FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

IMPLEMENTACIÓN DE UN FRAMEWORK DE CIBERSEGURIDAD COMPUESTO POR NORMAS Y CONTROLES PARA PROTEGER LA INFORMACIÓN DE LAS PEQUEÑAS Y MEDIANAS EMPRESAS EN LIMA

PRESENTADA POR

IRVING CHRISTIAN CABEZAS JUÁREZ

ASESOR

LUIS ALBERT LLATAS MARTÍNEZ

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

LIMA – PERÚ

2020

USMP
UNIVERSIDAD DE SAN MARTIN DE PORRES

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

IMPLEMENTACIÓN DE UN FRAMEWORK DE CIBERSEGURIDAD COMPUESTO POR NORMAS Y CONTROLES PARA PROTEGER LA INFORMACIÓN DE LAS PEQUEÑAS Y MEDIANAS EMPRESAS EN LIMA

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

PRESENTADA POR

CABEZAS JUÁREZ, IRVING CHRISTIAN

LIMA – PERÚ

2020

Dedico esta tesis a toda mi familia por brindarme su apoyo a lo largo de mi carrera universitaria.

A mi mamá Dora, mamá Rosana, hermano José Carlos y papá Juan por ser los grandes ejemplos de mi vida.

Y en especial, a mi tía Mechita y tío Engelberto, un beso hasta el cielo para ustedes.

Agradezco al Ing. Luis Llatas por contribuir en conjunto con el desarrollo de la tesis ejerciendo el fundamental rol de asesor.

ÍNDICE

ÍNDICE DE FIGURAS

Página

ÍNDICE DE TABLAS

Página

RESUMEN

La presente tesis busca ser una guía para aplicar los conceptos de ciberseguridad en PYMES del departamento de Lima. El marco de trabajo elaborado tiene como principales insumos los controles de seguridad (ISO/IEC 20071 y 27002) y los controles críticos de seguridad (Controles CIS), así como también, los lineamientos del marco de trabajo de ciberseguridad (NIST CSF). La justificación para la elaboración del framework propuesto se basa principalmente en brindar una solución viable y práctica ante una real necesidad para este tipo de empresas que requieren proteger su información y carecen de la misma por motivos económicos, recursos humanos, herramientas, entre otros. La metodología PDCA fue utilizada para la construcción del Framework. Consta de cuatro fases que permiten la mejora continua en todo su ciclo de vida. Esta característica asegura que el framework pueda aplicarse en cualquier empresa de acuerdo con su giro de negocio. Asimismo, se demostró el funcionamiento del marco de trabajo aplicándolo en una empresa que brinda servicios de tecnología. Como resultado, se logró correctamente la implementación de todos los controles de ciberseguridad generando un mayor grado responsabilidad y conciencia en función de la seguridad cibernética.

Palabras claves: Ciberseguridad, Controles, Seguridad, Framework, Empresas, Mejora continua.

ABSTRACT

This thesis seeks to be a guide to apply the concepts of cybersecurity in SMEs in the department of Lima. The framework developed has as main inputs the security controls (ISO / IEC 20071 and 27002) and the critical security controls (CIS Controls), as well as the guidelines of the cybersecurity framework (NIST CSF). The justification for the development this framework is based mainly on providing a viable and practical solution to a real need for these types of companies that need to protect their information and lack it for economic reasons, human resources, tools, among others. The PDCA methodology was used for the construction of the Framework. It consists of four phases that allow continuous improvement throughout its life cycle. This feature ensures that the framework can be applied in any company according to its line of business. Likewise, the working framework was demonstrated by applying it in a company that provides technology services. As a result, the implementation of all cybersecurity controls was successfully achieved, generating a greater degree of responsibility and awareness in terms of cybersecurity.

Keywords: Cybersecurity, Controls, Security, Framework, Enterprises, Continuous Improvement.

INTRODUCCIÓN

En los últimos años, la interconexión global de los sistemas informáticos ha traído consigo nuevas amenazas y vulnerabilidades que son explotadas en los activos de las organizaciones, ocasionando altos impactos negativos en la economía, los negocios, seguridad e infraestructura. Es por tal motivo que la ciberseguridad se posiciona como un pilar fundamental en la línea de defensa contra los ataques de seguridad cibernética y seguridad de la información.

La ciberseguridad contiene las actividades necesarias -incluyendo gestión del riesgo- para la protección de las infraestructuras críticas, logrando a su vez, un mayor nivel de disponibilidad en los servicios que brindan. En este sentido, se hace inevitable una gestión de seguridad cibernética.

En el Perú, es importante que todas las empresas -de cualquier tipo- empiecen a tomar conciencia y apliquen una cultura de ciberseguridad entre sus colaboradores, socios estratégicos, proveedores, y clientes. Una estrategia de ciberseguridad alineada a los objetivos del negocio, así como también, un programa de concienciación y capacitación, serán los factores claves de éxito.

El trabajo de investigación tiene como objetivos la elaboración y aplicación de un marco de trabajo que fue compuesto de las características y componentes más significativos de las normas y controles en función con la ciberseguridad, seguridad de la información y gestión del riesgo.

La presente investigación contiene seis (6) capítulos. El primero aborda el marco teórico, que es un conjunto de los antecedentes, enfoques

teóricos, y términos básicos. En el segundo, se trata sobre la metodología, que consta de los materiales y métodos que fueron utilizados para la elaboración de la tesis. El tercero presenta el desarrollo de la investigación, fases y actividades del framework propuesto. En el cuarto, se analizan las pruebas y resultados, que determinaron el nivel de cumplimiento de los objetivos del trabajo de investigación; y el quinto capítulo V se presentan las discusiones y aplicaciones, que permitieron elaborar un análisis e interpretación de los resultados obtenidos.

Sobre la situación problemática, en el año 2018, ESET –organización de seguridad informática– publicó un reporte de seguridad donde presenta la situación de la seguridad de la información en las empresas en la región Latinoamérica. El estudio analizó los tipos de ataques más comunes descubiertos hasta la fecha, tales como ransomware, malware, entre otros. La figura 1 muestra el resultado del índice de infecciones de códigos maliciosos (malware) por país, siendo Ecuador y Venezuela los países que más sufrieron, Perú registra un porcentaje del 18%.

Figura 1. Infecciones de malware por país
Fuente: (Security Report Latinoamérica, 2018)

Asimismo, se presentó el porcentaje de incidentes de códigos maliciosos por tamaño de empresa. Como se puede observar en la figura 2, el resultado del análisis presentado ayuda a comprender que los ataques cibernéticos de este tipo y en general, pueden ocurrir y causar un evento

negativo en todos los tamaños de empresa (pequeña, mediana, grande y empresarial).

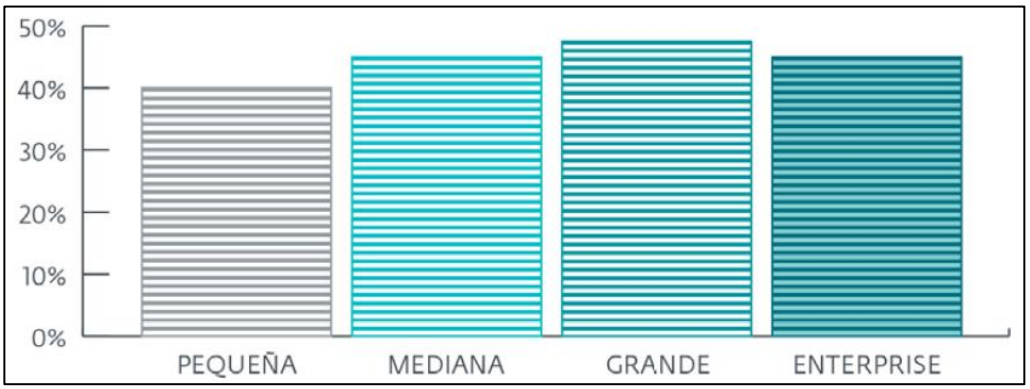


Figura 2. Porcentaje de incidentes de códigos maliciosos por tamaño de empresa
Fuente: (Security Report Latinoamérica, 2018)

Para contrarrestar esta situación, no necesariamente es implementar una solución tecnológica de protección que demande grandes cantidades de dinero. Una opción factible es aplicar controles de seguridad basados en la elaboración de políticas y planes de seguridad de la información, es decir, documentos que describan lineamientos y responsabilidades de los miembros internos y externos de las empresas con el fin de proteger la información. El estudio de la marca ESET presenta en la figura 3 el porcentaje de todos los tipos de empresa que no tienen ningún control de seguridad.

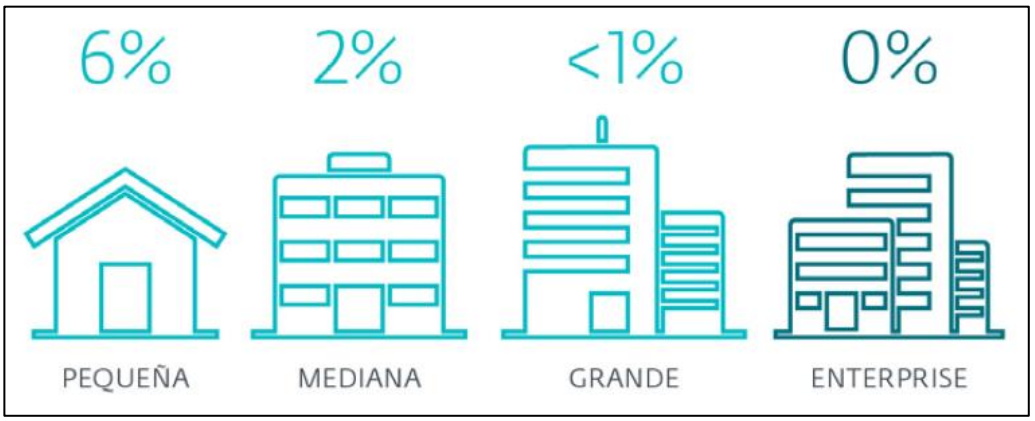


Figura 3. Porcentaje de empresas que no tienen ningún control de seguridad
Fuente: (Security Report Latinoamérica, 2018)

Por otro lado, también es importante conocer y analizar la situación de nuestro país en función de la ciberseguridad. Por ejemplo, el Diario Gestión en una publicación de abril del 2018 informó que las pequeñas y medianas empresas en el Perú muestran un desinterés en la seguridad cibernética y

este dato es reflejado por la poca inversión generada en ella. La figura 4 muestra el titular de la noticia consultada.

Figura 4. Ciberseguridad: Las pymes son las empresas menos protegidas en América Latina
Fuente: (Diario Gestión, 2018)

En el año de 2019, una estadística alarmante fue presentada en la Conferencia Anual de Ejecutivos (CADE) Digital. La firma ESET Perú señaló que más del 93% de las empresas que no cuentan con un plan de ciberseguridad son MYPES y PYMES. Es decir, estas empresas carecen de una seguridad cibernética y son altamente vulnerables a cualquier tipo de ataque. La figura 5 muestra el boletín de la noticia publicada en la web Andina.pe.

Figura 5. CADE Digital: Noticia de Ciberseguridad en PYMES
Fuente: (Agencia Peruana de Noticias, 2019)

En la identificación del problema, se considera una oportunidad de mejora para las pequeñas y medianas empresas ante la situación descrita en el punto anterior. La poca inversión de proyectos de ciberseguridad se

entiende que es por el alto costo de los sistemas y controles existentes, así como también, el alto grado de complejidad, tiempo y recurso humano necesario para implementarlos.

Otro factor para que las pymes no dirijan su mirada hacia la seguridad cibernética es porque no existe un mecanismo sencillo de comprender y práctico que se amolde a sus necesidades. Este mecanismo podría ser un sistema de información, una guía, un estándar o un framework que pueda identificar los recursos de tecnologías de información, evaluar los riesgos, auditar los controles y contemplar una mejora continua en función de la ciberseguridad, todo esto en términos básicos para una protección ante algún evento que afecte su información y reputación.

Por último, el autor toma en cuenta los problemas específicos identificados y expresa el problema principal en el siguiente párrafo.

Ausencia de una herramienta de ciberseguridad basado en normas y controles para la protección de la información de las pequeñas y medianas empresas en Lima.

El objetivo general es desarrollar un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima.

Los objetivos específicos son:

- Identificar, evaluar y armonizar las características de las normas y controles relacionados con la ciberseguridad.
- Elaborar las actividades y desarrollar entregables del framework de ciberseguridad.
- Aplicar el framework de ciberseguridad en una empresa para demostrar el modelo sugerido.

Como justificación, en esta investigación, se busca dotar de resiliencia y capacidad de respuesta ante un evento de seguridad cibernética de manera proactiva a las empresas, eliminando el clásico modelo reactivo.

El framework formulado podría sentar las bases de una posible implementación de la norma ISO/IEC 27001 porque contiene algunas características y controles.

El factor clave de éxito para minimizar los ataques cibernéticos está en las personas, por ende, se desarrollará un plan de capacitaciones y programas de ciberseguridad que reforzará la concienciación en los colaboradores, socios estratégicos, proveedores, y clientes.

Como limitaciones, las situaciones adversas en el desarrollo del trabajo de investigación fueron las siguientes:

- La tesis fue desarrollada de manera individual.
- La documentación de implementaciones de ciberseguridad en empresas peruanas es escasa.
- El acceso a los datos de la empresa fue complejo debido a las políticas de privacidad.

Como alcance, la delimitación del proyecto se basa en las características de las siguientes empresas.

- Empresas clasificadas e identificadas como pequeñas y medianas.
- Empresas con infraestructura tecnológica propias.
- Empresas con dispositivos locales (on-premise) ubicadas en la ciudad de Lima.

CAPÍTULO I
MARCO TEÓRICO

En el primer capítulo, se describieron los antecedentes, bases teóricas y las definiciones de términos básicos que fueron utilizados en la tesis.

1.1 Antecedentes

A continuación, las principales investigaciones desarrolladas que aportaron al trabajo de investigación elaborado.

1.1.1 Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú

(2017) presentaron esta tesis para optar el grado de Bachiller en Ingeniería Empresarial y de Sistemas. El documento muestra como problema principal el alto grado de vulnerabilidad de ciberataques y el impacto que pueden ocasionar en las pequeñas y medianas empresas. La metodología de investigación utilizada se basó en una investigación cuantitativa aplicada a la empresa Transporte Zavala Cargo S.A.C. Los resultados evidenciaron la carencia de planes contra ataques de seguridad cibernética de la empresa y las posibles consecuencias de no contar con una gestión de ciberseguridad.

1.1.2 Ciberdefensa y su incidencia en la protección de la información del ejército del Perú

(2017) presentó la tesis para optar el grado de Magister en Ingeniería de Sistema de Armas. El documento con más de 200 hojas presentó como problema principal las dificultades que impiden el mejoramiento de la ciberseguridad y su impacto en la protección de la

información del Ejército del Perú. La metodología utilizada fue una investigación aplicada y la muestra seleccionada fue todo el Personal Militar y Civil del Comando de Personal del Ejército (COPERE) que tienen responsabilidad en administrar y controlar las diferentes infraestructuras de TI. Los resultados obtenidos mostraron deficiencias en los programas de capacitación y ausencia de recursos disponibles para la ciberdefensa.

1.1.3 La auditoría de seguridad informática y su relación en la ciberseguridad de la fuerza aérea del Perú

(2017) presentó un artículo muy interesante y con mucho valor en función a la seguridad cibernética en la Fuerza Aérea del Perú. La muestra seleccionada abarcó 50 personas de la Especialidad de Informática del Cuartel General FAP. La técnica empleada para el estudio fue por medio de cuestionarios compuesto por las dimensiones Políticas de Ciberseguridad y Ethical Hacking. Los resultados evidenciaron la importancia de realizar una Auditoría de Seguridad Informática que involucre también la seguridad cibernética.

1.2 Bases teóricas

1.3.1 Framework de ciberseguridad

En febrero de 2013, el presidente de los Estados Unidos emitió la Orden Ejecutiva 13636 llamada Mejora de Ciberseguridad de Infraestructuras Críticas. La EO 13636 (por sus siglas en inglés) encargaba al Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) la elaboración un marco de trabajo para poder mitigar los riesgos de la ciberseguridad en el gobierno, industria y los usuarios. (National Institute of Standards and Technology, 2018) El uso del framework de ciberseguridad del NIST (NIST CSF, por sus siglas en inglés) es opcional y consiste en estándares, directrices y mejores prácticas para gestionar el riesgo de la ciberseguridad.

El NIST CSF pretende ser una guía de las actividades de ciberseguridad. (2018) El framework está formado por tres componentes (figura 6): El núcleo del marco de trabajo, Los niveles de implementación del framework y Los perfiles del framework.

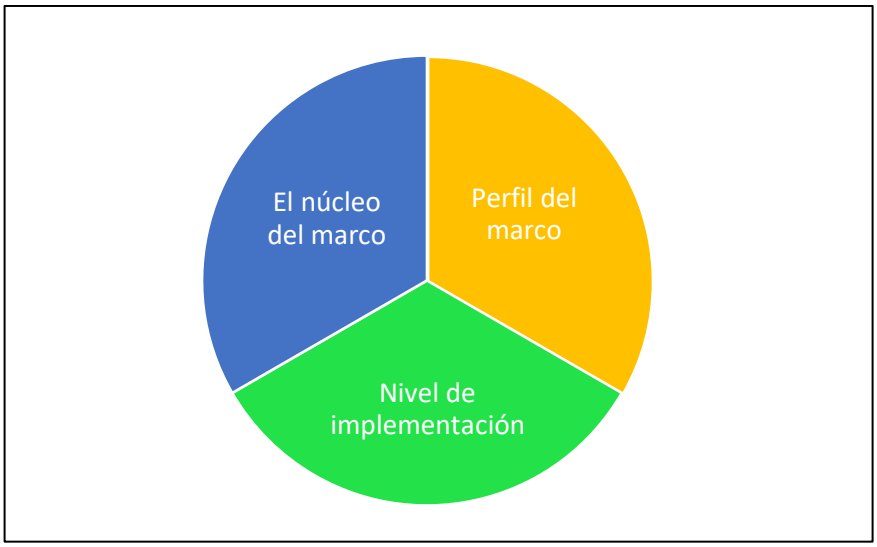


Figura 6. Componentes del NIST CSF
Elaboración: El autor

El núcleo del marco es un conjunto de tareas de ciberseguridad y referencias informativas para las infraestructuras críticas.

Los niveles de implementación proveen un contexto sobre cómo una organización gestiona el riesgo de ciberseguridad.

Los perfiles del marco representan el estado actual y deseado de las organizaciones y permite identificar oportunidades para mejorar la ciberseguridad comparando el perfil actual con el perfil objetivo.

A continuación, se describen con más detalles los componentes del framework.

- **El núcleo del marco**

(2018) El núcleo del marco proporciona un conjunto de actividades para alcanzar resultados específicos de ciberseguridad. Contiene cuatro

elementos: Funciones, Categorías, Subcategorías y Referencias informativas, representadas en la figura 7.

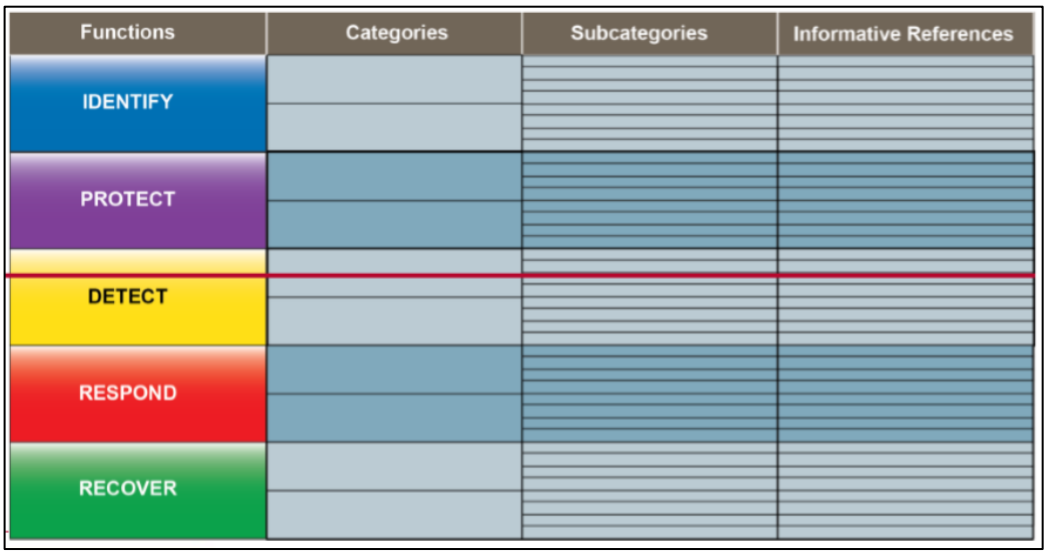


Figura 7. Elementos del Núcleo del marco
Fuente: (Framework for Improving Critical Infrastructure Cybersecurity 1.1, 2018)

Las funciones agrupan las actividades básicas de ciberseguridad. La función Identificar proporciona una gestión del riesgo de la ciberseguridad. La segunda función es Proteger, la cual elabora y aplica planes de contingencia. Detectar es la tercera función e implementa actividades para detectar la ocurrencia de un evento de ciberseguridad. La función Responder desarrolla actividades para tomar acción con respecto a un evento de ciberseguridad. Por último, Recuperar aplica actividades para mantener los planes de resiliencia y restaurar los servicios que se vieron afectados debidos a un evento de ciberseguridad.

Las categorías son divisiones de una función en grupos de resultados de seguridad cibernética. Las subcategorías dividen aún más una categoría en resultados específicos de actividades técnicas y/o de gestión. Por último, las referencias informativas reflejan la relación de normas, directrices y prácticas con una subcategoría. En el Anexo 1 se encuentra el detalle de cada elemento del núcleo del marco del NIST CSF.

- **Nivel de implementación**

(2018) Los niveles de implementación del marco proporcionan un contexto sobre cómo una organización analiza el riesgo de la ciberseguridad y los

procesos implementados para manejar ese riesgo. Los niveles describen el grado de las prácticas de gestión de riesgos de ciberseguridad de una organización. Durante el proceso de selección del nivel, una organización debe considerar sus prácticas actuales de gestión de riesgos. La figura 8 permite visualizar los cuatro niveles de implementación del NIST CSF.

