para sistemas / software comercial, incluidos los productos “a medida” o personalizados
274	La organización usa o proporciona aplicaciones web de comercio electrónico
275	Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio
276	Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)

277	Existe una gestión de incidentes y cambios para tratarlos
278	Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.
279	
280	Existe una política de desarrollo seguro que abarque la arquitectura de seguridad
281	Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios
282	Existen políticas, procedimientos y registros relacionados de la gestión de cambios incluidos los cambios de emergencia
283	Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión
284	Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado
285	Se hacen cambios a paquetes software adquiridos donde se verifica que los controles originales no hayan sido comprometidos
286	Se obtuvo el consentimiento y la participación del proveedor
287	Se hace una comprobación de compatibilidad con otro software en uso
288	Se siguen principios de SDLC que incluye controles de seguridad
289	Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación
290	Se aíslan los entornos de desarrollo
291	Se realizan comprobaciones de antecedentes de los desarrolladores
292	Se protegen los datos de prueba de la divulgación y dónde están almacenados
293	Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados
294	Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual
295	Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red
296	Las pruebas replican situaciones y entornos operativos realistas
297	Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado
298	Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo

299	Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.
300	Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas
301	Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI que abordan lo siguiente: • Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada • Información / propiedad intelectual, y obligaciones / limitaciones derivadas • Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001 • Identificación de controles físicos y lógicos • Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio • Habilitación de seguridad de los empleados y concienciación • Derecho de auditoría de seguridad por parte de la organización
302	Los contratos o acuerdos formales con proveedores cubren lo siguiente: • Gestión de las relaciones, incluyendo riesgos • Cláusulas de confidencialidad vinculantes • Descripción de la información que se maneja y el método de acceder a dicha información • Estructura de la clasificación de la información a usar • La Inmediata notificación de incidentes de seguridad • Aspectos de continuidad del negocio • Subcontratación y restricciones en las relaciones con otros proveedores • Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, “robo de empleados”, etc.)
303	Se puede rastrear el origen del producto o servicio
304	Existe un monitoreo de servicios y quien responsable de esta actividad
305	En caso que aplique: se comunican los cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados
306	Existen políticas, procedimientos e ITT´s para la gestión de incidentes que cubren lo siguiente: • El plan de respuesta a incidentes • Puntos de contacto para la notificación de incidentes, seguimiento y evaluación • Monitoreo, detección y reporte de eventos de seguridad
307	
308	

	• Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio • Método de recolección de evidencias y pruebas forenses digitales • Revisión post-evento de seguridad y procesos de aprendizaje / mejor
309	Se informan los eventos de seguridad de la información de acuerdo a la política o procedimiento documentado
310	Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen
311	Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución.
312	Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual
313	Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo
314	Existe un mecanismo o procedimiento de informe sobre eventos de seguridad de la información en donde se evidencie que existe una escala de clasificación en base al evento reportado
315	Existen medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes
316	Hay una matriz de escalamiento de incidentes para usar según sea necesario
317	Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?
318	Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes en donde se evalúe las acciones realizadas para que no vuelva a ocurrir.
319	La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área
320	Existe un plan de continuidad de negocio y se evalúa dicho plan periódicamente a través de pruebas.
321	Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares
322	La planificación de la continuidad es consistente e identifica las prioridades de restauración
323	Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades
324	Existe un método de pruebas del plan de continuidad
325	Con qué frecuencia se llevan a cabo dichas pruebas

326	Se han identificado deficiencias?, Se han remediado? y Se han vuelto a probar hasta que los resultados sean satisfactorios
327	Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga
328	Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí
329	Existe una política acerca del cumplimiento de requisitos legales
330	Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento
331	Existe una política que contemple lo siguiente: Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos
332	Se almacenan las firmas digitales de forma segura
333	Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado
334	Se verifica periódicamente la integridad de los registros
335	Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo
336	Existe un mecanismo para instruir al personal en el manejo de información de carácter personal
337	Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico
338	Estas actividades cumplen con los requisitos legales y reglamentarios
339	Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos
340	Se documentan los hallazgos de auditoría y las actuaciones para solventarlo
341	Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares, realizados por profesionales debidamente calificados, y se encuentra evidenciado.
342	Hay evidencias de medidas tomadas para abordar los problemas identificado