Nivel	Tipo	Proceso de gestión de riesgo	Programa Integrado de gestión de riesgo	Participación externa
1	Parcial	Las prácticas de gestión de riesgo no son formales y el riesgo se gestiona AD HOC	No hay conciencia sobre el riesgo de ciberseguridad	La organización puede no tener los procesos establecidos
2	Riesgo informado	Las prácticas de gestión de riesgos son aprobadas por la administración, pero no pueden establecerse como una política de toda la organización	Existe una conciencia de riesgo de ciberseguridad a nivel organizacional pero no se ha establecido un enfoque de toda la organización para gestionar el riesgo de Ciberseguridad	La organización conoce su rol, pero no ha formalizado sus capacidades para interactuar y compartir información externamente
3	Repetible	Las prácticas de gestión de riesgos de la organización están formalmente aprobadas y expresadas como política	Existe un enfoque de toda la organización para gestionar el riesgo de ciberseguridad	La organización entiende sus dependencias y recibe información de socios que permite la colaboración.
4	Adaptado	A través de un proceso de mejora continua que incorpora tecnologías y prácticas avanzadas de ciberseguridad, la organización se adapta activamente a un entorno cambiante de ciberseguridad y responde a las amenazas cambiantes y sofisticadas de manera oportuna	La gestión del riesgo de ciberseguridad forma parte de la cultura organizacional y evoluciona a partir de la conciencia de las actividades previas, la información compartida por otras fuentes y el conocimiento continuo de las actividades en sus sistemas y redes	La organización gestiona los riesgos y comparte activamente la información con los socios para garantizar que se distribuya y consuma información precisa y actualizada para mejorar la ciberseguridad antes de que se produzca un evento de ciberseguridad

Figura 8. Niveles de implementación NIST CSF

Fuente: (National Institute of Standards and Technology, 2018)

El éxito de la aplicación del marco de trabajo del NIST se basa en el resultado del perfil objetivo de la organización y no en la determinación del nivel. A continuación, se describe el concepto de perfiles del marco de trabajo.

- **Perfil del marco**

(2018) El perfil del marco es la alineación de las Funciones, Categorías y Subcategorías con los requisitos del negocio, tolerancia al riesgo y recursos de la organización. Un perfil permite a las organizaciones establecer un plan para mitigar el riesgo de ciberseguridad. El perfil actual describe los resultados

de ciberseguridad que se están logrando en el presente. El perfil objetivo indica los resultados deseados para lograr los objetivos de gestión de riesgos de ciberseguridad.

La comparación entre el perfil actual y objetivo revela brechas que deben ser analizadas para cumplir con los objetivos de la gestión de riesgos de ciberseguridad. Es importante la definición de un plan de acción para abordar las brechas identificadas en los perfiles. La figura 9 es una representación de la relación dependiente entre los niveles de implementación y los perfiles actual y destino del NIST CSF.

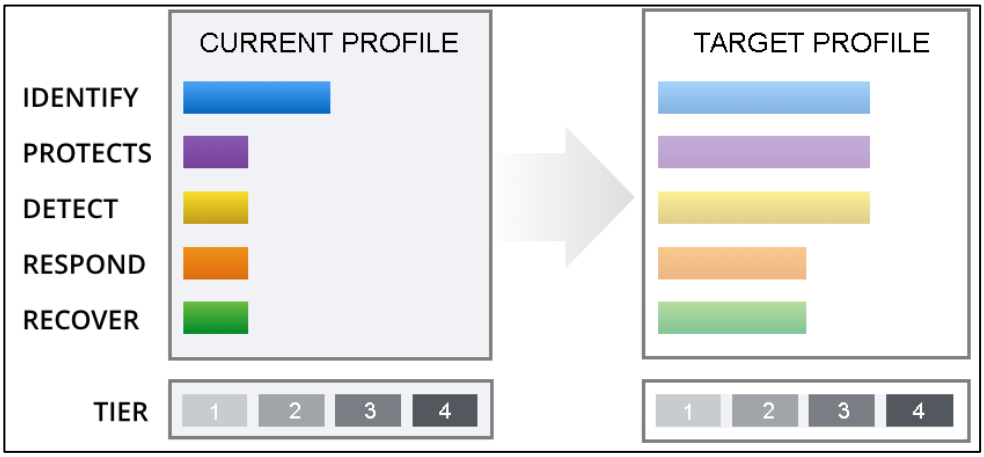


Figura 9. Perfiles del NIST CSF
Fuente: (Framework for Improving Critical Infrastructure Cybersecurity 1.1, 2018)

(2018) El marco de trabajo del NIST establece un programa de ciberseguridad que consta de 7 pasos necesarios para mejorar continuamente la ciberseguridad. A continuación, se describen el programa.

- Paso 1 – Priorización y alcance

  En el primer paso la organización determina sus objetivos y misión de negocio en función de la ciberseguridad.

- Paso 2 – Orientación
  La organización identifica todos los sistemas informáticos y activos.
- Paso 3 – Crear el perfil actual
  Permite crear un perfil del estado actual de la organización en función del resultado de las categorías y subcategorías del núcleo del marco.
- Paso 4 – Conducir evaluación del riesgo
  La evaluación del riesgo se amolda al proceso general de gestión del riesgo de la organización. Se determina la probabilidad de un evento de ciberseguridad y el impacto del evento en la organización.
- Paso 5 – Crear el perfil objetivo
  El perfil objetivo es el estado deseado de la organización y es determinado por la evaluación de las categorías y subcategorías del núcleo del marco.
- Paso 6 – Determinar, analizar y priorizar brechas
  La organización compara el perfil actual y el objetivo para determinar brechas y después elabora un plan de acción.
- Paso 7 – Implementar el plan de acción
  Finalmente, se ejecuta el plan de acción de acuerdo con la priorización de las actividades descritas en el paso 6.

1.3.2 Controles críticos de seguridad

Los controles críticos de seguridad (CSC, por sus siglas en inglés) fueron creados por el Centro para la seguridad de Internet (CIS, por sus siglas en inglés). (2018) CIS es una entidad sin fines de lucro creada para proteger a las organizaciones de las amenazas del ciberespacio. Los controles críticos de seguridad del CIS o controles CIS son un conjunto de acciones fundamentales que ayudan a las organizaciones en la defensa de los ataques más comunes contra sistemas de información y redes de comunicaciones.

En abril del presente año, se lanzó la versión 7 que contempla 20 controles CIS. (2018) Cada control, al mismo tiempo, contiene un conjunto de subcontroles que son requerimientos necesarios para su implementación. Es importante mencionar que el NIST CSF utiliza los controles CIS como parte de su estructura metodológica. La figura 10 muestra la representación de los 20 controles divididos en controles básicos, fundamentales y organizacionales.

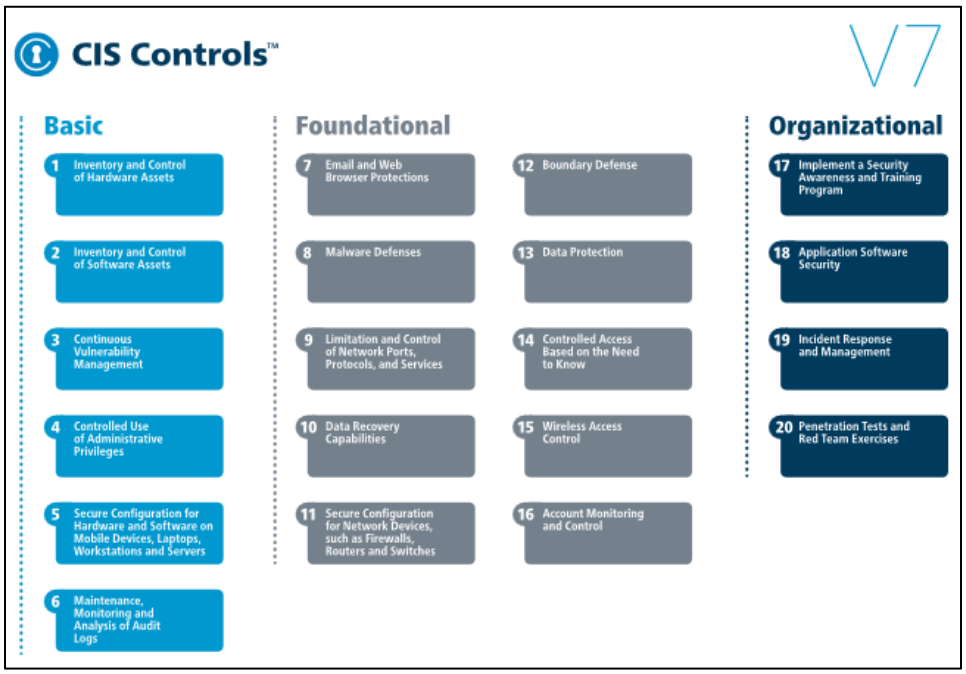


Figura 10. Controles críticos de seguridad del CIS
Fuente: (CIS Controls, 2018)

1.3.3 Normas ISO/IEC

Existe un organismo que elabora, provee y certifica a las organizaciones en base a una serie de normas internacionales de distintos ámbitos. La Organización Internacional de Normalización (ISO, por sus siglas en inglés) tiene como objetivo principal la estandarización de normas para las empresas públicas y privadas a nivel global.

Una organización que trabaja en conjunto con ISO es la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés). Esta organización

desarrolla y suministra normas en las áreas de los campos electrónicos, eléctricos y tecnología. A continuación, se presenta de manera puntual, una serie de normas relacionadas con la seguridad de la información.

- **Norma ISO/IEC 27001**

Es la principal y única norma certificable de la familia ISO 27k e incluye todos los requisitos del sistema de gestión de seguridad de la información (SGSI), entendiéndose por seguridad de la información “la preservación de la confidencialidad. Integridad y disponibilidad de la información” (NTP-ISO/IEC 27001, 2014). En el Perú, el Instituto Nacional de Calidad (INACAL) promueve las Normas Técnicas Peruanas (NTP), que son documentos que sirven como referencia técnica a las organizaciones para lograr calidad en sus servicios. La NTP-ISO/IEC 27001:2014 es una adopción de la norma ISO/IEC 27001:2013.

La ISO/IEC 27001 posee el siguiente nombre: “Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información: Requisitos” y, está compuesto por las siguientes cláusulas descritas en la figura 11.

Cláusula	Descripción
1 - Alcance	Directrices para la seguridad de la información en las organizaciones y prácticas de gestión de seguridad de la información.
2 - Referencias normativas	Son documentos que sirven de consulta para la aplicación de la norma.
3 - Términos y definiciones	Son los términos y definiciones relacionados con la norma.
4 - Contexto de la organización	Comprende las necesidades y expectativas de las partes interesadas, determina el alcance del sistema de gestión de seguridad de la información.
5- Liderazgo	La alta dirección debe mostrar un compromiso y liderazgo con respecto del sistema de gestión de seguridad de la información.
6 - Planificación	La organización debe asegurar que el sistema de gestión de seguridad de la información pueda lograr sus resultados esperados; prevenir, o reducir efectos indeseados; y lograr la mejora continua.
7 - Soporte	La organización debe determinar los recursos necesarios para el sistema de gestión de seguridad de la información.
8 - Operación	La organización debe planificar y controlar la operación del sistema de gestión de seguridad de la información; evaluar y tratar los riesgos de seguridad de la información.
9 - Evaluación del desempeño	Monitorear, medir, analizar y evaluar el desempeño del sistema de gestión de seguridad de la información.
10 - Mejoras	Se deberá mejorar continuamente el sistema de gestión de la seguridad de la información.

Figura 11. Cláusulas ISO/IEC 27001
Fuente: (NTP-ISO/IEC 27001, 2014)

(2014) La norma también contiene un apartado llamado “Anexo A” que incluye los llamados “objetivos de control de seguridad de la información”. Estos controles son derivados de la norma ISO/IEC 27002 (cláusulas 5 al 18) y, se utilizan en el apartado 6.1.3 “Tratamiento de riesgos de la seguridad de la información” de la norma ISO/IEC 27001.

Las organizaciones pueden argumentar no aplicar todos los controles de seguridad en su totalidad porque existe el documento Declaración de Aplicabilidad (SOA, por sus siglas en inglés) que expresa lo siguiente:

"Producir una Declaración de Aplicabilidad que contenga los controles necesarios (véase 6.1.3b y c) y la justificación de las inclusiones ya sea que se implementen o no, así como la justificación de excluir los controles del Anexo A"

(NTP-ISO/IEC 27001, 2014, pág. 7).

El documento nace de la cláusula 6.1.3, donde se menciona que la organización determina los controles necesarios para el tratamiento de riesgos. Esto quiere decir que la organización puede elaborar sus propios controles o seleccionar controles de otras fuentes (por ejemplo, los controles de seguridad del Anexo A). La tabla 1 muestra un ejemplo de una Declaración de Aplicabilidad elaborada por el autor.

Tabla 1
Declaración de aplicabilidad - ISO/IEC 27001

N°	ID Control	Control	Aplica	Justificación
1	5.1.1.	Políticas de seguridad de la información	Si aplica	Las políticas de seguridad de la información proveerán una guía para gestionar la seguridad de la información.
2	6.1.3.	Contacto con las autoridades	No aplica	El control no aplica porque no es necesario en la organización.
….	….	….	….	….

Elaboración: El autor

- **Norma ISO/IEC 27002**

La norma ISO/IEC 27002 llamada: “Tecnología de la información – Técnica de seguridad – Código de prácticas para los controles de seguridad de la información”, es una norma no certificable que sirve como guía donde se presentan los objetivos de control de seguridad de la información referenciados en la norma ISO/IEC 27001.

(2015) La cantidad de controles de seguridad es 144 organizados en 35 categorías y 14 dominios de seguridad. Cada categoría contiene un objetivo de control y uno o más controles aplicables para conseguir el objetivo respectivo. La norma contiene en su estructura las siguientes cláusulas: Alcance, Referencias normativas, Términos y definiciones, Estructura del estándar, Políticas de seguridad de la información, Organización de la seguridad de la información, Seguridad de los recursos humanos, Gestión de activos, Control de acceso, Criptografía, Seguridad física, Seguridad de las operaciones, Seguridad de las comunicaciones, Adquisición, desarrollo y mantenimiento de sistemas, Relaciones con los proveedores, Gestión de incidentes de seguridad de la información, Aspectos de seguridad de la información en la gestión de continuidad del negocio, Cumplimiento. En la figura 12 se observa los dominios de seguridad.

N°	Dominio
A.5	Políticas de seguridad de la información
A.6	Organización de la seguridad de la información
A.7	Seguridad de los recursos humanos
A.8	Gestión de activos
A.9	Control de acceso
A.10	Criptografía
A.11	Seguridad física
A.12	Seguridad de las operaciones
A.13	Seguridad de las comunicaciones
A.14	Adquisición, desarrollo y mantenimiento de sistemas
A.15	Relaciones con los proveedores
A.16	Gestión de incidentes de seguridad de la información
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio
A.18	Cumplimiento

Figura 12. Dominios ISO/IEC 27002
Fuente: (UNE-ISO/IEC 27002, 2015)

1.3.4 Metodología de gestión del riesgo

El Consejo Superior de Administración Electrónica (España) elabora y promueve MAGERIT, que es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (2012) MAGERIT divide la gestión de riesgos en dos actividades principales: análisis y tratamiento de riesgos. El análisis de riesgos permite determinar qué tiene la organización y estimar lo que podría pasar. En el tratamiento de los riesgos, se busca reducir los riesgos identificados. La figura 13 muestra el proceso de gestión del riesgo según MAGERIT.

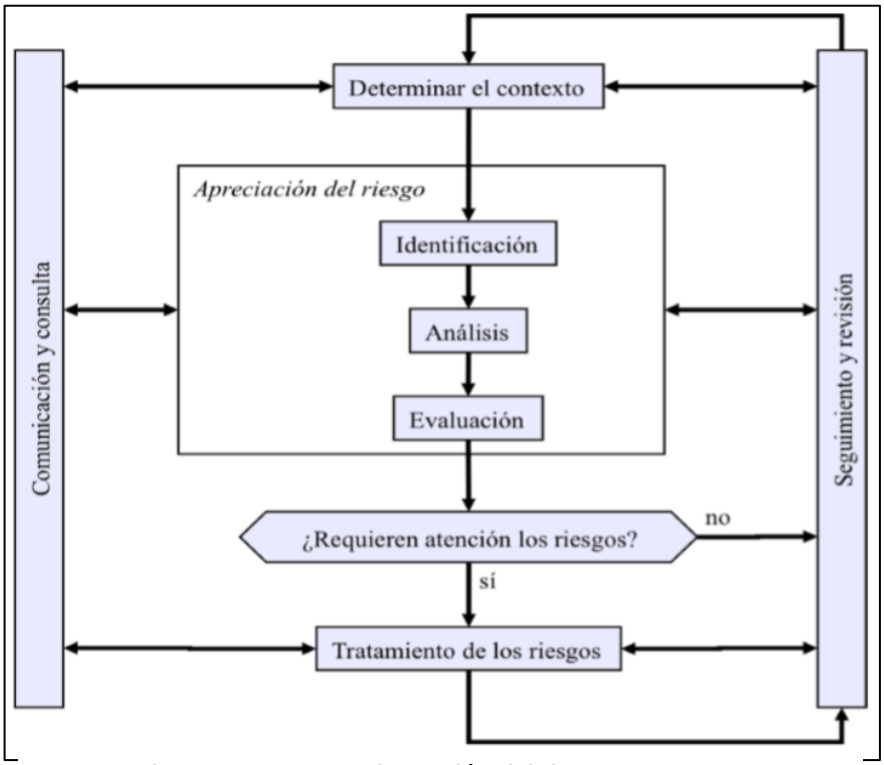


Figura 13. Proceso de gestión del riesgo MAGERIT
Fuente: (MAGERIT V3, 2012)

- Determinación del contexto

  Consiste en identificar los factores de la organización para elaborar la política de gestión del riesgo.

- Identificación de los riesgos

  Los riesgos de los activos de información identificados serán analizados en la siguiente etapa.

- Análisis de los riesgos

  Los riesgos son clasificados de manera cualitativa y cuantitativa.

- Evaluación de los riegos

Determinación de las consecuencias de los riesgos en la organización.

- Tratamiento de los riesgos

  Elaboración de las actividades para modificar el estado de los riesgos.

- Comunicación y consulta

  Es importante informar a los colaboradores sobre la situación de la gestión del riesgo, porque los activos de información soportan los sistemas que brindan soporte a los procesos y servicios de la organización.

- Seguimiento y revisión

  La gestión del riesgo es un proceso cíclico y mejorado continuamente.

A continuación, se presenta las principales actividades de la gestión del riesgo según MAGERIT.

- **Valoración de activos**

(2012) La valorización del activo comprende las dimensiones de la seguridad de la información. Por lo tanto, se valorará en función del grado de confidencialidad (C), disponibilidad (D) e integridad (I). A continuación, se visualiza la figura 14 que describe los valores de impacto y la figura 15 presentando una plantilla del modelo de valor respectivo.

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la organización.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.
3	Dañino	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la organización.
4	Severo	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la organización.
5	Crítico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la organización.

Figura 14. Matriz de impacto
Fuente: (MAGERIT V3, 2012)

Activo de información			Dimensiones			
N°	Activo	Descripción	C	D	I	Total
1	Servidor Controlador de Dominio	Servidor virtual que contiene datos e información de la organización	4	3	5	4
2	Servicio de Facturación	Servicio que soporta el proceso de facturación electrónica	2	2	2	2
…	…	…	..	..	..	..

Figura 15. Plantilla modelo de valor
Fuente: (MAGERIT V3, 2012)

- **Evaluación del riesgo**

(2012) La evaluación del riesgo comprende dos variables, la probabilidad de ocurrencia y el impacto que causaría si el riesgo se materializa. También, contempla la identificación de las amenazas de los activos. Las siguientes tablas corresponden a la matriz de probabilidad, zona de riegos, criterios de aceptación del riesgo, y el mapa de riesgos. Los valores del impacto fueron descritos en la figura 16.

Nivel	Descriptor	Descripción	Frecuencia
1	Improbable	El evento ocurre solo en circunstancias excepcionales	No se ha presentado en los últimos tres años.
2	Raro	El evento puede ocurrir en algún momento	Al menos una vez en los últimos tres años.
3	Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en todas las circunstancias	Al menos una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año.

Figura 16. Probabilidad de ocurrencia
Fuente: (MAGERIT V3, 2012)

Los criterios de aceptación del riesgo permiten realizar una acción en el tratamiento de los riesgos, es decir, implementar o no controles para modificar los riesgos según en la zona de riesgos en donde se encuentre. La figura 17 muestra los criterios respectivos y la figura 18 la descripción de las zonas de riesgos.

Probabilidad	Impacto				
	Insignificante (1)	Menor (2)	Dañino (3)	Severo (4)	Crítico (5)
Improbable (1)	1	2	3	4	5
Raro (2)	2	4	6	8	10
Posible (3)	3	6	9	12	15
Probable (4)	4	8	12	16	20
Casi seguro (5)	5	10	15	20	25

Figura 17. Criterios de aceptación
Fuente: (MAGERIT V3, 2012)

Zona	Descripción	Criterio de aceptación	Descripción
B	Zona de riesgo baja	Asumir el riesgo	Se acepta la pérdida probable y se elabora planes de contingencia.
M	Zona de riesgo moderada	Asumir el riesgo, evaluar reducir el riesgo	Reducir: Implica tomar medidas para disminuir tanto la probabilidad e impacto. Compartir: Reduce el efecto a través del traspaso de las pérdidas a otras organizaciones. Evitar: Tomar las medidas para prevenir la materialización del riesgo.
A	Zona de riesgo alta	Reducir el riesgo, evitar, compartir o transferir	
E	Zona de riesgo extrema	Reducir el riesgo, evitar, compartir o transferir	

Figura 18. Zona de riesgos
Fuente: (MAGERIT V3, 2012)

La figura 19 presenta una plantilla del mapa de riesgos donde se detallarán las amenazas más significativas de cada activo, caracterizándolas por su probabilidad de ocurrencia y el impacto que podría causar la materialización sobre el activo.

Activo de información			Amenaza		Ocurrencia		Evaluación del riesgo	
N°	Activo	Amenaza	Impacto	Valor	Probabilidad	Valor	Total	Zona de riesgo
1	Servidor Controlador de Dominio	Acceso no autorizado	Dañino	3	Improbable	2	6	Media
2	Servicio de Facturación	Alteración de los datos	Crítico	5	Posible	3	15	Alta
...	...	...	...	...	...	...	...	...

Figura 19. Plantilla Mapa de riesgos
Fuente: (MAGERIT V3, 2012)

- **Tratamiento del riesgo**

(2012) El tratamiento del riesgo permite identificar los controles o salvaguardas que se implementarán para mitigar los riesgos de los activos en función al mapa del riesgo previamente elaborado. La figura 20 presenta una plantilla del plan de tratamiento del riesgo respectivo.

Activo de información					Tratamiento del riesgo		
N°	Activo	Propietario del riesgo	Amenaza	Zona de riesgo	Control (Salvaguarda)	Observaciones	Estado
1	Servidor Controlador de Dominio	Administrador de servidores	Acceso no autorizado	Media	Eliminación de permisos de acceso a otros usuarios NO administradores del Directorio Activo	Se ejecutará el cambio en la fecha 15/07/2019	Pendiente
2	Servicio de Facturación	Personal de facturación	Alteración de los datos	Alta	Implementación de facturación electrónica	Se encuentra en fase de pruebas Pase a producción programado para el 10/12/2019	En progreso
..	...	...	...	...	...	...	...

Figura 20. Plantilla Plan de tratamiento del riesgo
Fuente: (MAGERIT V3, 2012)

1.4 Definición de términos básicos

Para los fines del documento se precisan los siguientes términos básicos.

1.4.1 Seguridad de la información

Los términos descritos se basan en la norma ISO/IEC 27000.

- Ataque; es un intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.
- Activo; es cualquier cosa que tenga valor para un individuo, una organización o un gobierno.
- Activo de información; son los datos que tienen valor para la persona o la organización.
- Confidencialidad; es una propiedad de que la información no se pone a disposición o se divulga a personas, entidades, o procesos no autorizados.
- Continuidad de seguridad de la información; son los procesos y procedimientos para asegurar la continuidad de las operaciones de seguridad de la información.
- Control; es una medida que está modificando el riesgo. El control incluye cualquier proceso, política, dispositivos, prácticas, u otras acciones que modifican el riesgo.
- Control de acceso; es el medio para garantizar que el acceso a los activos esté autorizado y restringido según el negocio y los requisitos de seguridad.
- Disponibilidad; es una propiedad de que la información puede ser accesible y utilizable a pedido por una entidad autorizada.
- Evento de seguridad de la información; es una ocurrencia identificada de un sistema, servicio, o estado de la red que indica un posible incumplimiento de la política de seguridad de la información.
- Incidente de seguridad de la información; es uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen un valor significativo que probablemente compromete las operaciones de negocio y amenaza con la seguridad de la información.
- Integridad; es una propiedad de exactitud y ser completo.
- Mejora continua; es una actividad recurrente para mejorar el rendimiento.

- Política; son direcciones de una organización según lo expresado formalmente por la alta dirección.
- Seguridad de la información; es la preservación de la confidencialidad, integridad, y disponibilidad de la información.
- Sistema de información; es un conjunto de aplicaciones, servicios, activos de TI, u otros componentes de manejo de información.

1.4.2 Ciberseguridad

Los términos descritos se basan en la norma ISO/IEC 27032.

- Aplicación; es una solución de TI que incluye programas, datos y procedimientos diseñados para ayudar a los usuarios de las organizaciones a realizar tareas específicas.
- Ataque potencial; es la percepción de las posibilidades de éxito de un ataque.
- Ciberespacio; es un entorno complejo que resulta de la interacción de las personas, software, y servicios a través de Internet por medio de dispositivos tecnológicos y redes conectadas, que no existe en forma física alguna.
- Ciberseguridad; es la preservación de la confidencialidad, integridad, y disponibilidad de la información en el ciberespacio.
- Delito informático (cibercrimen); es la actividad delictiva donde se utilizan los servicios o aplicaciones en el ciberespacio para o son objeto de un delito.
- Internet; es un sistema global de redes interconectadas en dominio público.
- Red interconectada (internet); es una interconexión de redes.
- Software malicioso (*malware*); es un software diseñado con malas intenciones que contiene características o capacidades que potencialmente puede causar daño al usuario y/o sistema.

1.4.3 Gestión del riesgo

Los términos descritos se basan en la norma ISO/IEC 27005.

- Amenaza; causa potencial de un incidente no deseado.
- Criterio del riesgo; término de referencia que se utilizará para evaluar el riesgo.
- Evaluación del riesgo; proceso que involucra la identificación, análisis y evaluación del riesgo.
- Gestión del riesgo; actividades coordinados para dirigir y controlar los riesgos de la organización.
- Nivel del riesgo; magnitud del riesgo, expresado en términos de la combinación de probabilidad e impacto.
- Probabilidad; posibilidad de que algo suceda.
- Riesgo; en seguridad de la información se asocia con el producto de la probabilidad e impacto de una amenaza explotada por las vulnerabilidades de un activo.
- Tratamiento del riesgo; proceso de modificar los riesgos.
- Vulnerabilidad; debilidad de un activo o control que puede ser explotado por una o más amenazas.

CAPÍTULO II
METODOLOGÍA

En el segundo capítulo, se describen los materiales y métodos que fueron utilizados en el trabajo de investigación.

2.1 Materiales

Para el desarrollo de la tesis se utilizaron los siguientes recursos.

2.1.1 Recursos humanos

Los responsables del desarrollo de la tesis se describen en la tabla 2.

Tabla 2
Recursos Humanos

Responsable	Rol	Descripción
Irving Cabezas Juárez	Investigador	Profesional que realiza las tareas de investigación en el proyecto.
Irving Cabezas Juárez	Implementador	Profesional que ejecuta las fases del proyecto.
Luis Llatas Martínez	Asesor	Profesional que orienta al investigador en la elaboración y desarrollo del proyecto.

Elaboración: El autor

2.1.2 Recursos Hardware

Los dispositivos tecnológicos utilizados se describen en la tabla 3.

Tabla 3
Recursos Hardware

Dispositivo	Características	Cantidad	Descripción
Laptop	CPU Intel i5 2.30 GHz	1	Computadora portátil que ejecuta instrucciones realizadas por los usuarios.
	Memoria RAM 12 GB	1	
	Disco Duro 1 TB	1	
Monitor	Resolución 1360 x 768 píxeles	1	Dispositivo que muestra la información al usuario.
Impresora	Wi-Fi, impresión, copia, y escaneo	1	Dispositivo que permite imprimir documentos digitales.

Elaboración: El autor

2.1.3 Recursos Software

Las aplicaciones utilizadas se describen en la tabla 4.

Tabla 4
Recursos Software

Software	Versión	Cantidad	Descripción
Microsoft Windows	10	1	Sistema operativo que se encuentra instalado en las computadoras
Microsoft Office	365	1	Suite de aplicaciones que permiten la gestión documentaria del proyecto
Microsoft Project	2016	1	Aplicación que permite gestionar el cronograma y tareas del proyecto

Elaboración: El autor

2.1.4 Presupuesto

El presupuesto de los recursos se describe en las siguientes tablas.

Tabla 5
Costos del recurso humano

Recurso	Costo por día (S/.)	Días invertidos	Mes	Costo total (S/.)
Investigador / Implementador	25	18	Setiembre 2018	450
	25	18	Octubre 2018	450
	25	21	Noviembre 2018	525
	25	22	Marzo 2019	550
	25	12	Abril 2019	300
	25	20	Mayo 2019	500
	25	15	Junio 2019	375
	25	16	Agosto 2019	400
	25	8	Setiembre 2019	200
	Costo total investigador / implementador * 150 días (S/.)			3,750
Asesor	35	2	Setiembre 2018	70
	35	2	Octubre 2018	70
	35	2	Noviembre 2018	70
	35	1	Marzo 2019	35
	35	2	Abril 2019	75
	35	0	Mayo 2019	0
	35	2	Junio 2019	70
	35	2	Agosto 2019	70
	35	5	Setiembre 2019	175
	Costo total asesor * 54 días (S/.)			630
Costo total recurso (S/.)				4,380

Elaboración: El autor

Tabla 6
Costos del recurso hardware

Recurso	Cantidad	Costo unitario (S/.)	Costo total (S/.)
Laptop	1	S/. 3,600	S/. 3,600

Monitor	1	S/. 650	S/. 650
Impresora	1	S/. 450	S/. 450
Costo total recurso (S/.)			S/. 4,700

Elaboración: El autor

Tabla 7
Costos del recurso software

Recurso	Cantidad	Costo unitario (S/.)	Costo total (S/.)
Microsoft Windows	1	S/. 0	S/. 0
Microsoft Office	1	S/. 0	S/. 0
Microsoft Project	1	S/. 150	S/. 150
Costo total del recurso (S/.)			S/. 150

Elaboración: El autor

Tabla 8
Costos de otros recursos

Recurso	Cantidad	Costo unitario (S/.)	Costo total (S/.)
ISO/IEC 27000:2018	1	S/. 0	0
Norma Técnica Peruana ISO/IEC 27001:2014	1	S/. 66.62	S/. 66.62
Una Norma Española ISO/IEC 27002:2015	1	S/. 0	S/. 0
Norma Técnica Peruana ISO/IEC 27005:2009	1	S/. 97.80	S/. 97.80
Norma Técnica Ecuatoriana ISO/IEC 27032:2015	1	S/. 0	S/. 0
Framework Ciberseguridad NIST V1.1	1	S/. 0	S/. 0
Controles CIS V7	1	S/. 0	S/. 0
MAGERIT V3	3	S/. 0	S/. 0
Costo total del recurso (S/.)			S/. 164.42

Elaboración: El autor

Tabla 9
Costos del proyecto resumen

Tipo del recurso	Costo total (S/.)
Recursos humanos	S/. 4,380

Recursos hardware	S/. 4,700
Recursos software	S/. 150
Otros recursos	S/. 164.42
Total (S/.)	S/. 9,394

Elaboración: El autor

2.1.5 Cronograma

El desarrollo de la tesis se inició con la elaboración de un plan de tesis que fue aprobado en setiembre del año 2018. A continuación, la figura 21 muestra las actividades de la elaboración del documento tesis.

Nombre de tarea	Duración	Fecha Inicio	Fecha Fin	Responsable
Implementación de un Framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima	**150 días**	**6/09/2018**	**12/09/2019**	-
Primera etapa - Introducción de la tesis	**18 días**	**6/09/2018**	**3/10/2019**	**-**
Elaboración de la "Introducción" del proyecto	8 días	6/09/2018	18/08/2018	Implementador
Elaboración de la "Situación problemática" del proyecto				
Elaboración de la "Identificación del problema" del proyecto				
Elaboración de los "Objetivos" del proyecto				
Elaboración de la "Justificación" del proyecto				
Elaboración de las "Limitaciones" del proyecto				
Elaboración del "Alcance" del proyecto				
Primera revisión de los avances	1 día	19/09/2018	19/09/2018	Implementador / Asesor
Levantamiento de observaciones	4 días	20/09/2018	25/09/2018	Implementador
Segunda revisión de los avances	1 día	26/09/2018	26/09/2018	Implementador / Asesor
Levantamiento de observaciones	4 días	27/09/2018	3/10/2019	Implementador
Segunda etapa - Capítulo I Marco Teórico	**18 días**	**4/10/2018**	**31/10/2018**	**-**
Elaboración de los "Antecedentes" del proyecto	8 días	4/10/2018	16/10/2018	Implementador
Elaboración de las "Bases teóricas" del proyecto				
Elaboración de la "Definición de términos básicos" del proyecto				
Primera revisión de los avances	1 día	17/10/2018	17/10/2018	Implementador / Asesor
Levantamiento de observaciones	4 días	18/10/2018	24/10/2018	Implementador
Segunda revisión de los avances	1 día	25/10/2018	25/10/2018	Implementador / Asesor
Levantamiento de observaciones	4 días	26/10/2018	31/10/2018	Implementador
Tercera etapa - Capítulo II Metodología	**21 días**	**11/11/2018**	**30/11/2018**	**-**
Elaboración de los "Materiales" del proyecto	12 días	1/11/2018	20/11/2018	Implementador
Elaboración de los "Métodos" del proyecto				
Primera revisión de los avances	1 día	21/11/2018	21/11/2018	Implementador / Asesor
Levantamiento de observaciones	4 días	22/11/2018	26/11/2018	Implementador
Segunda revisión de los avances	1 día	27/11/2018	27/11/2018	Implementador / Asesor
Levantamiento de observaciones	3 días	28/11/2018	30/11/2018	Implementador
Cuarta etapa - Capítulo III Desarrollo del proyecto	**34 días**	**4/03/2019**	**30/04/2019**	**-**
Elaboración de la metodología del proyecto (PDCA)	16 días	4/03/2019	26/03/2019	Implementador
Primera revisión de los avances	1 día	27/03/2019	27/03/2019	Implementador / Asesor
Levantamiento de observaciones	5 días	28/03/2019	9/04/2019	Implementador
Segunda revisión de los avances	1 día	10/04/2019	10/04/2019	Implementador / Asesor
Levantamiento de observaciones	7 días	11/04/2019	23/04/2019	Implementador
Tercera revisión de los avances	1 día	24/04/2019	24/04/2019	Implementador / Asesor
Levantamiento de observaciones	3 días	25/04/2019	30/04/2019	Implementador
Quinta etapa - Capítulo IV Pruebas y resultados	**35 días**	**6/05/2019**	**30/06/2019**	**-**
Elaboración de las "Pruebas" del proyecto (Aplicación del Framework en 3 empresas)	20 días	6/05/2019	31/05/2019	Implementador
Elaboración de los "Resultados" del proyecto (Auditoria del Framework en 3 empresas)	10 días	10/06/2019	24/06/2019	Implementador
Primera revisión de los avances	2 días	25/06/2019	26/06/2019.	Implementador / Asesor
Levantamiento de observaciones	3 días	27/06/2019	30/06/2019	Implementador
Sexta etapa - Capítulo V Discusiones y aplicaciones	**10 días**	**1/08/2019**	**21/08/2019**	**-**
Elaboración del Capítulo V	5 días	1/08/2019	9/08/2019	
Primera revisión de los avances	1 día	13/08/2019	13/08/2019	Implementador / Asesor
Levantamiento de observaciones	3 días	14/08/2019	20/08/2019	Implementador
Segunda revisión de los avances	1 día	21/08/2019	21/08/2019	Implementador / Asesor
Sétima etapa - Revisiones finales	**14 días**	**22/08/2019**	**12/09/2019**	**-**
Revisión general del proyecto	2 días	22/08/2019	23/08/2019	Implementador / Asesor
Levantamiento de observaciones	4 días	24/08/2019	29/08/2019	Implementador
Elaboración de presentación final	5 días	30/08/2019	3/09/2019	Implementador

Figura 21. Cronograma del proyecto

2.2 Métodos

El framework propuesto intenta ser un marco compacto, fácil de entender e implementar, asimismo, siguiendo las buenas prácticas que ofrece la industria, es importante que el marco de trabajo brinde procesos eficientes y retroactivos basándose en una gestión de la calidad.

2.4.1 Elección de la metodología

Se elaboró una comparación básica de las metodologías con el propósito de seleccionar una de manera objetiva en función a un sistema de puntuaciones.

La primera metodología en la comparación es desarrollada por el Instituto de Dirección de Proyectos (PMI, por sus siglas en inglés) y es una organización sin fines de lucro que certifica la profesión de dirección de proyectos a través de estándares reconocidos a nivel mundial. La conocida “Guía PMBOK” en su sexta edición, representa las buenas prácticas en la dirección de proyectos, asimismo, incluye la aplicación de estas buenas prácticas en proyectos agiles.

Las 10 áreas del conocimiento de la metodología PMBOK son Integración del proyecto, Gestión del alcance del proyecto, Gestión del tiempo del proyecto, Gestión de los costes del proyecto, Gestión de la calidad del proyecto, Gestión de los recursos humanos del proyecto, Gestión de las comunicaciones del proyecto, Gestión de los riesgos del proyecto, Gestión de las adquisiciones del proyecto, y Gestión de los interesados del proyecto. El costo de la guía oficial es de $ 99.00 dólares americanos (si eres miembro del PMI, tiene un valor de $ 49.50 dólares americanos).

Una ventaja de la metodología es el reconocimiento a nivel mundial, por lo tanto, es adaptable a cualquier tipo de proyectos y cualquier empresa. Por otro lado, la desventaja principal es la larga duración en la ejecución y finalización del proyecto debido a que involucra gran parte de las áreas de la organización.

SCRUM Alliance es una organización sin fines de lucro y es la encargada de difundir la metodología ágil con mayor aceptación desde hace varios años para el desarrollo de proyectos, en especial para el desarrollo de software. Las pequeñas y grandes empresas suelen utilizar SCRUM porque permite con un grupo reducido de personas, desarrollar y mantener los proyectos propuestos. La guía de SCRUM no tiene ningún costo y define los roles, eventos, artefactos y reglas que forman la estructura de la metodología.

La principal ventaja de SCRUM es la rapidez en el inicio y fin de los proyectos, asimismo, no es necesario un gran número de personas para el desarrollo. Sin embargo, se considera como una desventaja el alcance de su aplicación, quiere decir que, para proyectos más complejos es inevitable aplicar otra metodología.

La metodología PDCA, por sus siglas en inglés, es también conocida como ciclo PDCA o “Rueda de Deming”, es la metodología líder para implementar un sistema de gestión de la calidad. PDCA es un ciclo de solución de problemas, aumento de eficiencia y eficacia, aplicación de cambios y de mejora continua, logrando aumentar la satisfacción y fidelidad de los clientes internos y externos de una empresa.

PDCA tiene un valor agregado muy importante a considerar y es la relación directa con la norma ISO 9001 (Sistema de gestión de la calidad – requisitos). Esta norma brinda las directrices para poder implementar un sistema de gestión de calidad y se basa en esta metodología.

Finalmente, después de una breve descripción de las metodologías, se realizó la comparación respectiva considerando el rango de 1 al 5, siendo 1 como el nivel más bajo y 5 como el nivel más alto en la puntuación. La siguiente tabla muestra la valorización y elección de la metodología.

Tabla 10
Comparación metodologías

Características / Metodologías	Metodología PDCA (Mejora continua)	Metodología SCRUM (Desarrollo de Software)	Metodología PMBOK (Dirección de proyectos)
Realiza una planificación del proyecto	5	5	5
Desarrolla actividades cíclicas del proyecto	5	5	4
Evalúa constantemente las actividades del proyecto	5	5	4
Desarrolla el proyecto de una manera ágil	5	5	3
Corto alcance del proyecto en la organización	5	5	2
Compatibilidad con normas ISO	5	3	3
Total (Promedio)	5	4	3
Posición	1	2	3

Elaboración: El autor

Como se observa en la tabla anterior, la opción elegida es la metodología PDCA.

2.4.2 Metodología PDCA

(Camisón, Cruz, & Gonzáles, 2006) La metodología PDCA fue creada por el doctor Williams Edwards Deming, estadístico y encargado de difundir el concepto de calidad. PDCA es una estrategia de mejora continua que contempla las etapas de Planificar (*Plan*), Hacer (*Do*), Verificar (*Check*), y Actuar (*Act*), éstas se encuentran involucradas en cualquier proceso de una organización con el fin de lograr mejorar la calidad. La historia nos posiciona en Japón, en los años 50 donde se presenta la versión original de la metodología. Sin embargo, cuando la metodología fue puesta en práctica, se observaron deficiencias, lo que ocasionó una modificación de esta (figura 22).

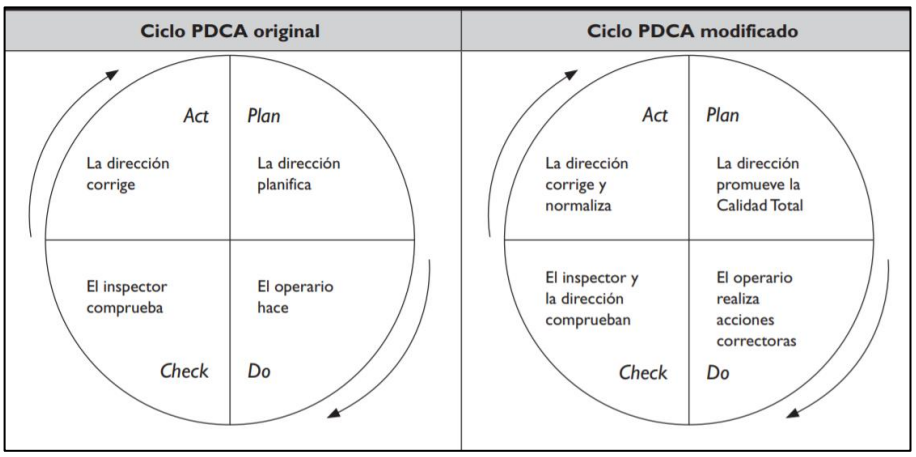


Figura 22. Ciclo PDCA evolución
Fuente: (Gestión de la calidad: Conceptos, enfoques, modelos y sistemas, 2006)

La metodología se compone de cuatro grandes etapas y son descritas a continuación.

- **Plan**

(Camisón, Cruz, & Gonzáles, 2006) La primera etapa define los objetivos que la empresa desea alcanzar con el fin de generar y proporcionar resultados. También, se establece los métodos a utilizar para alcanzar estos objetivos, es decir, identificar los medios necesarios, tales como normas técnicas y operativas. Analizar la situación actual, así como también, diseñar un plan de mejora o acción correctiva forman parte de esta primera fase.

- **Do**

(Camisón, Cruz, & Gonzáles, 2006) Esta etapa permite ejecutar todo lo planificado en la etapa anterior. Un factor clave de éxito es que los involucrados sepan aplicar las normas establecidas.

- **Check**

(Camisón, Cruz, & Gonzáles, 2006) La tercera proporciona la comprobación de los resultados, es decir, se valida si las actividades y procesos se están llevando a cabo de acuerdo con lo planificado. Esta comprobación se debe desarrollar de dos maneras, la primera es observar los trabajos en el mismo lugar donde se realizan, y la segunda, controlar los procesos y actividades observando los resultados.

- **Act**

(Camisón, Cruz, & Gonzáles, 2006) La cuarta etapa se define como la aplicación de una acción. En esta etapa se pueden dar dos situaciones distintas. Si se logró los resultados de manera satisfactoria de acuerdo con el plan establecido en la primera etapa, se deberá normalizar las actividades, procedimientos, y procesos, así como también, formalizar medidas correctoras si fuera necesario, para mantener el plan en el tiempo. Si no se alcanzó el objetivo del plan, se deberá identificar las falencias de las actividades y procesos, y las posibles causas que las producen, finalmente, se empezará un nuevo ciclo PDCA.

CAPÍTULO III
DESARROLLO DEL PROYECTO

En este capítulo, se elaboraron las actividades de la tesis utilizando las cuatro etapas de la metodología PDCA. El autor -en la figura 23- busca representar la relación e integración de la estructura de la norma ISO/IEC 27001 y marco de trabajo de ciberseguridad del NIST en función de la metodología PDCA.

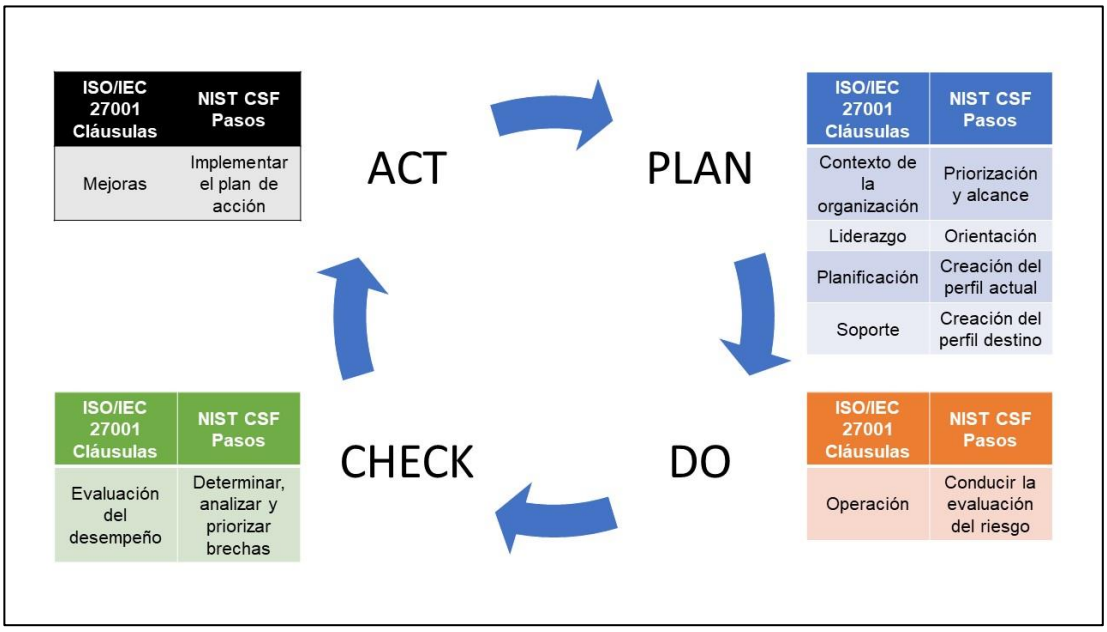


Figura 23. Integración PDCA vs ISO/IEC 27001 y NIST CSF
Elaboración: El autor

Asimismo, la figura 24 presenta la Estructura Desglosada de Trabajo o el EDT de la tesis donde se visualiza cada etapa del framework con sus respectivas actividades y documentos (entregables).