Anexo 3. Marco de trabajo propuesto

	ISO 27001:2013	NIST SP 800-53			
Sección	Dominio / Subdominio	Función	Categoría	Subcategoría	Puntos de atención (ISO + NIST)
A5	**Políticas de seguridad de la información**				
A5.1	**Directrices de gestión de la seguridad de la información**				
A5.1.1	Políticas para la seguridad de la información	Identificar (ID)	**Gobierno (ID.GV):** Las políticas, procedimientos y procesos para manejar y monitorear los requerimientos regulatorios, legales, riesgos, ambientales y operacionales de la organización son entendidos e informados a la Gerencia de riesgo de Ciberseguridad	**ID.GV-1:** La Política de Seguridad de la Información se encuentra establecida	Nivel de evidencia de una estructura de Seguridad de la Información razonablemente diseñada y administrada Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes Existen mecanismos de autorización, comunicación, comprensión y aceptación de las políticas Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores Incorporan controles adecuados y suficientes Cubren todos los activos de información esenciales: sistemas y servicios Se refuerzan las políticas de seguridad de la información
A5.1.2	Revisión de las políticas para la seguridad de la información				Se hacen revisiones periódicas de las políticas Sus revisiones han sido aprobadas y socializadas
A6	**Organización de la seguridad de la información**				

1: Inicial *La organización tiene un enfoque ad-hoc o desestructurado en esta práctica o estándar.*	**2: Gestionado** *La organización tiene un enfoque consistente, pero en su mayoría no está documentado.*	**3: Definido** *La organización aplica un enfoque detallado, documentado. Pero no medido ni reforzado*	**4: Gestionado Cuantitativamente** *La organización regularmente mide su cumplimiento y hace mejoras al proceso de forma regular.*	**5: En Optimización** *La organización ha refinado su cumplimiento a un nivel de buena práctica.*	**Observaciones**

Anexo 4. Selección de expertos

Entrevistado(a): Catania Játiva				Total Ponderación
Preguntas		Respuesta		1
No.	Dominio del tema abordado	SI	NO	Detalle Ponderación
1	¿Conoce usted la situación actual de la Seguridad de la Información en la empresa que labora?	X		0.125
2	¿Sabe usted cuáles son las posibles oportunidades de mejora que su organización debe tener en cuanto a la Seguridad de la Información?	X		0.125
3	¿Conoce usted cuál es el objetivo de la norma ISO 27001:2013?	X		0.125
4	¿Sabe usted cómo determinar el nivel de madurez de los procesos en una Organización?	X		0.125
5	¿Conoce usted acerca de temas relacionados a la Ciberseguridad?	X		0.125
6	¿Conoce más de dos normas relacionado a Seguridad de la Información?	X		0.125
7	¿Sabe acerca del concepto del Ciclo de Deming?	X		0.125
8	¿Ha realizado Auditorías basado en la norma ISO 27001:2013?	X		0.125
Años de experiencia				
1	Señale los años de experiencia que tiene en manejo de temas relacionados a la Seguridad de la Información	12 años		1

Entrevistado(a): Javier Baquero				Total Ponderación
Preguntas		Respuesta		0.75
No.	Dominio del tema abordado	SI	NO	Detalle Ponderación

1	¿Conoce usted la situación actual de la Seguridad de la Información en la empresa que labora?	X		0.125
2	¿Sabe usted cuáles son las posibles oportunidades de mejora que su organización debe tener en cuanto a la Seguridad de la Información?	X		0.125
3	¿Conoce usted cuál es el objetivo de la norma ISO 27001:2013?	X		0.125
4	¿Sabe usted cómo determinar el nivel de madurez de los procesos en una Organización?		X	0
5	¿Conoce usted acerca de temas relacionados a la Ciberseguridad?	X		0.125
6	¿Conoce más de dos normas relacionado a Seguridad de la Información?	X		0.125
7	¿Sabe acerca del concepto del Ciclo de Deming?	X		0.125
8	¿Ha realizado Auditorías basado en la norma ISO 27001:2013?		X	0
Años de experiencia				
1	Señale los años de experiencia que tiene en manejo de temas relacionados a la Seguridad de la Información	13 años		1

Entrevistado(a): Susan Noboa				**Total Ponderación**
Preguntas		**Respuesta**		0.75
No.	**Dominio del tema abordado**	**SI**	**NO**	**Detalle Ponderación**
1	¿Conoce usted la situación actual de la Seguridad de la Información en la empresa que labora?	X		0.125
2	¿Sabe usted cuáles son las posibles oportunidades de mejora que su organización debe tener en cuanto a la Seguridad de la Información?	X		0.125