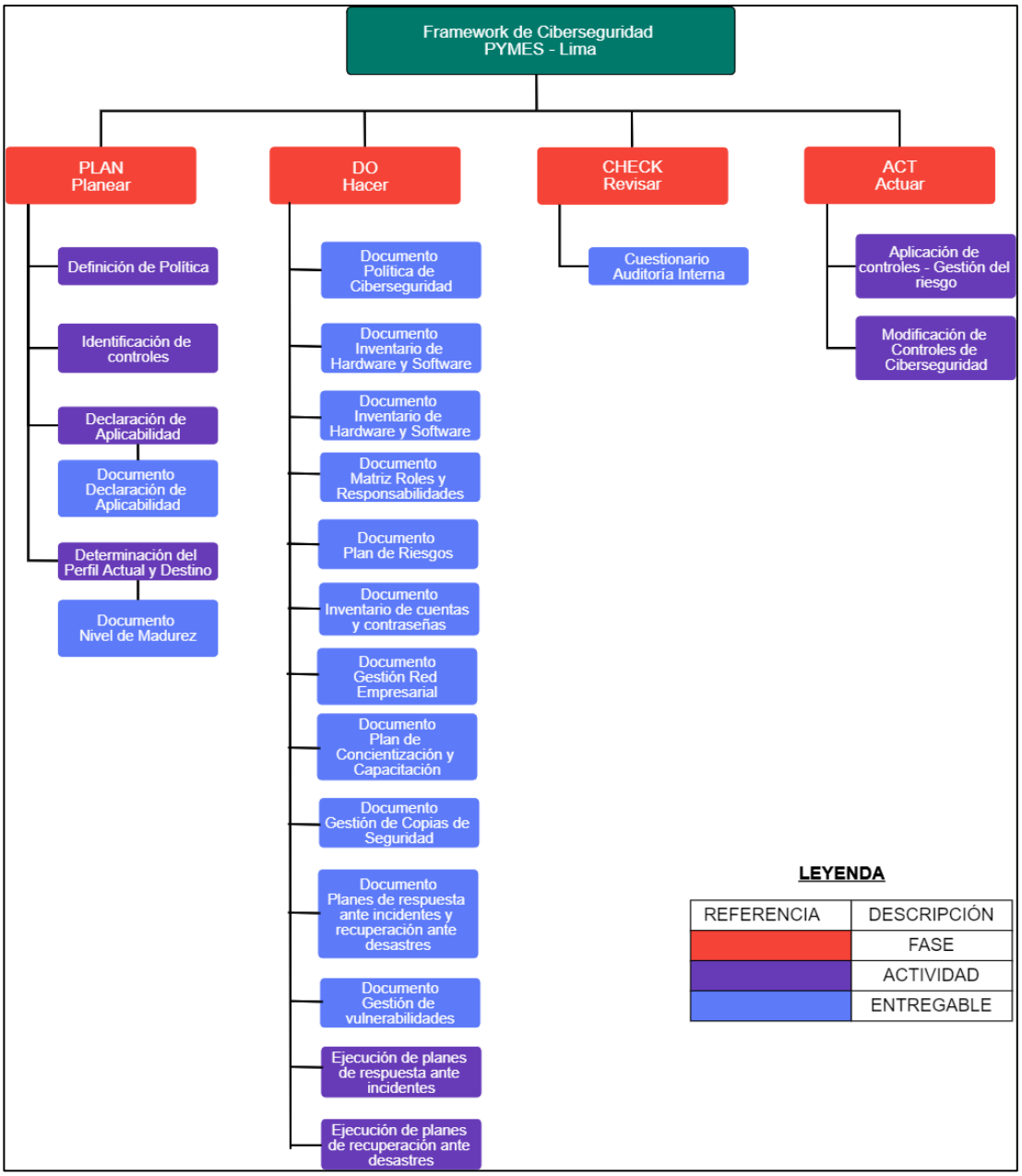


Figura 24. Estructura Desglosada de Trabajo - EDT
Elaboración: El autor

Las fases y actividades pertenecientes al EDT serán desarrolladas en los siguientes apartados.

3.1 Plan

En esta primera etapa, la empresa deberá crear una política definiendo su alcance y exponiendo el compromiso de protección de la información. Además, se definirá los controles de ciberseguridad y se creará los perfiles

actual y destino. La figura 25 muestra las actividades de esta primera etapa, así como también, los documentos o entregables que deberá ser elaborados.

Actividad	Descripción	Entregable
Definición de política	Documento que provee un marco para definir los objetivos, compromiso, y alcance de la empresa	Política de ciberseguridad
Identificación de controles	Documento que suministra información de los principales controles de ciberseguridad	Controles de ciberseguridad
Declaración de aplicabilidad	Documento que sustenta la implementación y exclusión de los controles de ciberseguridad	Declaración de aplicabilidad
Determinación del perfil actual y destino	Documento que proporciona los niveles de madurez de la empresa	Modelo de madurez

Figura 25. Actividades de la etapa PLAN
Elaborado por: El autor

3.1.1 Definición de política

La política es un documento formal que identifica los objetivos, alcances y compromisos de los miembros de la empresa. La política de ciberseguridad debe estar disponible y ser comunicada a todas las partes interesadas según sea conveniente. El primer control de ciberseguridad propuesto por el autor es la elaboración de una Política de ciberseguridad y es desarrollada en la etapa Do.

3.1.2 Identificación de controles

La identificación de controles de ciberseguridad se basa en la armonización de los controles de seguridad de información (ISO/IEC 27001) y de los controles críticos de seguridad (CIS). Asimismo, estos controles estarán bajo la estructura de las cinco funciones del NIST CSF. A continuación, se muestran los controles de ciberseguridad.

Función	Código	Control	Descripción	Referencia informativa
Identidad	ID-01	Política de ciberseguridad	Establecimiento de una política de ciberseguridad	ISO/IEC 27001:2013 A.5.1.1 NIST CSF ID-GV-1
	ID-02	Inventario de activos de hardware y software	Los dispositivos de hardware y los sistemas de información son inventariados	CIS CSC 1, 2 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST CSF ID.AM-1, ID.AM-2
	ID-03	Matriz de roles y responsabilidades	Los roles y responsabilidades de ciberseguridad se definen y asignan tanto para los colaboradores y entidades externas de la organización	CIS CSC 19 ISO/IEC 27001:2013 A.6.1.1 NIST CSF ID.AM-6
	ID-04	Plan de riesgos	La evaluación y tratamiento de los riegos estarán basados en una metodología de gestión del riesgo	NIST CSF ID.RM-1, ID.RM-2, ID.RM-3

Figura 26. Controles de ciberseguridad - Identidad
Elaboración: El autor

Función	Código	Control	Descripción	Referencia informativa
Proteger	PR-01	Gestión de cuentas de usuario y contraseñas	Las credenciales se gestionan, incluyendo un inventario y procedimientos	CISC CSC 4 ISO/IEC 27001:2013 A.9.2.1-A.9.2.4, A.9.3.1, A.9.4.3, A.9.2.5, A.9.2.6 NIST PR.AC-6
	PR-02	Gestión de la red empresarial	Limitar y controlar protocolos de red, servicios, segmentación de red deberán ser implementados	CIS CSC 9, 14, 15 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3 NIST CSF PR.AC-5
	PR-03	Plan de concientización y capacitación	Los colaboradores deberán participar en los programas de concientización y capacitación de ciberseguridad desarrolladas por la organización	CIS CSC 17 ISO/IEC 27001:2013 A.7.2.2 NIST CSF PR.AT-1
	PR-04	Gestión de copias de seguridad	Se deberá implementar un respaldo de información de los sistemas y aplicaciones, así mismo, deberá ser documentado y probado en la organización.	CIS CSC 10 ISO/IEC 27001:2013 A.12.3.1, NIST CSF PR.IP-4
	PR-05	Plan de respuesta ante incidentes y plan de recuperación ante desastres	Planes de respuesta ante incidentes y planes de recuperación ante desastres son probados, implementados y administrados	CIS CSC 19 ISO/IEC 27001:2013 A.16.1.5, A.17.1.1 - A.17.1.3 NIST CSF PR.IP-9, PR.IP-10

Figura 27. Controles de ciberseguridad – Proteger
Elaboración: El autor

Función	Código	Control	Descripción	Referencia informativa
Detectar	DE-01	Gestión de vulnerabilidades	Se deberá realizar una búsqueda de las vulnerabilidades y remediación de los activos identificados en el inventario de hardware y software	CIS CSC 3 ISO/IEC 27001:2013 A.12.6.1 NIST CSF DE.CM-8
Responder	RS-01	Ejecución de plan de respuesta ante incidentes	Los planes son ejecutados durante o después de un evento de ciberseguridad	CIS CSC 19 ISO/IEC 27001:2013 A.16.1.5 NIST CSF RS.RP-1
Recuperar	RC-01	Ejecución de plan de recuperación ante desastres	Los planes son ejecutados durante o después de un evento de ciberseguridad	CIS CSC 10 ISO/IEC 27001:2013 A.16.1.5 NIST CSF RC.RP-1

Figura 28. Controles de ciberseguridad - Detectar, Responder, Recuperar
Elaboración: El autor

El autor considera estos primeros controles para salvaguardar la información de las pequeñas y medianas empresas, sin embargo, el framework propuesto aplicará la mejora continua logrando la actualización constante de estos controles. Es decir, las empresas podrán adoptar nuevos controles de acuerdo con sus necesidades y requerimientos.

3.1.3 Declaración de aplicabilidad

La declaración de aplicabilidad es un documento perteneciente a la ISO/IEC 27001 cláusula 6.1.3d. En el proyecto, se utilizará para identificar la implementación y exclusión de los controles de ciberseguridad en una determinada empresa. La tabla 11 representa la plantilla de la declaración de aplicabilidad.

Tabla 11
Plantilla declaración de aplicabilidad

N°	Código	Control	Aplica	Justificación
#	*Código control*	*Nombre control*	*Si aplica / No aplica*	*Descripción*

Elaboración: El autor

3.1.4 Determinación del perfil actual y destino

El propósito de determinar el perfil actual y destino de la empresa en función de la ciberseguridad es conocer en qué estado se encuentra y así tomar decisiones que permitan reconocer deficiencias, esto se conoce como análisis de brechas.

Para lograrlo, se utilizó del modelo de integración de capacidad de madurez (CMMI, por sus siglas en inglés). Los niveles de madurez del CMMI se presentan en la figura 29.

Nivel	Descriptor	Descripción
1	Inexistente	Falta total de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver
2	Iniciado	Hay evidencia de que la organización ha reconocido que los problemas existen y que necesita ser resueltos, sin embargo, no hay procesos estandarizados, pero en cambio, hay métodos ad hoc que tienen a ser aplicados en forma individual
3	Definido	Los procedimientos han sido estandarizados, documentados y comunicados a través de capacitación, sin embargo, se ha dejado en manos de las personas el seguimiento de estos procesos, y es improbable que se detecten desviaciones
4	Gestionado	Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acciones donde los procesos parecen no estar funcionando efectivamente. Los procesos son constantemente mejorados y proveen buenas prácticas.
5	Optimizado	Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejora continua y diseño de madurez con otras organizaciones

Figura 29. Niveles de madurez CMMI
Elaboración: El autor

La tabla 12 representa la plantilla del perfil actual y destino de los controles de ciberseguridad.

Tabla 12
Plantilla nivel de madurez controles de ciberseguridad

Código	Control	Nivel madurez actual	Nivel madurez destino
Código control	*Nombre control*	*Inexistente / Iniciado / Definido / Gestionado / Optimizado*	*Iniciado / Definido / Gestionado / Optimizado*

Elaboración: El autor

3.2 Do

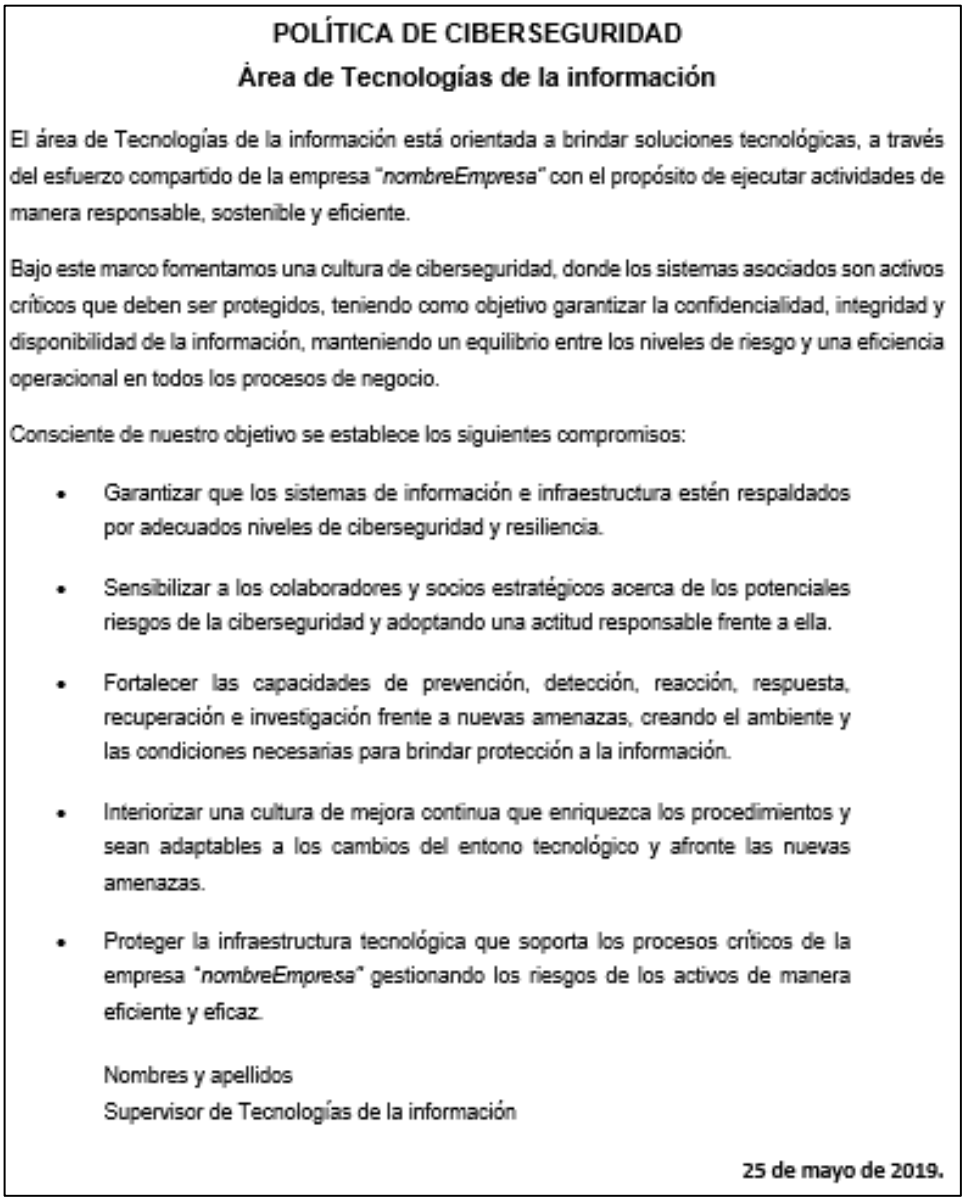
Esta fase se encarga del desarrollo de los controles de ciberseguridad.

3.2.1 Política de ciberseguridad

Esta política se basa en los lineamientos de la cláusula A.5.1.1 ISO/IEC 27001 y NIST CSC ID.GV-1. Deberá contemplar revisiones periódicas con el fin de asegurar su correcta aplicación. El documento propuesto se basa en las siguientes características.

- Identificación de objetivos y compromisos del área de TI.
- Alineado con los objetivos estratégicos de la empresa.
- Aprobado por la gerencia de la empresa.
- Difundido y comunicado a los colaboradores de la empresa.
- Deberá ser almacenada en un repositorio de datos y disponible para todos los colaboradores.

A continuación, se muestra en la figura 30 un modelo del documento respectivo.



POLÍTICA DE CIBERSEGURIDAD

Área de Tecnologías de la información

El área de Tecnologías de la información está orientada a brindar soluciones tecnológicas, a través del esfuerzo compartido de la empresa "*nombreEmpresa*" con el propósito de ejecutar actividades de manera responsable, sostenible y eficiente.

Bajo este marco fomentamos una cultura de ciberseguridad, donde los sistemas asociados son activos críticos que deben ser protegidos, teniendo como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información, manteniendo un equilibrio entre los niveles de riesgo y una eficiencia operacional en todos los procesos de negocio.

Consciente de nuestro objetivo se establece los siguientes compromisos:

- Garantizar que los sistemas de información e infraestructura estén respaldados por adecuados niveles de ciberseguridad y resiliencia.
- Sensibilizar a los colaboradores y socios estratégicos acerca de los potenciales riesgos de la ciberseguridad y adoptando una actitud responsable frente a ella.
- Fortalecer las capacidades de prevención, detección, reacción, respuesta, recuperación e investigación frente a nuevas amenazas, creando el ambiente y las condiciones necesarias para brindar protección a la información.
- Interiorizar una cultura de mejora continua que enriquezca los procedimientos y sean adaptables a los cambios del entono tecnológico y afronte las nuevas amenazas.
- Proteger la infraestructura tecnológica que soporta los procesos críticos de la empresa "*nombreEmpresa*" gestionando los riesgos de los activos de manera eficiente y eficaz.

Nombres y apellidos
Supervisor de Tecnologías de la información

25 de mayo de 2019.

Figura 30. Plantilla política de ciberseguridad
Elaboración: El autor

3.2.2 Inventario de activos de hardware y software

El inventario de activos de hardware y software es la herramienta básica y primordial que toda empresa debería elaborar. El inventario sugerido se basa en las siguientes características.

- Utilizar una herramienta de descubrimiento para identificar los dispositivos conectados a la red empresarial. La herramienta también deberá reconocer el software instalado en los dispositivos físicos.
- El inventario debe contemplar como mínimo los siguientes campos:
    - Código de inventario
    - Nombre de activo
    - Descripción
    - Propietario del activo
    - Estado
    - Tipo de activo
    - Características del activo
- Se debe documentar un procedimiento de las tareas respectivas al registro de un activo y cambios de estados respectivos.
- Se debe contemplar una lista blanca del software aprobado por la empresa. El software que no se encuentre en la lista blanca se considera prohibido.
- El inventario y lista blanca deben ser almacenados en un repositorio de datos disponible para el personal autorizado.

La plantilla del inventario propuesto se presenta en la tabla 13.

Tabla 13
Control Inventario de activos de hardware y software

COD	Nombre	Descripción	Propietario	Estado	Tipo	Hardware			Software		
						Dirección MAC	Dirección IP	S/N	Versión	Licencia	Fecha Adquisición
INV-HW/SW-XX	*Activo*	*Descripción*	*Nombre usuario*	*Operativo / Retirado / Mantenimiento*	*Hardware / Software*	*Dirección física*	*Dirección lógica*	*Número de serie*	*Versión del software*	*Cantidad de licencias / Key*	*Fecha de compra del activo*

Elaboración: El autor

3.2.3 Matriz de roles y responsabilidades

Se utilizó una matriz de asignación de responsabilidades, también llamada “matriz RACI” la cual permitió la identificación de roles y responsabilidades de los trabajadores de la empresa. A continuación, la matriz RACI del framework propuesto se encuentra en la tabla 14.

Tabla 14
Matriz RACI Framework Ciberseguridad

Roles / Responsabilidades	Oficial de ciberseguridad	Equipo de respuesta ante incidentes	Equipo de recuperación ante desastres	Gerente de TI	Gerencia general
Gestionar diariamente los controles de ciberseguridad	**R**	**-**	**-**	**C, I, A**	**I**
Seguridad física y tecnologías de la organización	**R**	**-**	**-**	**C, I, A**	**I**
Garantizar la ciberseguridad en la organización	**R**	**-**	**-**	**C, I, A**	**I**
Ejecutar actividades durante o después de un incidente de ciberseguridad	**I, A**	**R**	**C**	**I**	**I**
Ejecutar actividades durante o después de un desastre de ciberseguridad	**I, A**	**C**	**R**	**I**	**I**

Elaboración: El autor

Se debe documentar un procedimiento de control de cambios respectivo. Asimismo, la matriz RACI y ser almacenada en un repositorio de datos disponible para el personal autorizado.

3.2.4 Plan de riesgos

El objetivo del control es proteger los activos de la empresa ante las vulnerabilidades y amenazas identificadas. La gestión del riesgo debe

identificar una metodología que contemple la identificación de activos, amenazas, asimismo, definir la evaluación y el plan de tratamiento del riesgo.

Como punto de partida se selecciona la metodología MAGERIT. Con MAGERIT la empresa tiene un método sistemático para analizar y tratar los riesgos, así como también, una rápida implementación de las actividades de la gestión del riesgo. Por otro lado, la pequeña y mediana empresa debe tomar en cuenta un contexto básico (factores internos y externos) que permitirá sentar las bases del plan del riesgo de cada empresa.

- Contexto interno
    - Política General.
    - Estrategias y objetivos.
    - Cultura organizacional.
    - Política de ciberseguridad.
- Contexto externo
    - Factores económicos
        - Demanda y oferta de productos o servicios.
        - Demanda y oferta de moneda local y extranjera.
    - Factores tecnológicos
        - Nuevos sistemas de información.
        - Implementación en La Nube.
        - Conexiones remotas a través de redes privadas.
        - Seguridad informática y cibernética.
    - Factores legales
        - Leyes
        - Reglamentaciones

Finalmente, se presentan las actividades del plan de gestión del riesgo respectivo.

- **Valoración de activos**

Luego de realizar el inventario de activos, se deben valorizar los activos en función a las dimensiones de la seguridad de la información: confidencialidad (C), disponibilidad (D) e integridad (I). A continuación, la figura 31muestra el modelo de valor respectivo.

Activo de información				Dimensiones			
N°	Código	Activo	Descripción	C	D	I	Total
#	*Código del activo*	*Nombre del activo*	*Descripción del activo*	*1 / 2 / 3 / 4 / 5*	*1 / 2 / 3 / 4 / 5*	*1 / 2 / 3 / 4 / 5*	*Valor promedio*

Figura 31. Modelo de valor
Elaboración: El autor

- **Evaluación del riesgo**

El valor del riesgo es producto de las variables probabilidad de ocurrencia e impacto. Asimismo, se identifica el criterio de aceptación del riesgo dependiendo de la zona del riesgo en la que se encuentre. La figura 31 representa el mapa de riesgos respectivo.

Activo de información				Amenaza		Ocurrencia		Evaluación del riesgo	
N°	Código	Activo	Amenaza	Impacto	Valor	Probabilidad	Valor	Total	Zona de riesgo
#	*Código del activo*	*Nombre del activo*	*Lista de amenazas del activo*	*Insignificante / Menor / Dañino / Severo / Crítico*	*1 / 2 / 3 / 4 / 5*	*Raro / Improbable / Posible / Probable / Casi seguro*	*1 / 2 / 3 / 4 / 5*	*1 - 25*	*Baja / Moderada / Alta / Extrema*

Figura 32. Mapa de riesgos
Elaboración: El autor

- **Tratamiento del riesgo**

Después de evaluar los riesgos e identificar el criterio de aceptación del riesgo, se determinará los controles o salvaguardas para reducir, evitar, compartir o transferir los riesgos. A continuación, la figura 33 permite visualizar el plan de tratamiento del riesgo.

Activo de información						Tratamiento del riesgo		
N°	Código	Activo	Propietario del riesgo	Amenaza	Zona de riesgo	Control	Observación	Estado
#	*Código del activo*	*Nombre del activo*	*Dueño del riesgo del activo*	*Lista de amenazas del activo*	*Baja / Moderada / Alta / Extrema*	*Descripción del control*	*Comentarios*	*No iniciado / Pendiente / En progreso / Finalizado*

Figura 33. Plan de tratamiento del riesgo
Elaboración: El autor

3.2.5 Gestión de cuentas de usuario y contraseñas

El control tiene como objetivo principal administrar eficiente las cuentas usuarios y credenciales de acceso. La gestión incluye los siguientes parámetros.

- Las cuentas son referencias como objetos de directorio activo (Active Directory) e incluye, cuentas de administradores, usuarios y servicios.
- Las cuentas locales, bases de datos y aplicaciones también serán gestionadas.
- Las credenciales de las cuentas por defecto de los equipos de comunicación (servidores) y networking (switches, routers, firewalls, otros) deberán ser modificadas antes de ingresar a la red empresarial.
- Las credenciales sin excepción deberán cumplir con las siguientes características
    - Longitud mínima de 8 caracteres.
    - Deberá contener letras mayúsculas, minúsculas, números y caracteres especiales.
    - La vigencia de credenciales será de 4 meses.
- Todas las cuentas y contraseñas (excepción cuentas de usuarios) serán inventariadas.
- Un procedimiento debe ser elaborado y describirá los pasos a seguir para actualizar (agregar, modificar o eliminar) el inventario de cuentas.
- Los documentos deben contar con un procedimiento de copias de seguridad y control de cambios.

A continuación, la tabla 15 representa una plantilla del inventario propuesto.

Tabla 15
Plantilla de inventario de cuentas de usuario y contraseñas

N°	Usuario	Password	Dominio	Tipo de cuenta	Servicio asociado	Fecha de creación	Fecha de actualización
#	*Nombre de usuario*	*Contraseña de usuario*	*Nombre Dominio / Otros*	*Dominio / Local*	*Usuario / Servidor / Switch / Router / Firewall*	*Fecha de creación del usuario*	*Fecha de actualización de contraseña*

Elaboración: El autor

3.2.6 Gestión de la red empresarial

El objetivo del control es proteger la red empresarial. Los siguientes parámetros deberán ser considerados como actividades básicas en la organización.

- La red debe ser segmentada lógica y físicamente para limitar y controlar el acceso a los servicios empresariales. Se utilizan redes virtuales (VLAN) para diferenciar los segmentos de red respectivos.
- Se aplican restricciones de puertos de comunicación en los equipos de firewall. Es decir, se habilitan los puertos a demanda.
- Los puertos de los equipos de conmutación de red (switches) deberán ser encendidos y habilitados cuando se utilicen. Caso contrario, deben estar apagados e inhabilitados.
- Se debe contemplar una lista de las direcciones IP utilizadas en los dispositivos de red de la empresa.

3.2.7 Plan de concientización y capacitación

La empresa debe desarrollar un plan de concientización y capacitaciones en función de los riesgos, impactos y consecuencias de un ataque cibernético. Charlas mensuales y dinámicas de grupo son las principales actividades.

3.2.8 Gestión de copias de seguridad

El objetivo principal es respaldar los datos de la empresa. Se deben contemplar los siguientes parámetros.

- Utilizar una herramienta automatizada que realice las copias de seguridad (backup) de los archivos de un equipo, sistema, aplicación o servicio.
- El medio de backup debe tener capacidad para almacenar la información respectiva. El recurso de backup contempla discos duros, cintas magnéticas, solución en la nube.
- Se deberá contemplar una copia de seguridad adicional a modo de contingencia.
- Las tareas de copias de seguridad deben considerar los tipos de backup (full, incremental y/o diferencial).
- Las pruebas de integridad de las copias de seguridad deben ser ejecutadas y programadas en un intervalo de tiempo no menor a 6 meses.
- Un procedimiento debe ser elaborado que describa las tareas de backup y programación de las tareas de backup, asimismo, la identificación del recurso de backup y pruebas de integridad.

3.2.9 Planes de respuesta ante incidentes y recuperación ante desastres

El objetivo del control es identificar las actividades y responsabilidades del equipo de respuesta ante incidentes y recuperación ante desastres cibernéticos. Los planes deben considerar los siguientes parámetros.

- Identificación del equipo de respuesta ante incidentes.
- Identificación del equipo de recuperación ante desastres.
- Identificación de roles y responsabilidades de los equipos.
- Identificación de los canales de comunicación ante incidentes y desastres.
- Descripción de las tareas a realizar ante un incidente y desastre de ciberseguridad.

- Los documentos deberán contener copias de seguridad, control de cambios y estar disponibles cuando ocurra el evento respectivo.

3.2.10 Gestión de vulnerabilidades

La organización debe implementar un sistema de búsqueda y remediación de vulnerabilidades de los activos de hardware y software. Herramientas de código abierto (Open Source en inglés) tales como Arachni, OpenVAS, entre otras plataformas pueden ser utilizadas para escanear las vulnerabilidades de los equipos de red. Los valores del CVE (Common Vulnerabilities and Exposures) son las puntuaciones que reciben las vulnerabilidades y deben ser remediadas de acuerdo a su nivel de criticidad (Riesgo Alto, Riesgo Medio, Riesgo Bajo).

Un procedimiento que describa las tareas de la gestión de vulnerabilidades debe ser elaborado. Asimismo, el documento debe contener una copia de seguridad y control de cambios.

3.2.11 Ejecución de plan de respuesta ante incidentes

El control es una referencia de la acción de poner en marcha los planes de respuesta ante incidentes de ciberseguridad. Las actividades del plan deben ser ejecutados durante o después del evento.

Una vez ejecutadas las tareas descritas en el plan y, confirmar que el incidente de ciberseguridad fue controlado y resuelto, se identifican nuevas oportunidades y se corregirán las deficiencias encontradas con el propósito de actualizar el plan.

3.2.12 Ejecución de plan de recuperación ante desastres

Así como en el control anterior, el control 3.2.12 es poner en marcha las actividades descritas en los planes de recuperación ante desastres de ciberseguridad.

Después de ejecutar las tareas descritas en el plan y, validar la recuperación exitosa o no de la información, se identifican nuevas oportunidades y se corregirán las deficiencias encontradas con el propósito de actualizar el plan.

3.3 Check

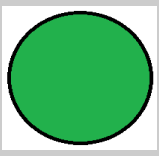
La siguiente etapa permitirá realizar una auditoría interna que evalúa el desempeño de la ciberseguridad en la organización con el propósito de identificar brechas. Esta actividad se basa en la cláusula 9 de la ISO/IEC 27001 (9.2 auditoría interna), y deberá ser ejecutada, como mínimo, una vez al año. La auditoría debe contemplar lo siguiente.

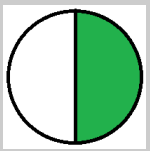
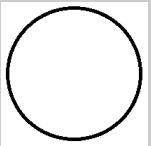
- Imparcial elección del equipo auditor.
- Brindar conformidad de la implementación de los controles de ciberseguridad.
- Almacenar la información como evidencia del procedimiento y resultados de la auditoría.
- Exponer retroalimentación y oportunidades de mejora continua.

Se utilizó un cuestionario como herramienta para reunir la información y realizar el análisis respectivo. La persona responsable del área de sistemas fue la encargada de responder el cuestionario. También, se representará de manera gráfica, el porcentaje de cumplimiento.

A continuación, la tabla 16 muestra la descripción del estado de cumplimiento y la tabla 17 el cuestionario propuesto.

Tabla 16
Auditoría interna porcentajes de cumplimiento

Ítem	Descripción	Porcentaje de cumplimiento (%)	Gráfica
Totalmente cubierto	Los requerimientos de los controles de ciberseguridad están totalmente cubiertos.	100%	

Considerablemente cubierto	Falta realizar algunas tareas y actividades para cubrir totalmente los requerimientos de los controles de ciberseguridad.	75%	
Parcialmente cubierto	Se han realizado tareas y actividades que cubren parcialmente los requerimientos de los controles de ciberseguridad.	50%	
Limitadamente cubierto	Se han realizado algunas tareas y actividades para cubrir los requerimientos de los controles de ciberseguridad.	25 %	
No cubierto	No se ha realizado ninguna actividad en función de los requerimientos de los controles de ciberseguridad.	0%	

Elaboración: El autor

Tabla 17
Auditoría interna cuestionario

N°	Control	Consultas	Respuestas	Observaciones	Recomendaciones	Cumplimiento (%)
	ID-01 Política de ciberseguridad	*¿Existe un documento de política de ciberseguridad que identifique objetivos y compromisos aprobada por la gerencia?* *¿La política de ciberseguridad es difundida y comunicada a los colaboradores de la empresa?* *¿Existe un procedimiento de respaldo del documento?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*

N°	Control	Consultas	Respuestas	Observaciones	Recomendaciones	Cumplimiento (%)
	ID-02 Inventario de hardware y software	*¿Existe un inventario de activos de hardware y software?* *¿Existe un procedimiento que controle los cambios del inventario?* *¿Existe una lista blanca de software y aplicaciones?* *¿Cuenta con un procedimiento de respaldo del documento?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*
	ID-03 Matriz de roles y responsabilidades	*¿Se han creado roles para identificar las diferentes responsabilidades sobre la ciberseguridad?* *¿Existe un documento donde estén registrados los roles y responsabilidades?* *¿Existe un procedimiento que registre las modificaciones y/o actualizaciones?* *¿Existe un procedimiento de respaldo del documento?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*
	ID-04 Plan de riesgos	*¿Existe un plan de riesgos?* *¿Existe un procedimiento de control de cambios?* *¿Existe un procedimiento de respaldo de los documentos?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*
	PR-01 Gestión de cuentas de usuarios y contraseñas	*¿Existe un inventario de cuentas y contraseñas de usuarios?* *¿Se modifica las contraseñas de las cuentas por defecto?* *¿Existen restricciones en la elaboración de contraseñas?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*

N°	Control	Consultas	Respuestas	Observaciones	Recomendaciones	Cumplimiento (%)
	PR-02 Gestión de la red empresarial	*¿Se realiza una segmentación lógica y física en la red empresarial?* *¿Existen redes virtuales VLAN para dividir los segmentes de red?* *¿Todos los puertos de red de los switches se encuentran habilitados?* *¿Todos los puertos de comunicación están habilitados en el equipo firewall?* *¿La red inalámbrica se encuentra en una red virtual y habilitada con protocolos de seguridad?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*
	PR-03 Plan de concientización y capacitación	*¿Existen planes de concientización y capacitación de ciberseguridad para los colaboradores?* *¿Cuál es la frecuencia de las capacitaciones?* *¿Cuándo fue la última capacitación?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*
	PR-04 Gestión de copias de seguridad	*¿Se realiza copias de seguridad de los archivos de los equipos, sistemas, aplicaciones o servicios?* *¿Utilizan una herramienta automatizada o labor manual para realizar la copia de seguridad?* *¿Cuál es la frecuencia de backup?* *¿Cuál es el medio utilizado para almacenar la copia de seguridad?* *¿Cuáles son los tipos de backup configurados?* *¿Existen duplicados de las copias de seguridad como medida preventiva?* *¿Se realizan pruebas de restauración del backup para comprobar la integridad de los datos?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*

N°	Control	Consultas	Respuestas	Observaciones	Recomendaciones	Cumplimiento (%)
	PR-05 Plan de respuesta ante incidentes y plan de recuperación ante desastres	*¿Existe un plan de respuesta ante incidentes de ciberseguridad? ¿El plan de respuesta ante incidentes se encuentra disponible y cuenta con una copia de seguridad? ¿Existe un plan de recuperación ante desastres de ciberseguridad? ¿Los roles y responsabilidades del equipo de recuperación ante desastres se encuentran identificados?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*
	DE-01 Gestión de vulnerabilidades	*¿Se realiza una búsqueda de vulnerabilidades de los activos a través de un software? ¿Cuál es la frecuencia del proceso de búsqueda de vulnerabilidades? ¿Existe un procedimiento que describa las actividades de la búsqueda y remediación de vulnerabilidades?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*
	RS-01 Ejecución de plan de respuesta ante incidentes	*¿Existe un control cambios en el plan de respuesta ante incidentes después de finalizar las actividades ante un evento de ciberseguridad?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*
	RC-01 Ejecución de plan de recuperación ante desastres	*¿Existe un control cambios en el plan de recuperación ante desastres después de finalizar las actividades ante un evento de ciberseguridad?*	*Respuesta del entrevistado*	*Observaciones encontradas por el auditor interno*	*Sugerencias del auditor interno*	*0% / 25% / 50% / 75% / 100%*

Elaboración: El autor

3.4 Act

En esta etapa, se aplican los controles y salvaguardas identificados en el tratamiento del riesgo y las oportunidades encontradas en la auditoría interna. También, se deberá evaluar si la empresa requiere nuevos controles de ciberseguridad, es decir, se analizan nuevamente las subcategorías del NIST CSF, los controles CIS y los controles de seguridad de la información, con el fin de insertarlos y documentarlos en la declaración de aplicabilidad.

Finalmente, debido a que el framework contempla la mejora continua por medio de la metodología PDCA, se ejecutaron nuevamente las actividades con los nuevos controles y brechas identificadas en las etapas anteriores.

CAPÍTULO IV
PRUEBAS Y RESULTADOS

En el capítulo IV, se presentan las pruebas y resultados de los objetivos de la tesis.

4.1 Pruebas

Las pruebas realizadas para lograr los objetivos específicos se presentan a continuación.

4.1.1 Identificar, evaluar y armonizar las características de las normas y controles relacionados con la ciberseguridad

El desarrollo de la primera etapa del framework evidencia la esencia del objetivo específico 1. La figura 34 representa gráficamente lo realizado.

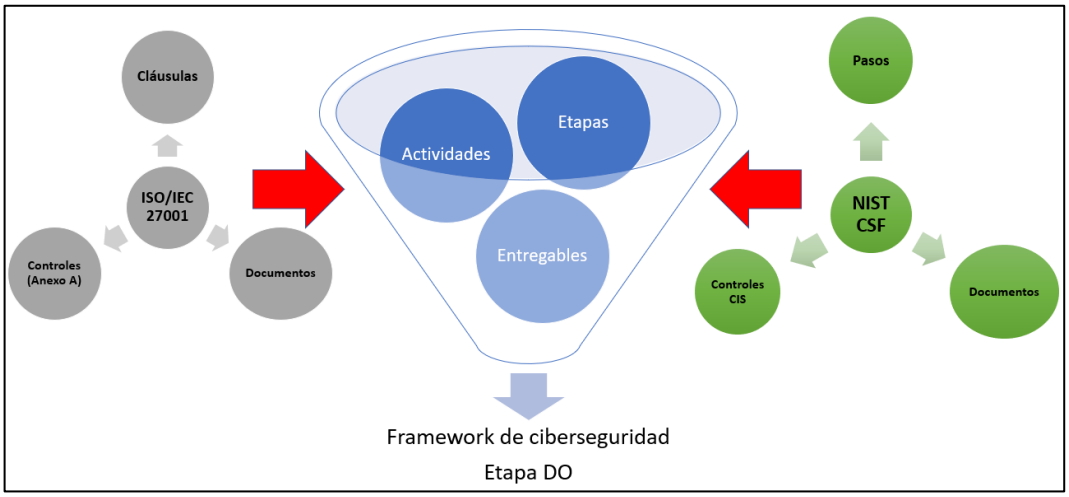


Figura 34. Representación objetivo específico 1
Elaboración: El autor

4.1.2 Elaborar las actividades y desarrollar entregables del framework de ciberseguridad

El segundo objetivo específico se fundamenta en la construcción del marco de trabajo propuesto, es decir, desarrollar las etapas, actividades y documentos necesarios para implementar el framework.

La figura 35 representa gráficamente la elaboración de las actividades que se realizaron en función a la metodología elegida, es decir, la metodología PDCA que permitirá la mejora continua del framework propuesto.

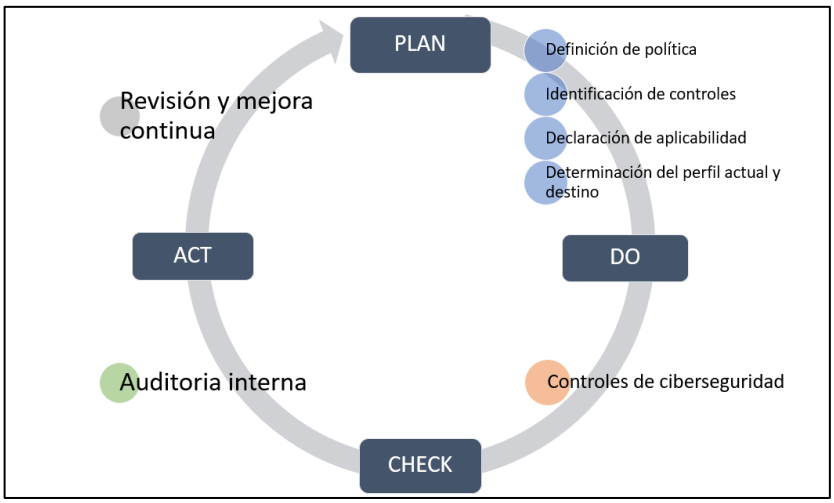


Figura 35. Etapas y actividades Framework de ciberseguridad
Elaboración: El autor

4.1.3 Aplicar el framework en una empresa para demostrar del modelo sugerido

El último objetivo específico permite demostrar el funcionamiento del framework de ciberseguridad, para lograrlo se aplicó el marco de trabajo en una empresa. Xentic S.A.C es una empresa que brinda servicios tecnológicos, tales como seguridad, networking, infraestructura entre otros. El anexo 1 contiene el detalle de la información de la empresa.

El desarrollo del framework se inició elaborando la declaración de aplicabilidad, es decir, la empresa justificó la implementación o exclusión de los controles de ciberseguridad. Después, se definió el perfil actual y destino de las empresas. Finalmente, se implementaron los controles de ciberseguridad durante el desarrollo de la tesis según la disponibilidad del personal encargado.

- **Declaración de aplicabilidad**

La siguiente figura representa el documento “declaración de aplicabilidad” de la empresa elegida.

N°	Código	Control	Aplica	Justificación
1	ID-01	Política de ciberseguridad	Aplica	*El área de sistemas debe contar con una política de seguridad cibernética para establecer lineamientos*
2	ID-02	Inventario de activos de hardware y software	Aplica	*Administrar correctamente los activos de hardware y software es importante para la empresa*
3	ID-03	Matriz de roles y responsabilidades	Aplica	*Las funciones y las personas encargadas de las actividades de ciberseguridad deben estar documentadas*
4	ID-04	Plan de riesgos	Aplica	*Identificar amenazas y vulnerabilidades de los activos es minimizar los ataques de ciberseguridad*
5	PR-01	Gestión de cuentas de usuario y contraseñas	Aplica	*Administrar las credenciales de acceso de los usuarios es controlar sus identidades en la red empresarial*
6	PR-02	Gestión de la red empresarial	Aplica	*Restringir el uso y acceso de dispositivos en la red empresarial permitirá reducir un ataque cibernético*
7	PR-03	Plan de concientización y capacitación	Aplica	*Capacitaciones a los colaboradores en función de la ciberseguridad ayudará a tomar conciencia de los riesgos identificados*
8	PR-04	Gestión de copias de seguridad	Aplica	*Recuperar los datos de los sistemas e información de clientes es crucial para la continuidad de la empresa*
9	PR-05	Plan de respuesta ante incidentes y plan de recuperación ante desastres	Aplica	*Establecer procedimientos ante los eventos de ciberseguridad brindará una respuesta proactiva*
10	DE-01	Gestión de vulnerabilidades	Aplica	*Actualizar los sistemas operativos de los equipos es parte de las funciones del área de sistemas*
11	RS-01	Ejecución de plan de respuesta ante incidentes	Aplica	*Mejorar los procedimientos ante los incidentes de ciberseguridad deben ser aplicados por el área de sistemas*
12	RC-01	Ejecución de plan de recuperación ante desastres	Aplica	*Mejorar los procedimientos ante los desastres de ciberseguridad deben ser aplicados por el área de sistemas*

Figura 36. Declaración de aplicabilidad empresa
Elaboración: El autor

- **Perfil actual y destino**

A continuación, se muestra el nivel de madurez de los controles de ciberseguridad en función del estado actual y destino de la empresa seleccionada.

Para realizar esta actividad, se utilizaron los niveles de madurez del CMMI. Estos niveles son: Inexistente, Iniciado, Definido, Gestionado y Optimizado.

N°	Código	Control	Nivel madurez actual	Nivel madurez destino
1	ID-01	Política de ciberseguridad	Inexistente	Definido
2	ID-02	Inventario de activos de hardware y software	Inexistente	Definido
3	ID-03	Matriz de roles y responsabilidades	Inexistente	Definido
4	ID-04	Plan de riesgos	Inexistente	Definido
5	PR-01	Gestión de cuentas de usuario y contraseñas	Inexistente	Definido
6	PR-02	Gestión de la red empresarial	Inexistente	Definido
7	PR-03	Plan de concientización y capacitación	Inexistente	Definido
8	PR-04	Gestión de copias de seguridad	Inexistente	Definido
9	PR-05	Plan de respuesta ante incidentes y plan de recuperación ante desastres	Inexistente	Definido
10	DE-01	Gestión de vulnerabilidades	Inexistente	Definido
11	RS-01	Ejecución de plan de respuesta ante incidentes	Inexistente	Definido
12	RC-01	Ejecución de plan de recuperación ante desastres	Inexistente	Definido

Figura 37. Perfil actual y destino empresa
Elaboración: El autor

De la imagen anterior, se visualiza que la empresa Xentic no tiene implementado ningún control, es decir, no reconocen que son vulnerables a un ataque de ciberseguridad. Por lo tanto, establecieron el nivel “definido” como perfil destino, quiere decir, desean concretar procedimientos documentados y estandarizados.

- **Desarrollo de controles de ciberseguridad**

Los controles de ciberseguridad se desarrollaron e implementaron de acuerdo con la disponibilidad del personal a cargo. La empresa XENTIC logró implementar todos los controles. Los anexos 2 hasta el 12 permiten visualizar el desarrollo de los controles en la empresa.