3	¿Conoce usted cuál es el objetivo de la norma ISO 27001:2013?	X		0.125
4	¿Sabe usted cómo determinar el nivel de madurez de los procesos en una Organización?		X	0
5	¿Conoce usted acerca de temas relacionados a la Ciberseguridad?		X	0
6	¿Conoce más de dos normas relacionado a Seguridad de la Información?	X		0.125
7	¿Sabe acerca del concepto del Ciclo de Deming?	X		0.125
8	¿Ha realizado Auditorías basado en la norma ISO 27001:2013?	X		0.125
Años de experiencia				
1	Señale los años de experiencia que tiene en manejo de temas relacionados a la Seguridad de la Información	9 años		1

Entrevistado(a): Jorge Romero				**Total Ponderación**
Preguntas		**Respuesta**		0.875
No.	**Dominio del tema abordado**	**SI**	**NO**	**Detalle Ponderación**
1	¿Conoce usted la situación actual de la Seguridad de la Información en la empresa que labora?	X		0.125
2	¿Sabe usted cuáles son las posibles oportunidades de mejora que su organización debe tener en cuanto a la Seguridad de la Información?	X		0.125
3	¿Conoce usted cuál es el objetivo de la norma ISO 27001:2013?	X		0.125
4	¿Sabe usted cómo determinar el nivel de madurez de los procesos en una Organización?		X	0
5	¿Conoce usted acerca de temas relacionados a la Ciberseguridad?	X		0.125

6	¿Conoce más de dos normas relacionado a Seguridad de la Información?	X		0.125
7	¿Sabe acerca del concepto del Ciclo de Deming?	X		0.125
8	¿Ha realizado Auditorías basado en la norma ISO 27001:2013?	X		0.125
Años de experiencia				
1	Señale los años de experiencia que tiene en manejo de temas relacionados a la Seguridad de la Información	8 años		1

Entrevistado(a): Jaime De La Cuadra				**Total Ponderación**
Preguntas		**Respuesta**		0.625
No.	**Dominio del tema abordado**	**SI**	**NO**	**Detalle Ponderación**
1	¿Conoce usted la situación actual de la Seguridad de la Información en la empresa que labora?	X		0.125
2	¿Sabe usted cuáles son las posibles oportunidades de mejora que su organización debe tener en cuanto a la Seguridad de la Información?	X		0.125
3	¿Conoce usted cuál es el objetivo de la norma ISO 27001:2013?	X		0.125
4	¿Sabe usted cómo determinar el nivel de madurez de los procesos en una Organización?	X		0.125
5	¿Conoce usted acerca de temas relacionados a la Ciberseguridad?		X	0
6	¿Conoce más de dos normas relacionado a Seguridad de la Información?		X	0
7	¿Sabe acerca del concepto del Ciclo de Deming?	X		0.125
8	¿Ha realizado Auditorías basado en la norma ISO 27001:2013?		X	0
Años de experiencia				

1	Señale los años de experiencia que tiene en manejo de temas relacionados a la Seguridad de la Información	20 años	1

Entrevistado(a): María Elena Ríos				Total Ponderación
Preguntas		Respuesta		0.5
No.	Dominio del tema abordado	SI	NO	Detalle Ponderación
1	¿Conoce usted la situación actual de la Seguridad de la Información en la empresa que labora?	X		0.125
2	¿Sabe usted cuáles son las posibles oportunidades de mejora que su organización debe tener en cuanto a la Seguridad de la Información?	X		0.125
3	¿Conoce usted cuál es el objetivo de la norma ISO 27001:2013?	X		0.125
4	¿Sabe usted cómo determinar el nivel de madurez de los procesos en una Organización?		X	0
5	¿Conoce usted acerca de temas relacionados a la Ciberseguridad?		X	0
6	¿Conoce más de dos normas relacionado a Seguridad de la Información?		X	0
7	¿Sabe acerca del concepto del Ciclo de Deming?	X		0.125
8	¿Ha realizado Auditorías basado en la norma ISO 27001:2013?		X	0
Años de experiencia				
1	Señale los años de experiencia que tiene en manejo de temas relacionados a la Seguridad de la Información	15 años		1

Anexo 5. Revisión del marco de trabajo propuesto por el grupo de expertos seleccionados