4.2 Resultados

La evidencia del logro de los objetivos se sustenta en los resultados de la auditoría interna realizada en la empresa. Es decir, se evaluó el grado de cumplimiento de los controles de ciberseguridad. La siguiente figura muestra los resultados.

N°	Código	Control	Cumplimiento (%)	Nivel madurez actual	Nivel madurez destino	Observaciones
1	ID-01	Política de ciberseguridad	100 %	Inexistente	Definido	El documento fue elaborado y aprobado por la gerencia de la empresa
2	ID-02	Inventario de activos de hardware y software	100 %	Inexistente	Definido	El inventario y el procedimiento fueron elaborados y aplicados en la empresa
3	ID-03	Matriz de roles y responsabilidades	100 %	Inexistente	Definido	La matriz de roles y responsabilidades fue desarrollada y aplicada
4	ID-04	Plan de riesgos	100%	Inexistente	Definido	La valoración y evaluación de activos, así como el tratamiento de riegos fue identificado y elaborado
5	PR-01	Gestión de cuentas de usuario y contraseñas	100%	Inexistente	Definido	El inventario de cuentas y el procedimiento fueron elaborados y aplicados en la empresa
6	PR-02	Gestión de la red empresarial	100%	Inexistente	Definido	Las configuraciones de red fueron aplicadas en la empresa
7	PR-03	Plan de concientización y capacitación	100%	Inexistente	Definido	Se elaboró un cronograma y dictó charlas de ciberseguridad a los colaboradores
8	PR-04	Gestión de copias de seguridad	100%	Inexistente	Definido	El procedimiento y ejecución de tareas de Backup se implementaron
9	PR-05	Plan de respuesta ante incidentes y plan de recuperación ante desastres	100%	Inexistente	Definido	Se elaboraron planes y tareas ante incidentes y desastres de ciberseguridad
10	DE-01	Gestión de vulnerabilidades	100%	Inexistente	Definido	Se elaboró un procedimiento y aplicó el escaneo de vulnerabilidades en la red

Figura 38. Resultados auditoría interna empresa
Elaboración: El autor

CAPÍTULO V
DISCUSIONES Y APLICACIONES

En el último capítulo, se analizaron los resultados de los objetivos de la tesis, así como también, se proponen nuevas aplicaciones para el trabajo de investigación.

5.1 Discusión de resultados del proyecto

En esta sección, se describen los resultados obtenidos de los objetivos de la tesis.

5.1.1 Desarrollar un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima

La principal justificación para el desarrollo del proyecto es la falta de conocimiento de las pequeñas y medianas empresas en el Perú ante un ataque cibernético. El autor considera al framework como una base importante para que las empresas tomen conciencia y puedan aplicar los controles de ciberseguridad para proteger su información.

5.1.2 Identificar, evaluar y armonizar las características de las normas y controles relacionados con la ciberseguridad

Las normas ISO 27k, el NIST CSF y los controles CIS usados en el presente proyecto, fueron seleccionados debido al gran impacto positivo que tienen en la industria. Las grandes empresas tienen como fortaleza la implementación de estas herramientas para contrarrestar los eventos de ciberseguridad y seguridad de la información. El autor de la tesis basa su framework propuesto en las bondades de cada herramienta con el fin de entregar una solución compacta y con un origen reconocido por las empresas a nivel mundial.

5.1.3 Elaborar las actividades y desarrollar entregables del framework de ciberseguridad

La importancia de la retroalimentación, es decir, la mejora continua en los procesos de una empresa es de vital importancia para poder entregar un servicio de calidad. La metodología PDCA es la más utilizada e importante en todas las empresas a nivel mundial. Las fases permiten planear, ejecutar, revisar y actuar de manera eficiente la mejora de procesos de una empresa. El autor considera esta metodología como pieza clave de éxito para el framework propuesto porque las actividades y procedimientos estarán en constante actualización permitiendo una mejor implementación en una determinada empresa.

5.1.4 Aplicar el framework en una empresa para demostrar el modelo sugerido

La principal razón de la elaboración del framework de ciberseguridad propuesto es brindar una herramienta práctica, eficiente y fácil de entender para salvaguardar la información de las PYMES en la ciudad de Lima. Para probar la funcionalidad del marco de trabajo, las fases y actividades del framework fueron aplicados en una empresa. El resultado final fue la implementación de los controles de ciberseguridad logrando a su vez, concientizar de manera progresiva la importancia de gestionar la seguridad cibernética.

5.2 Aporte y otras aplicaciones del proyecto

El principal aporte que genera la sustentación de la tesis, es decir, el desarrollo de un framework de ciberseguridad es la concientización de las personas en función de la seguridad cibernética. Por otro lado, el marco de trabajo podría servir como un primer paso hacia un proceso de certificación de la norma ISO/IEC 27001 debido a que el framework propuesto se basa en algunos lineamientos, directrices y controles de la norma.

CONCLUSIONES

1. El desarrollo del framework de ciberseguridad logró la implementación de los controles de ciberseguridad que permitirán la protección de la información de las PYMES en Lima.

2. El análisis y levantamiento de información de las normas y controles relacionados con la ciberseguridad, permitió consolidar las características más resaltantes de estos logrando sentar las bases del framework propuesto.

3. Las fases del framework de ciberseguridad se fundamentaron en las etapas de la metodología PDCA, obteniendo un proceso de mejora continua en las actividades del marco de trabajo elaborado.

4. Aplicando el framework de ciberseguridad, permitió la concientización de los colaboradores con el objetivo de proteger la información de la empresa.

RECOMENDACIONES

1. Todas las empresas deberían considerar capacitaciones de ciberseguridad en horarios dentro y fuera de oficina para los colaboradores con el objetivo de reforzar la importancia de gestionar la seguridad cibernética.

2. Las empresas necesitarán de invertir en dispositivos tecnológicos para almacenar los datos de manera interna y externa. El objetivo principal es contemplar la información después de sufrir un ataque cibernético.

3. Las PYMES deberían realizar periódicamente una auditoría interna porque es fundamental conocer el estado actual y analizar mejoras en la gestión de la ciberseguridad para permitir la mejora continua que el framework propone en su ciclo de vida.

FUENTES DE INFORMACIÓN

Bibliográficas:

Camisón, C., Cruz, S., & Gonzáles, T. (2006). *Gestión de la calidad: Conceptos, enfoques, modelos y sistemas.* Madrid: Pearson Educación S.A.

Center for Internet Security. (2018). CIS Controls.

Consejo Superior de Administración Electrónica. (2012). MAGERIT V3.

INACAL. (Noviembre de 2014). NTP-ISO/IEC 27001. *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información. Requisitos*.

International Organization for Standardization. (2011). ISO/IEC 27005.

ISO/IEC. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary.

National Institute of Standards and Technology. (Abril de 2018). Framework for Improving Critical Infrastructure Cybersecurity 1.1.

NTE. (Diciembre de 2015). ISO/IEC 27032. *Tecnologías de la información - Técnicas de seguridad - Directrices para ciberseguridad*.

Taipe Domínguez, D. (4 de Agosto de 2017). La auditoría de seguridad informática y su relación en la ciberseguridad de la fuerza aérea del Perú. Lima, Lima, Perú.

UNE. (Julio de 2015). UNE-ISO/IEC 27002. *Tecnología de la información - Técnicas de seguridad - Códigos de prácticas para los controles de seguridad de la información*.

Electrónicas:

Agencia Peruana de Noticias. (24 de Abril de 2019). *Andina*. Obtenido de Andina Web site: https://andina.pe/agencia/noticia-cade-digital-inversion-ciberseguridad-pymes-es-desde-5-soles-al-mes-749481.aspx

Diario Gestión. (25 de Abril de 2018). *Gestión.pe*. Obtenido de Gestión.pe: https://gestion.pe/tecnologia/ciberseguridad-pymes-son-empresas-protegidas-america-latina-232266-noticia/

ESET. (Diciembre de 2018). Security Report Latinoamérica. Buenos Aires, Argentina. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

Macha Moreno, E., & Inoguchi Rojas, A. (10 de Octubre de 2017). Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú. Lima, Lima, Perú. Obtenido de Repositorio Usil Edu: http://repositorio.usil.edu.pe/bitstream/USIL/2810/1/2017_Inoguchi_Gestion-de-la-ciberseguridad.pdf

Zuñiga Figueroa, J. (20 de Abril de 2017). *Repositorio ICTE Ejército.* Obtenido de Repositorio ICTE Ejército: http://repositorio.icte.ejercito.mil.pe/bitstream/ICTE/32/1/Tesis%20Bach.%20Zu%C3%B1iga%20Figueroa%2C%20Jesus%20Rolando.pdf

Anexo 01: Descripción Xentic S.A.C

Xentic S.A.C. es una empresa integradora de soluciones tecnológicas creada en el año 2009 y cuenta con un equipo de profesionales certificados en distintas marcas tecnológicas. Las áreas que comprenden la empresa son Gerencia, recursos humanos, ventas y operaciones TI.

La empresa se encuentra ubicada en el distrito de Jesús María, en la dirección Avenida Faustino Sánchez Carrión N°611-615 piso 5 - oficina 506 (figura 14).

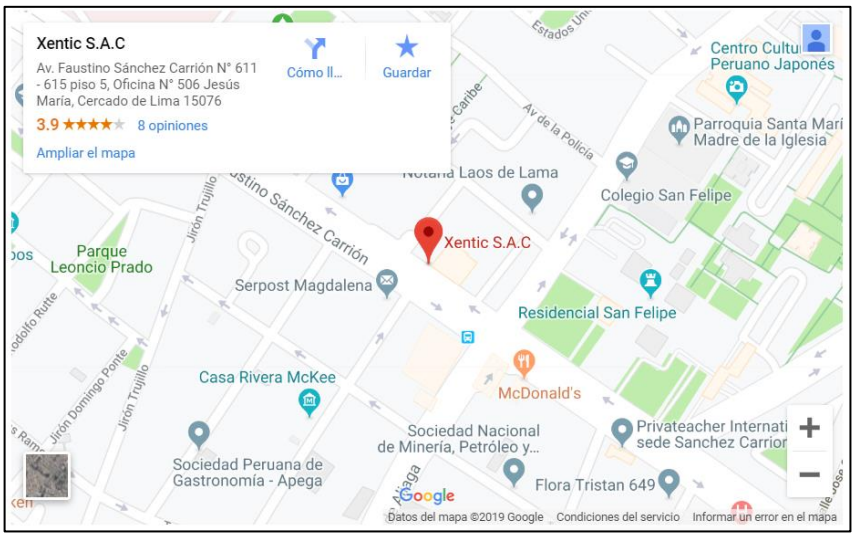


Figura 39. Ubicación geográfica empresa Xentic S.A.C.
Fuente: Mapas de Google

El portafolio de servicios de Xentic se presenta en la figura 15. Son 8 servicios y varían desde infraestructura TI hasta capacitaciones.

Figura 40. Portafolio de servicios empresa Xentic S.A.C.

Anexo 02: ID-01 Política de ciberseguridad

A continuación, se presenta el documento Política de ciberseguridad de la empresa Xentic.

Política de ciberseguridad - Xentic

Política de ciberseguridad

Área de sistemas

El propósito del área de sistemas es soportar tecnológicamente los procesos de las áreas de la empresa Xentic S.A.C. Asimismo, proteger los activos de información es fundamental para contrarrestar los posibles ataques de seguridad cibernética, es por tal motivo, que se establecen los siguientes compromisos en función de la ciberseguridad:

- Identificar y proteger los activos de información.
- Respaldar los datos e información de los sistemas a través copias de seguridad.
- Sensibilizar a todos los colaboradores y socios estratégicos acerca de los riesgos y ataques de ciberseguridad.
- Reforzar las capacidades de prevención, detección y respuesta frente a nuevas amenazas de los activos y sistemas de información.

John Rentería

Coordinador de Sistemas

Mayo de 2019.

Anexo 03: ID-02 Inventario de activos de hardware y software

A continuación, se presenta el inventario de los activos de hardware y software de la empresa Xentic, asimismo, el procedimiento respectivo.

Inventario - Xentic

COD	Nombre	Descripción	Propietario	Estado	Tipo	Hardware			Software		
						Fabricante	Dirección IP	S/N	Versión	Licencia	Fecha Adquisición
HAR-001	LXEN-IT001	Laptop área sistemas	Sistemas 01	Operativo	Hardware Laptop	Lenovo	IP DHCP	-	-	OEM	-
HAR-002	LXEN-IT002	Laptop área sistemas	Sistemas 02	Operativo	Hardware Laptop	Lenovo	IP DHCP	-	-	OEM	-
HAR-003	LXEN-IT003	Laptop área sistemas	Sistemas 03	Operativo	Hardware Laptop	Lenovo	IP DHCP	-	-	OEM	-
HAR-004	LXEN-IT004	Laptop área sistemas	Sistemas 04	Operativo	Hardware Laptop	Lenovo	IP DHCP	-	-	OEM	-
HAR-005	LXEN-IT005	Laptop área sistemas	Sistemas 05	Operativo	Hardware Laptop	Lenovo	IP DHCP	-	-	OEM	-
HAR-006	LXEN-IT006	Laptop área sistemas – SPARE	Sistemas 01	Almacén	Hardware Laptop	Lenovo	IP DHCP	-	-	OEM	-
HAR-007	LXEN-IT007	Laptop área sistemas	Sistemas 06	Operativo	Hardware Laptop	Lenovo	IP DHCP	-	-	OEM	-
HAR-008	LXEN-IT008	Laptop área sistemas SPARE	Sistemas 01	Mantenimiento	Hardware Laptop	Lenovo	IP DHCP	-	-	OEM	-
HAR-009	DXEN-VEN001	Desktop área ventas	Ventas 01	Operativo	Hardware Desktop	Lenovo	IP DHCP	-	-	OEM	-
HAR-010	DXEN-VEN002	Desktop área ventas	Ventas 02	Operativo	Hardware Desktop	Lenovo	IP DHCP	-	-	OEM	-
HAR-011	DXEN-VEN003	Desktop área ventas	Ventas 03	Operativo	Hardware Desktop	Lenovo	IP DHCP	-	-	OEM	-
HAR-012	DXEN-VEN004	Desktop área ventas	Ventas 04	Operativo	Hardware Desktop	Lenovo	IP DHCP	-	-	OEM	-

COD	Nombre	Descripción	Propietario	Estado	Tipo	Hardware			Software		
						Fabricante	Dirección IP	S/N	Versión	Licencia	Fecha Adquisición
HAR-013	DXEN-ADM001	Desktop área administración	Administración 01	Operativo	Hardware Desktop	Lenovo	IP DHCP	-	-	OEM	-
HAR-014	DXEN-ADM002	Desktop área administración	Administración 02	Operativo	Hardware Desktop	Lenovo	IP DHCP	-	-	OEM	-
HAR-015	DXEN-ADM003	Desktop área administración	Administración 03	Operativo	Hardware Desktop	Lenovo	IP DHCP	-	-	OEM	-
HAR-016	DXEN-ADM004	Desktop área administración	Administración 04	Operativo	Hardware Desktop	Lenovo	IP DHCP	-	-	OEM	-
HAR-017	SXEN-IT001	Servidor físico área sistemas	Sistemas 01	Operativo	Hardware Servidor	HP	IP Estática	-	-	OEM	-
HAR-018	SXEN-IT002	Servidor físico área sistemas	Sistemas 01	Operativo	Hardware Servidor	HP	IP Estática	-	-	OEM	-
HAR-019	VXEN-IT001	Servidor virtual Base de datos Área sistemas	Sistemas 01	Operativo	Hardware Servidor Virtual	Hyper-V	IP Estática	-	-	-	-
HAR-020	VXEN-IT002	Servidor virtual Aplicaciones 01 Área sistemas	Sistemas 01	Operativo	Hardware Servidor Virtual	Hyper-V	IP Estática	-	-	-	-
HAR-021	VXEN-IT003	Servidor virtual Aplicaciones 02 Área sistemas	Sistemas 01	Operativo	Hardware Servidor Virtual	Hyper-V	IP Estática	-	-	-	-
HAR-022	VXEN-IT004	Servidor virtual Aplicaciones 03 Área sistemas	Sistemas 01	Operativo	Hardware Servidor Virtual	Hyper-V	IP Estática	-	-	-	-
HAR-023	PXEN-IT001	Impresora área sistemas	Sistemas 01	Operativo	Hardware Impresora	EPSON	IP Estática	-	-	-	-
HAR-024	PXEN-VEN001	Impresora área ventas	Ventas 01	Operativo	Hardware Impresora	EPSON	IP Estática	-	-	-	-
HAR-025	PXEN-ADM001	Impresora área administración	Administración 01	Operativo	Hardware Impresora	EPSON	IP Estática	-	-	-	-
HAR-026	PXEN-ADM002	Impresora matricial facturas área administración	Administración 01	Operativo	Hardware Impresora	EPSON	IP Estática	-	-	-	-

COD	Nombre	Descripción	Propietario	Estado	Tipo	Hardware			Software		
						Fabricante	Dirección IP	S/N	Versión	Licencia	Fecha Adquisición
HAR-027	RXEN-IT001	Router principal	Sistemas 01	Operativo	Hardware Router	Cisco	IP Estática	-	-	-	-
HAR-028	FXEN-IT001	Firewall principal	Sistemas 01	Operativo	Hardware Firewall	Watchguard	IP Estática	-	-	-	-
HAR-029	SWXEN-IT001	Switch área sistemas	Sistemas 01	Operativo	Hardware Switch	Cisco	IP Estática	-	-	-	-
HAR-030	SWXEN-IT002	Switch área ventas	Sistemas 01	Operativo	Hardware Switch	Cisco	IP Estática	-	-	-	-
HAR-031	SWXEN-IT003	Switch área administración	Sistemas 01	Operativo	Hardware Switch	Cisco	IP Estática	-	-	-	-
HAR-032	APXEN-IT001	Access Point área sistemas	Sistemas 01	Operativo	Hardware Access Point	TP-Link	IP Estática	-	-	-	-
HAR-033	APXEN-IT002	Access Point área administración	Sistemas 01	Operativo	Hardware Access Point	TP-Link	IP Estática	-	-	-	-
SOF-001	Windows 10 Pro	Sistema operativo estaciones de trabajo	Sistemas 01	Permitido	Software Sistema Operativo	-	-	-	10 PRO 1809	Licencia por volumen	20-abril-2018
SOF-002	Windows Server 2016	Sistema operativo servidores	Sistemas 01	Permitido	Software Sistema Operativo	-	-	-	Standard	Licencia por Core	20-abril-2018
SOF-003	Office 365	Plataforma de mensajería y colaboración	Sistemas 01	Permitido	Software Mensajería	-	-	-	Enterprise	Licencia por usuario	20-abril-2018
SOF-004	SOHO Desk	Plataforma de tickets	Sistemas 01	Permitido	Software Tickets	-	-	-	Enterprise	Licencia por año	02-febrero-2016
SOF-005	System Xentic	Plataforma de gestión de ventas y administración	Sistemas 01	Permitido	Software Gestión	-	-	-	Standard	Propietario	10-septiembre-2015
SOF-006	StarSoft	Plataforma contable y administrativo	Sistemas 01	Permitido	Software Gestión	-	-	-	Gold Edition	Licencia por año	15-enero-2019
SOF-007	eScan	Plataforma de antivirus	Sistemas 01	Permitido	Software Antivirus	-	-	-	Standard	Licencia por usuario	01-enero-2019

Procedimiento inventario - Xentic

- La herramienta de descubrimiento de dispositivos será ejecutada y monitoreada por el coordinador de sistemas.
- Las siguientes tareas describen un nuevo registro de un activo de hardware en el inventario.
    - El hardware será conectado en la red de la empresa.
    - El personal de sistemas realizará las configuraciones básicas en el dispositivo.
    - La herramienta Lansweeper detectará el nuevo dispositivo recopilando la información de hardware y software.
    - Los datos serán registrados en el inventario de hardware y software, así como también, el estado del activo.
- Para realizar un nuevo registro de un activo de software en el inventario, será aprobado por el coordinador de sistemas y registrado en el inventario por el personal del área. El software será considerado autorizado (lista blanca).
- Las siguientes tareas describen el retiro de un activo de hardware en el inventario.
    - La confirmación del retiro del activo será a través del coordinador de sistemas.
    - El personal de sistemas restablecerá el equipo a modo de fábrica.
    - La eliminación del dispositivo desde la herramienta Lansweeper será realizada por el coordinar de sistemas. Así como también, se eliminará el activo del inventario.
- Las siguientes tareas describen el retiro de un activo de software en el inventario.
    - La confirmación será a través del coordinador de sistemas.
    - El activo de software será eliminado del inventario, por lo tanto, será considerado como prohibido.

Anexo 04: ID-03 Matriz de roles y responsabilidades

A continuación, se presenta la matriz de roles y responsabilidades de la empresa Xentic.

Roles y responsabilidad - Xentic

Roles / Responsabilidades	Oficial de ciberseguridad	Equipo de respuesta ante incidentes	Equipo de recuperación ante desastres	Coordinador de Sistemas	Gerencia general
Gestionar diariamente los controles de ciberseguridad	R	-	-	C, I, A	I
Seguridad física y tecnologías de la organización	R	-	-	C, I, A	I
Garantizar la ciberseguridad en la organización	R	-	-	C, I, A	I
Ejecutar actividades durante o después de un incidente de ciberseguridad	I, A	R	C	I	I
Ejecutar actividades durante o después de un desastre de ciberseguridad	I, A	C	R	I	I

La empresa Xentic decidió seleccionar a uno de los integrantes del área de sistemas como Oficial de ciberseguridad, asimismo, los equipos de respuesta ante incidentes y recuperación ante desastres, los conforman todas las personas del área de sistemas.

Anexo 05: ID-04 Plan de riesgos

A continuación, se presenta el plan de riesgos -basado en MAGERIT- de la empresa Xentic.

Plan de riesgos - Xentic

La descripción de las actividades del plan de riesgos, se presentan a continuación.

a. Valoración de activos

El modelo de valor de la empresa Xentic se presenta en la siguiente matriz.

Activo de información				Dimensiones			
N°	Código	Activo	Descripción	C	D	I	Total
1	HAR-001	LXEN-IT001	Laptop área sistemas	3	3	3	3
2	HAR-002	LXEN-IT002	Laptop área sistemas	2	3	2	2
3	HAR-003	LXEN-IT003	Laptop área sistemas	2	3	2	2
4	HAR-004	LXEN-IT004	Laptop área sistemas	2	3	2	2
5	HAR-005	LXEN-IT005	Laptop área sistemas	2	3	2	2
6	HAR-006	LXEN-IT006	Laptop área sistemas – SPARE	1	1	1	1
7	HAR-007	LXEN-IT007	Laptop área sistemas	2	3	2	2
8	HAR-008	LXEN-IT008	Laptop área sistemas SPARE	1	1	1	1
9	HAR-009	DXEN-VEN001	Desktop área ventas	5	3	4	4
10	HAR-010	DXEN-VEN002	Desktop área ventas	4	3	4	4
11	HAR-011	DXEN-VEN003	Desktop área ventas	4	3	4	4
12	HAR-012	DXEN-VEN004	Desktop área ventas	4	3	4	4
13	HAR-013	DXEN-ADM001	Desktop área administración	5	3	5	4

Activo de información				Dimensiones			
N°	Código	Activo	Descripción	C	D	I	Total
14	HAR-014	DXEN-ADM002	Desktop área administración	5	3	5	4
15	HAR-015	DXEN-ADM003	Desktop área administración	5	3	5	4
16	HAR-016	DXEN-ADM004	Desktop área administración	5	3	5	4
17	HAR-017	SXEN-IT001	Servidor físico área sistemas	3	5	3	4
18	HAR-018	SXEN-IT002	Servidor físico área sistemas	3	5	3	4
19	HAR-019	VXEN-IT001	Servidor virtual Base de datos Área sistemas	4	3	5	4
20	HAR-020	VXEN-IT002	Servidor virtual Aplicaciones 01 Área sistemas	2	3	2	2
21	HAR-021	VXEN-IT003	Servidor virtual Aplicaciones 02 Área sistemas	2	3	2	2
22	HAR-022	VXEN-IT004	Servidor virtual Aplicaciones 03 Área sistemas	2	3	2	2
23	HAR-023	PXEN-IT001	Impresora área sistemas	1	2	1	1
24	HAR-024	PXEN-VEN001	Impresora área ventas	1	2	1	1
25	HAR-025	PXEN-ADM001	Impresora área administración	3	2	3	3
26	HAR-026	PXEN-ADM002	Impresora matricial facturas área administración	3	2	3	3
27	HAR-027	RXEN-IT001	Router principal	4	4	4	4
28	HAR-028	FXEN-IT001	Firewall principal	4	2	4	3
29	HAR-029	SWXEN-IT001	Switch área sistemas	2	3	3	3
30	HAR-030	SWXEN-IT002	Switch área ventas	2	3	3	3

Activo de información				Dimensiones			
N°	Código	Activo	Descripción	C	D	I	Total
31	HAR-031	SWXEN-IT003	Switch área administración	2	3	3	3
32	HAR-032	APXEN-IT001	Access Point área sistemas	2	3	3	3
33	HAR-033	APXEN-IT002	Access Point área administración	2	3	3	3
34	SOF-001	Windows 10 Pro	Sistema operativo estaciones de trabajo	1	3	2	2
35	SOF-002	Windows Server 2016	Sistema operativo servidores	1	3	2	2
36	SOF-003	Office 365	Plataforma de mensajería y colaboración	1	3	2	2
37	SOF-004	SOHO Desk	Plataforma de tickets	2	3	3	3
38	SOF-005	System Xentic	Plataforma de gestión de ventas y administración	4	3	4	4
39	SOF-006	StarSoft	Plataforma contable y administrativo	4	3	4	4
40	SOF-007	eScan	Plataforma de antivirus	4	4	4	4
41	PER-001	Usuarios internos	Personal de la planilla de la empresa	5	5	5	5
42	PER-002	Usuarios externos	Personal que no pertenece a la empresa	5	2	5	4

b. Evaluación del riesgo

El mapa de riesgos de la empresa Xentic se presenta en la siguiente matriz.

Activo de información			Amenaza			Ocurrencia		Evaluación del riesgo	
N°	Código	Descripción	Amenaza	Impacto	Valor	Probabilidad	Valor	Total	Zona de riesgo
1	HAR-001	Laptop área sistemas Coordinador de sistemas	Acceso no autorizado	Menor	2	Raro	2	4	Baja
			Infección de virus (cualquier tipo)	Dañino	3	Posible	3	9	Alta
			Hurto o robo de activo	Dañino	3	Raro	2	6	Moderada
2	HAR-002	Laptop área sistemas Personal de sistemas	Acceso no autorizado	Menor	2	Raro	2	4	Baja
			Infección de virus (cualquier tipo)	Dañino	3	Posible	3	9	Alta
			Hurto o robo de activo	Dañino	3	Posible	3	9	Alta
3	HAR-003	Laptop área sistemas Personal de sistemas	Acceso no autorizado	Menor	2	Raro	2	4	Baja
			Infección de virus (cualquier tipo)	Dañino	3	Posible	3	9	Alta
			Hurto o robo de activo	Dañino	3	Posible	3	9	Alta
4	HAR-004	Laptop área sistemas Personal de sistemas	Acceso no autorizado	Menor	2	Raro	2	4	Baja
			Infección de virus (cualquier tipo)	Dañino	3	Posible	3	9	Alta
			Hurto o robo de activo	Dañino	3	Posible	3	9	Alta
5	HAR-005	Laptop área sistemas Personal de sistemas	Acceso no autorizado	Menor	2	Raro	2	4	Baja
			Infección de virus (cualquier tipo)	Dañino	3	Posible	3	9	Alta
			Hurto o robo de activo	Dañino	3	Posible	3	9	Alta
6	HAR-006	Laptop área sistemas – SPARE	Infección de virus (cualquier tipo)	Dañino	3	Raro	2	6	Moderada
7	HAR-007	Laptop área sistemas Personal de sistemas	Acceso no autorizado	Menor	2	Raro	2	4	Baja
			Infección de virus (cualquier tipo)	Dañino	3	Posible	3	9	Alta
			Hurto o robo de activo	Dañino	3	Posible	3	9	Alta

Activo de información				Amenaza		Ocurrencia		Evaluación del riesgo	
N°	Código	Descripción	Amenaza	Impacto	Valor	Probabilidad	Valor	Total	Zona de riesgo
8	HAR-008	Laptop área sistemas SPARE	Infección de virus (cualquier tipo)	Dañino	3	Raro	2	6	Moderada
9	HAR-009	Desktop área ventas Coordinadora de ventas	Acceso no autorizado	Dañino	3	Raro	2	6	Moderada
			Infección de virus (cualquier tipo)	Dañino	3	Raro	2	6	Moderada
10	HAR-010	Desktop área ventas Personal de ventas	Acceso no autorizado	Dañino	3	Raro	2	6	Moderada
			Infección de virus (cualquier tipo)	Dañino	3	Raro	2	6	Moderada
11	HAR-011	Desktop área ventas Personal de ventas	Acceso no autorizado	Dañino	3	Raro	2	6	Moderada
			Infección de virus (cualquier tipo)	Dañino	3	Raro	2	6	Moderada
12	HAR-012	Desktop área ventas Personal de ventas	Acceso no autorizado	Dañino	3	Raro	2	6	Moderada
			Infección de virus (cualquier tipo)	Dañino	3	Raro	2	6	Moderada
13	HAR-013	Desktop área administración Gerente general	Acceso no autorizado	Severo	4	Raro	2	8	Alta
			Infección de virus (cualquier tipo)	Severo	4	Raro	2	8	Alta
14	HAR-014	Desktop área administración Contador	Acceso no autorizado	Severo	4	Raro	2	8	Alta
			Infección de virus (cualquier tipo)	Severo	4	Raro	2	8	Alta
15	HAR-015	Desktop área administración Recursos humanos	Acceso no autorizado	Severo	4	Raro	2	8	Alta
			Infección de virus (cualquier tipo)	Severo	4	Raro	2	8	Alta
16	HAR-016	Desktop área administración Asistente gerencia	Acceso no autorizado	Severo	4	Raro	2	8	Alta
			Infección de virus (cualquier tipo)	Severo	4	Raro	2	8	Alta
17	HAR-017	Servidor físico área sistemas Host ESXi	Acceso no autorizado	Severo	4	Raro	2	8	Alta
			Modificación de configuraciones básicas	Severo	4	Raro	2	8	Alta
18	HAR-018	Servidor físico área sistemas Host ESXi	Acceso no autorizado	Severo	4	Raro	2	8	Alta
			Modificación de configuraciones básicas	Severo	4	Raro	2	8	Alta

Activo de información			Amenaza			Ocurrencia		Evaluación del riesgo	
N°	Código	Descripción	Amenaza	Impacto	Valor	Probabilidad	Valor	Total	Zona de riesgo
19	HAR-019	Servidor virtual Base de datos Área sistemas	Acceso no autorizado	Dañino	3	Raro	2	6	Moderada
			Alteración de data en las bases de datos	Crítico	5	Raro	2	10	Alta
			Infección de virus (cualquier tipo)	Crítico	5	Raro	2	10	Alta
20	HAR-020	Servidor virtual Aplicaciones 01 Área sistemas Test	Acceso no autorizado	Menor	2	Raro	2	4	Baja
			Alteración de las configuraciones	Menor	2	Raro	2	4	Baja
			Infección de virus (cualquier tipo)	Menor	2	Raro	2	4	Baja
21	HAR-021	Servidor virtual Aplicaciones 02 Área sistemas Test	Acceso no autorizado	Menor	2	Raro	2	4	Baja
			Alteración de las configuraciones	Menor	2	Raro	2	4	Baja
			Infección de virus (cualquier tipo)	Menor	2	Raro	2	4	Baja
22	HAR-022	Servidor virtual Aplicaciones 03 Área sistemas Desarrollo	Acceso no autorizado	Menor	2	Raro	2	4	Baja
			Alteración de las configuraciones	Menor	2	Raro	2	4	Baja
			Infección de virus (cualquier tipo)	Menor	2	Raro	2	4	Baja
23	HAR-023	Impresora área sistemas	Modificación de configuraciones de red	Insignificante	1	Raro	2	2	Baja
24	HAR-024	Impresora área ventas	Modificación de configuraciones de red	Insignificante	1	Raro	2	2	Baja
			Acceso a documentos confidenciales	Dañino	3	Posible	3	9	Alta
25	HAR-025	Impresora área administración	Modificación de configuraciones de red	Insignificante	1	Raro	2	2	Baja
			Acceso a documentos confidenciales	Dañino	3	Posible	3	9	Alta
26	HAR-026	Impresora matricial facturas área administración	Acceso a documentos confidenciales	Severo	4	Posible	3	12	Alta
27	HAR-027	Router principal	Acceso no autorizado	Dañino	3	Raro	2	6	Moderada
			Modificación de configuraciones de red	Dañino	3	Raro	2	6	Moderada

Activo de información				Amenaza		Ocurrencia		Evaluación del riesgo	
N°	Código	Descripción	Amenaza	Impacto	Valor	Probabilidad	Valor	Total	Zona de riesgo
28	HAR-028	Firewall principal	Acceso no autorizado	Dañino	3	Raro	2	6	Moderada
			Modificación de configuraciones de red	Dañino	3	Raro	2	6	Moderada
29	HAR-029	Switch área sistemas	Modificación de configuraciones de red	Menor	2	Raro	2	4	Baja
30	HAR-030	Switch área ventas	Modificación de configuraciones de red	Menor	2	Raro	2	4	Baja
31	HAR-031	Switch área administración	Modificación de configuraciones de red	Menor	2	Raro	2	4	Baja
32	HAR-032	Access Point área sistemas	Modificación de configuraciones de red	Menor	2	Raro	2	4	Baja
33	HAR-033	Access Point área administración	Modificación de configuraciones de red	Menor	2	Raro	2	4	Baja
34	SOF-001	Sistema operativo estaciones de trabajo	-	-	-	-	-	-	-
35	SOF-002	Sistema operativo servidores	-	-	-	-	-	-	-
36	SOF-003	Plataforma de mensajería y colaboración	Suplantación de identidad del dominio	Dañino	3	Raro	2	6	Moderada
37	SOF-004	Plataforma de tickets	Alteración de tickets clientes	Severo	4	Raro	2	8	Alta
38	SOF-005	Plataforma de gestión de ventas y administración	Modificación de información	Severo	4	Raro	2	8	Alta
39	SOF-006	Plataforma contable y administrativo	Modificación de información	Crítico	5	Raro	2	10	Alta
40	SOF-007	Plataforma de antivirus	Bases de firmas desactualizada	Crítico	5	Posible	3	15	Alta
41	PER-001	Usuarios internos	Ataque cibernético con o sin intención	Crítico	5	Probable	4	20	Extrema
42	PER-002	Usuarios externos	Acceso sin autorización a la información o sistemas de datos	Severo	4	Raro	2	8	Alta

c. Tratamiento del riesgo

El plan de tratamiento del riesgo elaborado por la empresa Xentic se presenta en la siguiente matriz.

Activo de información					Tratamiento del riesgo	
N°	**Código**	**Activo**	**Amenaza**	**Zona de riesgo**	**Salvaguarda**	**Observación**
1	HAR-001	Laptop área sistemas Coordinador de sistemas	Acceso no autorizado	**Baja**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	**Alta**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
			Hurto o robo de activo	**Moderada**	Solicitar al área administrativa una movilidad particular para el traslado hacia las oficinas de los clientes	El coordinador de sistemas en ocasiones realiza reuniones de preventa llevando el activo en sus pertenencias
2	HAR-002	Laptop área sistemas Personal de sistemas	Acceso no autorizado	**Baja**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	**Alta**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
			Hurto o robo de activo	**Alta**	Solicitar al área administrativa una movilidad particular para el traslado hacia las oficinas de los clientes	El personal de sistemas realiza visitas proactivas e implementa los proyectos en las instalaciones del cliente llevando el activo en sus pertenencias
3	HAR-003	Laptop área sistemas Personal de sistemas	Acceso no autorizado	**Baja**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	**Alta**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
			Hurto o robo de activo	**Alta**	Solicitar al área administrativa una movilidad particular para el traslado hacia las oficinas de los clientes	El personal de sistemas realiza visitas proactivas e implementa los proyectos en las instalaciones del cliente llevando el activo en sus pertenencias
4	HAR-004	Laptop área sistemas Personal de sistemas	Acceso no autorizado	**Baja**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	**Alta**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
			Hurto o robo de activo	**Alta**	Solicitar al área administrativa una movilidad particular para el traslado hacia las oficinas de los clientes	El personal de sistemas realiza visitas proactivas e implementa los proyectos en las instalaciones del cliente llevando el activo en sus pertenencias

Activo de información					Tratamiento del riesgo	
N°	Código	Activo	Amenaza	Zona de riesgo	Salvaguarda	Observación
5	HAR-005	Laptop área sistemas Personal de sistemas	Acceso no autorizado	Baja	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	Alta	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
			Hurto o robo de activo	Alta	Solicitar al área administrativa una movilidad particular para el traslado hacia las oficinas de los clientes	El personal de sistemas realiza visitas proactivas e implementa los proyectos en las instalaciones del cliente llevando el activo en sus pertenencias
6	HAR-006	Laptop área sistemas – SPARE	Infección de virus (cualquier tipo)	Moderada	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
7	HAR-007	Laptop área sistemas Personal de sistemas	Acceso no autorizado	Baja	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	Alta	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
			Hurto o robo de activo	Alta	Solicitar al área administrativa una movilidad particular para el traslado hacia las oficinas de los clientes	El personal de sistemas realiza visitas proactivas e implementa los proyectos en las instalaciones del cliente llevando el activo en sus pertenencias
8	HAR-008	Laptop área sistemas SPARE	Infección de virus (cualquier tipo)	Moderada	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
9	HAR-009	Desktop área ventas Coordinadora de ventas	Acceso no autorizado	Moderada	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	Moderada	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
10	HAR-010	Desktop área ventas Personal de ventas	Acceso no autorizado	Moderada	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	Moderada	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
11	HAR-011	Desktop área ventas Personal de ventas	Acceso no autorizado	Moderada	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	Moderada	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada

Activo de información					Tratamiento del riesgo	
N°	**Código**	**Activo**	**Amenaza**	**Zona de riesgo**	**Salvaguarda**	**Observación**
12	HAR-012	Desktop área ventas Personal de ventas	Acceso no autorizado	**Moderada**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	**Moderada**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
13	HAR-013	Desktop área administración Gerente general	Acceso no autorizado	**Alta**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	**Alta**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
14	HAR-014	Desktop área administración Contador	Acceso no autorizado	**Alta**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	**Alta**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
15	HAR-015	Desktop área administración Recursos humanos	Acceso no autorizado	**Alta**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	**Alta**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
16	HAR-016	Desktop área administración Asistente gerencia	Acceso no autorizado	**Alta**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Infección de virus (cualquier tipo)	**Alta**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
17	HAR-017	Servidor físico área sistemas Host ESXi	Acceso no autorizado	**Alta**	Modificar las credenciales predefinidas del dispositivo	Las credenciales de los usuarios no contemplan directivas de complejidad
			Modificación de configuraciones básicas	**Alta**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
18	HAR-018	Servidor físico área sistemas Host ESXi	Acceso no autorizado	**Alta**	Modificar las credenciales predefinidas del dispositivo	Las credenciales de los usuarios no contemplan directivas de complejidad
			Modificación de configuraciones básicas	**Alta**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
19	HAR-019	Servidor virtual Base de datos Área sistemas	Acceso no autorizado	**Moderada**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad

Activo de información					Tratamiento del riesgo	
N°	**Código**	**Activo**	**Amenaza**	**Zona de riesgo**	**Salvaguarda**	**Observación**
			Alteración de data en las bases de datos	**Alta**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
			Infección de virus (cualquier tipo)	**Alta**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
20	HAR-020	Servidor virtual Aplicaciones 01 Área sistemas Test	Acceso no autorizado	**Baja**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Alteración de las configuraciones	**Baja**	Ejecutar una copia de seguridad del estado del sistema operativo	No se encontró copias de respaldo
			Infección de virus (cualquier tipo)	**Baja**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
21	HAR-021	Servidor virtual Aplicaciones 02 Área sistemas Test	Acceso no autorizado	**Baja**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Alteración de las configuraciones	**Baja**	Ejecutar una copia de seguridad del estado del sistema operativo	No se encontró copias de respaldo
			Infección de virus (cualquier tipo)	**Baja**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
22	HAR-022	Servidor virtual Aplicaciones 03 Área sistemas Desarrollo	Acceso no autorizado	**Baja**	Gestionar las credenciales de los usuarios a través de un software	Las credenciales de los usuarios no contemplan directivas de complejidad
			Alteración de las configuraciones	**Baja**	Ejecutar una copia de seguridad del estado del sistema operativo	No se encontró copias de respaldo
			Infección de virus (cualquier tipo)	**Baja**	Instalar y mantener actualizada la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
23	HAR-023	Impresora área sistemas	Modificación de configuraciones de red	**Baja**	Habilitar un usuario (rol administrador) que permita la aprobación de cualquier cambio en el dispositivo	Cualquier usuario puede cambiar los parámetros de red
24	HAR-024	Impresora área ventas	Modificación de configuraciones de red	**Baja**	Habilitar un usuario (rol administrador) que permita la aprobación de cualquier cambio en el dispositivo	Cualquier usuario puede cambiar los parámetros de red
			Acceso a documentos confidenciales	**Alta**	Configurar únicamente los usuarios de ventas en la impresora	Cualquier usuario puede enviar documentos a la impresora
25	HAR-025	Impresora área administración	Modificación de configuraciones de red	**Baja**	Habilitar un usuario (rol administrador) que permita la aprobación de cualquier cambio en el dispositivo	Cualquier usuario puede cambiar los parámetros de red

Activo de información					Tratamiento del riesgo	
N°	**Código**	**Activo**	**Amenaza**	**Zona de riesgo**	**Salvaguarda**	**Observación**
			Acceso a documentos confidenciales	**Alta**	Configurar únicamente los usuarios de administración en la impresora	Cualquier usuario puede enviar documentos a la impresora
26	HAR-026	Impresora matricial facturas área administración	Acceso a documentos confidenciales	**Alta**	Configurar únicamente los usuarios de administración en la impresora	Cualquier usuario puede enviar documentos a la impresora
27	HAR-027	Router principal	Acceso no autorizado	**Moderada**	Modificar las credenciales predefinidas del dispositivo	Las credenciales de los usuarios no contemplan directivas de complejidad
			Modificación de configuraciones de red	**Moderada**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
28	HAR-028	Firewall principal	Acceso no autorizado	**Moderada**	Modificar las credenciales predefinidas del dispositivo	Las credenciales de los usuarios no contemplan directivas de complejidad
			Modificación de configuraciones de red	**Moderada**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
29	HAR-029	Switch área sistemas	Modificación de configuraciones de red	**Baja**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
30	HAR-030	Switch área ventas	Modificación de configuraciones de red	**Baja**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
31	HAR-031	Switch área administración	Modificación de configuraciones de red	**Baja**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
32	HAR-032	Access Point área sistemas	Modificación de configuraciones de red	**Baja**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
33	HAR-033	Access Point área administración	Modificación de configuraciones de red	**Baja**	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
34	SOF-001	Sistema operativo estaciones de trabajo	-	-	-	-
35	SOF-002	Sistema operativo servidores	-	-	-	-
36	SOF-003	Plataforma de mensajería y colaboración	Suplantación de identidad del dominio	**Moderada**	Implementar registros DNS SPF y DMARC	El proveedor DNS no contempla estos registros

Activo de información					Tratamiento del riesgo	
N°	Código	Activo	Amenaza	Zona de riesgo	Salvaguarda	Observación
37	SOF-004	Plataforma de tickets	Alteración de tickets clientes	Alta	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
38	SOF-005	Plataforma de gestión de ventas y administración	Modificación de información	Alta	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
39	SOF-006	Plataforma contable y administrativo	Modificación de información	Alta	Ejecutar una copia de seguridad de las configuraciones del dispositivo	No se encontró copias de respaldo de las configuraciones
40	SOF-007	Plataforma de antivirus	Bases de firmas desactualizada	Alta	Actualizar la base de firmas del antivirus	La base de datos de antivirus se encontraba desactualizada
41	PER-001	Usuarios internos	Ataque cibernético con o sin intención	Extrema	Elaborar y ejecutar un plan de capacitaciones en función de la ciberseguridad	El personal deberá ser capacitado en horas laborales y remoto para reforzar los temas involucrados en el plan
42	PER-002	Usuarios externos	Acceso sin autorización a la información o sistemas de datos	Alta	Deshabilitar cualquier usuario y acceso a los sistemas que no correspondan al personal de la empresa	Se identificará todos los usuarios en los equipos y sistemas de la empresa

Anexo 06: PR-01 Gestión de cuentas de usuario y contraseñas

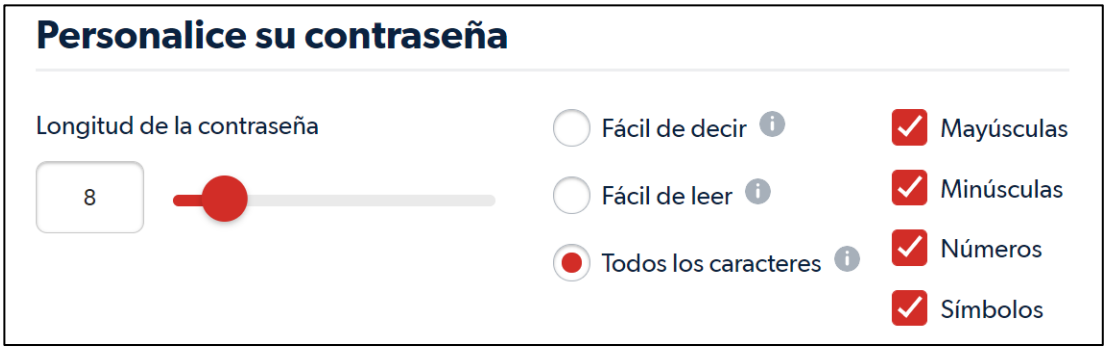
A continuación, se presenta el desarrollo del control de la empresa Xentic. El inventario de cuentas de usuario y contraseñas, así como también, el procedimiento del registro del documento.