Revisión de Marco de Trabajo Propuesto						
Entrevistado: Catania Játiva						
Ítems		**Valoración**				
No.	**Ítem**	**Muy Adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco Adecuado**	**Inadecuado**
1	¿El Marco de trabajo cubre la integridad, confidencialidad y disponibilidad de la información?	X				
2	¿El marco de trabajo define correctamente el nivel de madurez de la Empresa?	X				
3	¿El marco de trabajo asocia correctamente las normas de ciberseguridad con las normas de Seguridad de la Información?	X				
4	¿El marco es claro en sus preguntas para conocer la madurez de los procesos?	X				
5	¿Está de acuerdo con el nivel de madurez definido?	X				
6	¿Considera que las preguntas apuntan a mejoras dentro del proceso de Seguridad de la Información?	X				

Revisión de Marco de Trabajo Propuesto

Entrevistado: Susan Noboa						
Ítems		Valoración				
No.	Ítem	Muy Adecuado	Bastante Adecuado	Adecuado	Poco Adecuado	Inadecuado
1	¿El Marco de trabajo cubre la integridad, confidencialidad y disponibilidad de la información?	X				
2	¿El marco de trabajo define correctamente el nivel de madurez de la Empresa?	X				
3	¿El marco de trabajo asocia correctamente las normas de ciberseguridad con las normas de Seguridad de la Información?	X				
4	¿El marco es claro en sus preguntas para conocer la madurez de los procesos?	X				
5	¿Está de acuerdo con el nivel de madurez definido?	X				
6	¿Considera que las preguntas apuntan a mejoras dentro del proceso de Seguridad de la Información?	X				

Revisión de Marco de Trabajo Propuesto	
Entrevistado: Jorge Romero	
Ítems	Valoración

No.	Ítem	Muy Adecuado	Bastante Adecuado	Adecuado	Poco Adecuado	Inadecuado
1	¿El Marco de trabajo cubre la integridad, confidencialidad y disponibilidad de la información?	X				
2	¿El marco de trabajo define correctamente el nivel de madurez de la Empresa?	X				
3	¿El marco de trabajo asocia correctamente las normas de ciberseguridad con las normas de Seguridad de la Información?	X				
4	¿El marco es claro en sus preguntas para conocer la madurez de los procesos?	X				
5	¿Está de acuerdo con el nivel de madurez definido?	X				
6	¿Considera que las preguntas apuntan a mejoras dentro del proceso de Seguridad de la Información?	X				

Revisión de Marco de Trabajo Propuesto						
Entrevistado: Javier Baquero						
Ítems		**Valoración**				
No.	**Ítem**	**Muy Adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco Adecuado**	**Inadecuado**

1	¿El Marco de trabajo cubre la integridad, confidencialidad y disponibilidad de la información?	X				
2	¿El marco de trabajo define correctamente el nivel de madurez de la Empresa?	X				
3	¿El marco de trabajo asocia correctamente las normas de ciberseguridad con las normas de Seguridad de la Información?	X				
4	¿El marco es claro en sus preguntas para conocer la madurez de los procesos?	X				
5	¿Está de acuerdo con el nivel de madurez definido?	X				
6	¿Considera que las preguntas apuntan a mejoras dentro del proceso de Seguridad de la Información?	X				

Anexo 6. Cadena de valor de la organización

Actividades de Apoyo	**INFRAESTRUCTURA EMPRESARIAL**				
	Administración, Finanzas, Departamento Legal, Contraloría, Auditoría Interna				
	ADMINISTRACIÓN DE RECURSOS HUMANOS				
	Selección de personal, Nómina, Bienestar Social, Programas de Capacitación, Evaluaciones de Desempeño				
	DESARROLLO DE TECNOLOGÍA				
	Sistemas Informáticos, Business Intelligence, Redes LAN, Redes WAN				
	ABASTECIMIENTO				
	Compra de insumos, Partes y Repuestos, Equipos				
Actividades Primarias	**Logística de Entrada**	**Compras**	**Marketing**	**Operaciones de las Tiendas**	**Servicio de Taller**
	Recepción y Almacenamiento	Pedidos de mercadería	Combinación de Productos	Ventas/Pedidos	Garantías
	Control de Inventarios	Reabastecimiento	Promociones	Control de Inventario	Reparaciones
	Despacho de Mercadería	Contratos con proveedores	Publicidad	Asignación de Crédito	Revisión
	Consignación	Pagos	Descuentos a Clientes	Gestión de Cobranzas	Rehabilitación
	Dación				
	Transporte				