N°	Usuario	Dominio	Tipo de cuenta	Servicio asociado	Fecha de creación	Fecha de actualización
1	Administrador	Sin dominio	Local	Computadoras & Laptops	2018	Oct-2020
2	Administrador	Xentic.local	Dominio	Controlador de Dominio	2011	Abr-2015
3	Root	Sin dominio	Local	Router principal	2011	Feb-2011
4	Root	Sin dominio	Local	Switches	2011	Feb-2011
5	Root	Sin dominio	Local	Switch Sistemas	2018	Set-2018
6	adminAP	Sin dominio	Local	Access Points	2017	Abr-2017
7	Admin	Sin dominio	Local	Servidores Físicos	2018	Abr-2018
8	Sa	Sin dominio	Local	Cuenta SA bases de datos	2016	Dic-2016
9	Xentic_admin	Sin dominio	Local	Cuenta admin Sistema XENTIC	2015	Set-2015
10	Admin_starsoft	Sin dominio	Local	Cuenta admin Sistema StarSoft	2019	Ene-2019
11	Escan_admin	Sin dominio	Local	Cuenta admin Sistema antivirus eScan	2017	Jul-2017
12	sohoadmin	Sin dominio	Local	Cuenta admin SOHO Desk	2016	Feb-2016

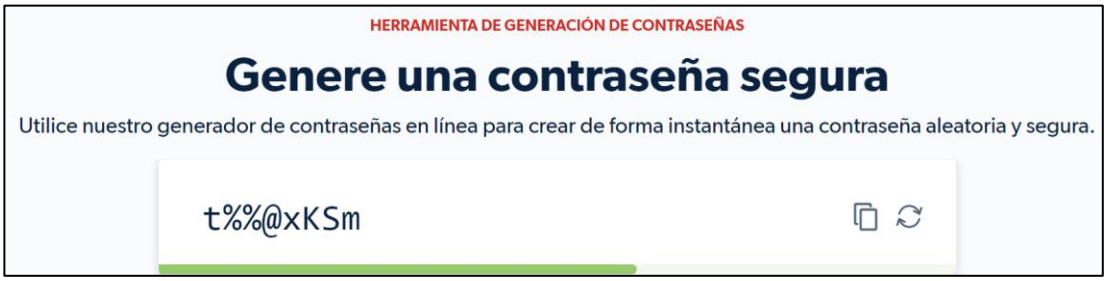
Procedimiento inventario - Xentic

- El coordinador de sistemas será el responsable del uso, modificación y almacenamiento del inventario de cuentas y contraseñas.
- La contraseña deberá ser modificada cada 6 meses.

- La contraseña deberá tener mínimo 8 caracteres y contemplar mayúsculas, minúsculas, números y caracteres especiales.
- Se utilizará el programa en línea “LastPass” para generar las contraseñas colocando los parámetros respectivos.
- A continuación, se muestra las capturas del uso del programa.
    - Ingresar al url: https://www.lastpass.com/es/password-generator
    - Identificar los parámetros



- Generar contraseña



- Modificar el valor de la contraseña en el inventario
- Guardar los cambios en el inventario.

Anexo 07: PR-02 Gestión de la red empresarial

A continuación, se presenta el desarrollo del control de la empresa Xentic. Las configuraciones básicas de la red se detallan en los siguientes puntos.

- El coordinador de sistemas segmentó la red en redes virtuales (VLAN) en los equipos Switch de la empresa.
    - VLAN por Defecto (DEFAULT_VLAN)
    - VLAN Administrativa (VLAN_DATAGAF)
    - VLAN Voz (VLAN_VOIP)
    - VLAN CCTV (VLAN_CCTV)
    - VLAN Operativa (VLAN_DATAGOP)
    - VLAN Gestión (VLAN_MGMT)
- La VLAN de Voz y CCTV están en modo de prueba para su futura implementación.
- La VLAN Administrativa pertenece a las áreas de ventas y administración. La VLAN Operativa es del área de Sistemas (incluye equipos de redes y servidores).
- Los puertos no utilizados se encuentran deshabilitados siguiendo las recomendaciones.
- Por motivos de seguridad, la lista de direcciones no fue enviada, sin embargo, se muestra tres capturas de la configuración del equipo Switch.
    - Configuración de VLAN

```
Status and Counters - VLAN Information

 Maximum VLANs to support : 256
 Primary VLAN : VLAN_DATAGAF
 Management VLAN : VLAN_MGMT

 VLAN ID Name                            | Status     Voice Jumbo
 ------- ------------------------------- + ---------- ----- -----
 1       DEFAULT_VLAN                    | Port-based No    No
 2       VLAN_DATAGAF                    | Port-based No    No
 3       VLAN_VOIP                       | Port-based Yes   No
 4       VLAN_CCTV                       | Port-based No    No
 5       VLAN_DATAGOP                    | Port-based No    No
 99      VLAN_MGMT                       | Port-based No    No
```

    - Captura del archivo de configuración del Switch

```
vlan 99
   name "VLAN_MGMT"
   untagged 13,24
   ip address [redacted] 255.255.255.0
   qos priority 1
   exit
primary-vlan 2
management-vlan 99
no tftp server
no dhcp config-file-update
password [redacted]
password [redacted]
```

- Configuración de puertos del Switch

```
Status and Counters - Port Status

                | Intrusion                          MDI  Flow Bcast
 Port  Type     | Alert     Enabled Status Mode      Mode Ctrl Limit
 ----- -------- + --------- ------- ------ --------- ---- ---- -----
 1     100/1000T | No        Yes     Up     1000FDx   MDI  off  0
 2     100/1000T | No        Yes     Up     1000FDx   MDI  off  0
 3     100/1000T | No        Yes     Up     1000FDx   MDIX off  0
 4     100/1000T | No        Yes     Up     1000FDx   MDI  off  0
 5     100/1000T | No        Yes     Down   1000FDx   MDI  off  0
 6     100/1000T | No        Yes     Up     1000FDx   MDI  off  0
 7     100/1000T | No        Yes     Down   1000FDx   MDI  off  0
 8     100/1000T | No        Yes     Down   1000FDx   MDI  off  0
 9     100/1000T | No        Yes     Down   1000FDx   MDIX off  0
 10    100/1000T | No        Yes     Down   1000FDx   MDIX off  0
 11    100/1000T | No        Yes     Down   1000FDx   MDIX off  0
 12    100/1000T | No        Yes     Down   1000FDx   MDIX off  0
 13    100/1000T | No        Yes     Up     1000FDx   MDIX off  0
 14    100/1000T | No        Yes     Down   1000FDx   MDI  off  0
 15    100/1000T | No        Yes     Down   1000FDx   MDIX off  0
 16    100/1000T | No        Yes     Down   1000FDx   MDI  off  0
 17    100/1000T | No        Yes     Down   1000FDx   MDIX off  0
 18    100/1000T | No        Yes     Down   1000FDx   MDI  off  0
 19    100/1000T | No        Yes     Down   1000FDx   MDIX off  0
 20    100/1000T | No        Yes     Down   1000FDx   MDI  off  0
 21    100/1000T | No        Yes     Down   1000FDx   MDI  off  0
 22    100/1000T | No        Yes     Down   1000FDx   MDI  off  0
 23    100/1000T | No        Yes     Up     1000FDx   MDI  off  0
 24    100/1000T | No        Yes     Up     1000FDx   MDI  off  0
 25              | No        No      Down              off  0
 26              | No        No      Down              off  0
 27              | No        No      Down              off  0
 28              | No        No      Down              off  0
```

Anexo 08: PR-03 Plan de concientización y capacitación

A continuación, se presenta el desarrollo del control de la empresa Xentic. Se desarrolló un cronograma de capacitaciones en función de la seguridad cibernética para los meses noviembre y diciembre del 2020.

El detalle de las reuniones se encuentra en los siguientes puntos:

- Ciberseguridad Inducción
    - Fecha: 08-Nov-2020
    - Hora: 20:00
    - Duración: 30 minutos
    - Lugar: Sesión remota Microsoft Teams
- Impacto de la ciberseguridad
    - Fecha: 27-Nov-2020
    - Hora: 20:00
    - Duración: 30 minutos
    - Lugar: Sesión remota Microsoft Teams
- Vectores de los ataques cibernéticos
    - Fecha: 18-Dic-2020
    - Hora: 20:00
    - Duración: 30 minutos
    - Lugar: Sesión remota Microsoft Teams

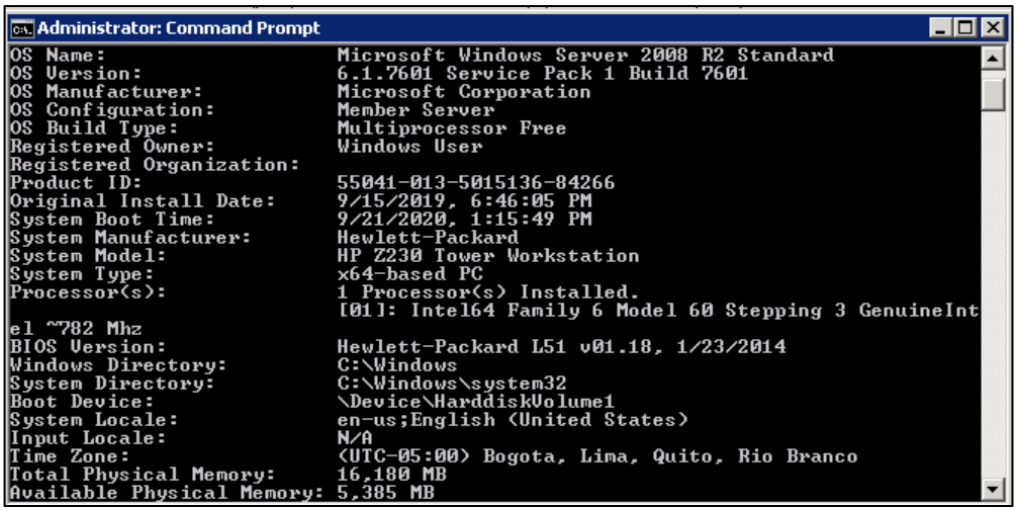
Anexo 09: PR-04 Gestión de copias de seguridad

A continuación, se presenta el desarrollo del control de la empresa Xentic. Se elaboró un procedimiento e implementación de la herramienta Veeam Backup para el desarrollo del control.

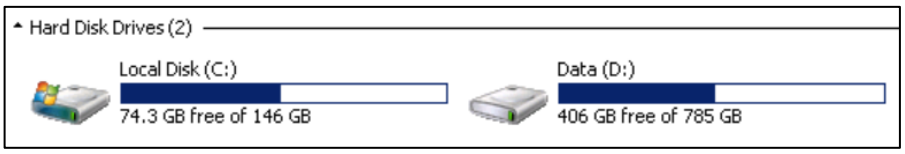
- El coordinador de sistemas es el responsable de la administración del sistema Veeam Backup.
- Veeam Backup (edición Community) permite ejecutar copias de seguridad de hasta 10 servidores virtuales.
- Existe un servidor de Backup que tiene instalado Veeam Backup y puede ejecutar tareas de copias de seguridad y restauración de datos.
- Los servidores con respaldo de información son los siguientes:
    - N4W2008R2EN22
    - N4LNX70ENFTP
    - N4CL70X64EN07
    - N4CL70X64EN05
    - N4W7ENCLIENT01
    - N4CL70X64EN01
    - N4CL70X64EN20
    - N4CL70X64EN18
    - N4W2008R2EN19V3
- El detalle de la tarea de copias de seguridad es la siguiente:
    - Programación: Todos los días a las 10:00 pm
    - Almacenamiento: Disco Local D:
    - Puntos de restauración: 4.
    - Tipo de Backup: Full
- Como medida de contingencia, la segunda tarea de Backup es realizar una copia de la unidad local D a un disco externo.
- Esta segunda tarea se realiza todos los días a las 08:00 am.

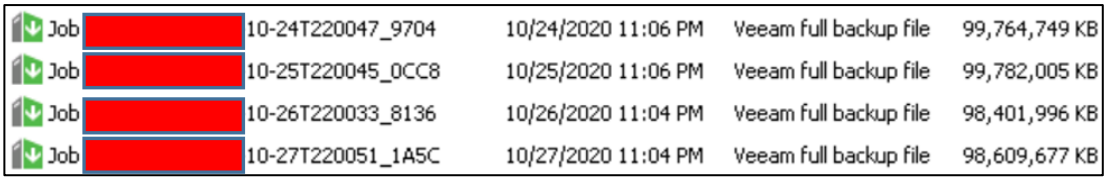
Las siguientes capturas muestran la configuración del Backup en la empresa Xentic.

- Datos del servidor

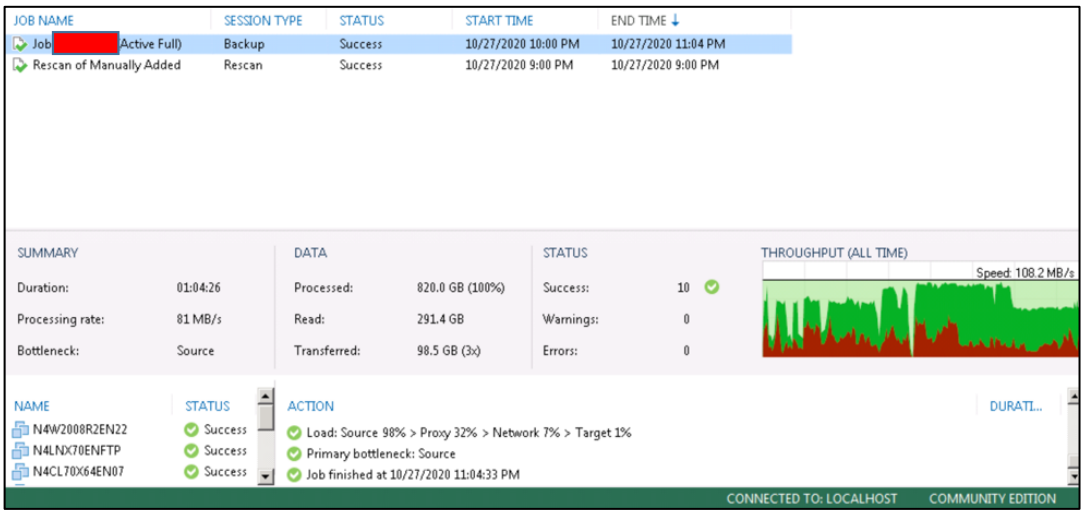


- Almacenamiento copias de seguridad





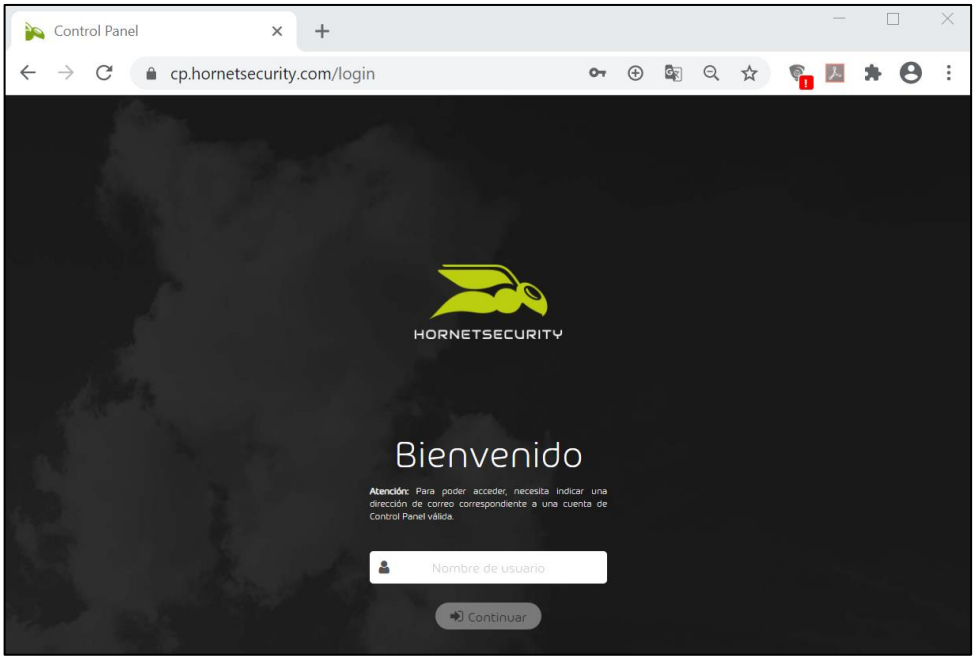
- Tarea de Backup



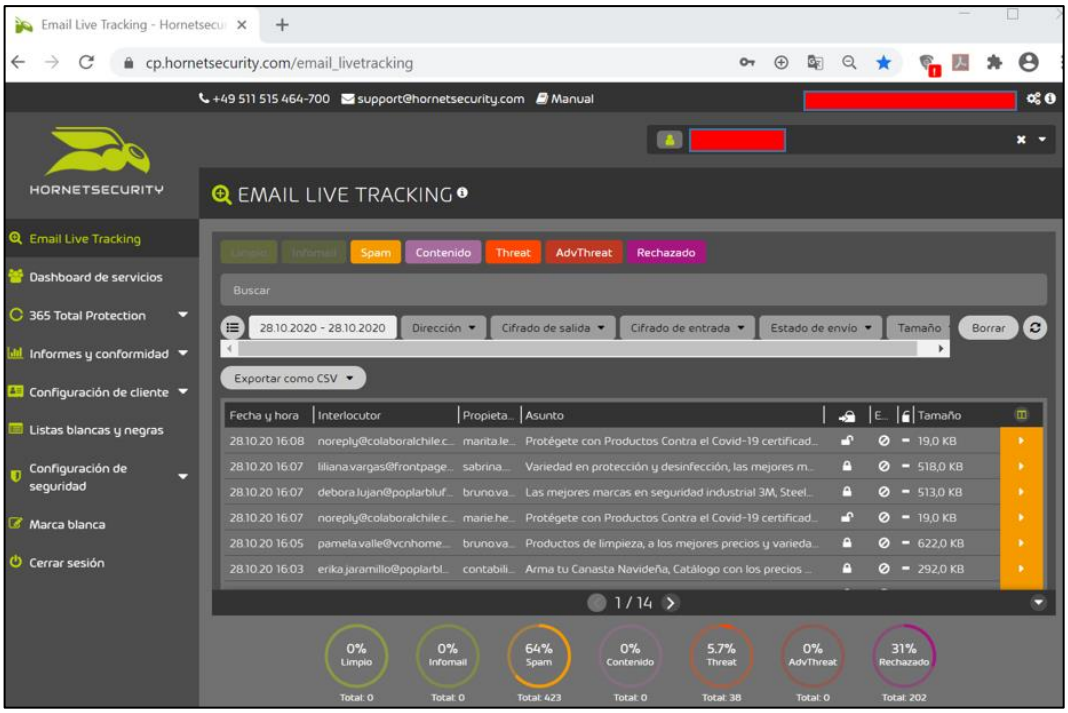
Anexo 10: PR-05 Plan de respuesta ante incidentes y plan de recuperación ante desastres

A continuación, se presenta el desarrollo del control de la empresa Xentic. Se establecieron dos planes ante incidentes y uno para desastres con el objetivo de evidenciar las tareas a ejecutar cuando ocurran estos eventos.

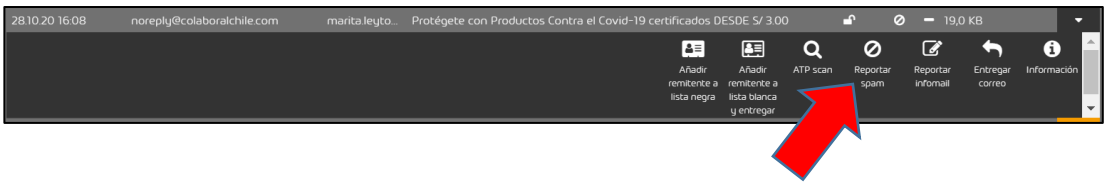
- **Plan de respuesta ante incidentes 01**
    - Evento: Correos SPAM.
    - Objetivo: Reducir el riesgo de suspensión del servicio de correo electrónico por SPAM.
    - Servicio afectado: Correo electrónico.
    - Responsables: Equipo de respuesta ante incidentes.
        i. Coordinador de sistemas
        ii. Auxiliar de sistemas 1
        iii. Auxiliar de sistemas 2
    - Descripción:
        i. El usuario afectado deberá reportar el correo SPAM al área de sistemas mediante un email o llamada telefónica.
        ii. El personal de sistemas deberá ingresar al sistema de antispam (Hornet Security) con las credenciales asignadas.



        iii. En la página principal, filtrar los correos SPAM.



iv. Identificar el correo y seleccionar la opción ***"reportar spam"***

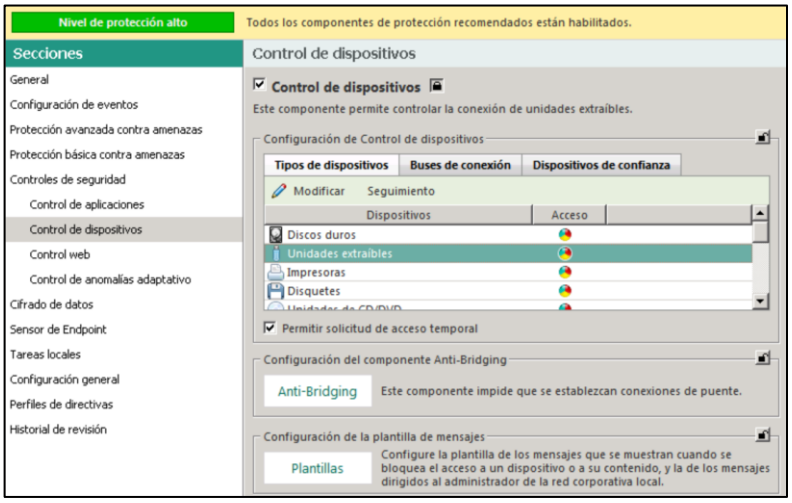


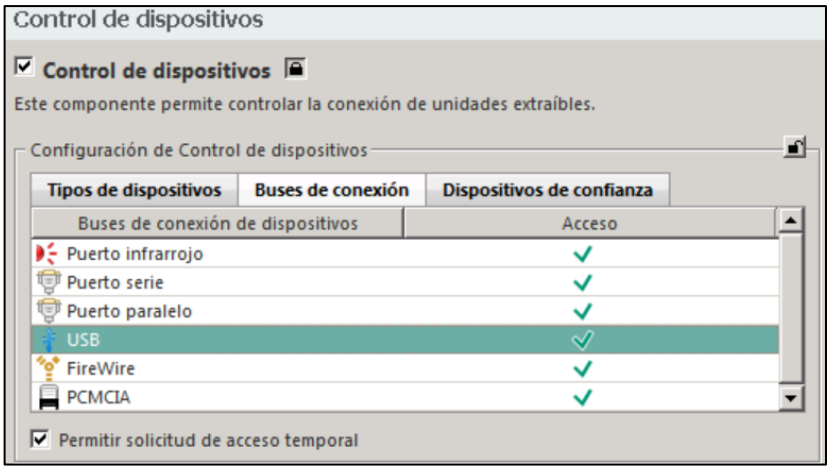
v. Como opción secundaria, se puede seleccionar ***"añadir remitente a lista negra"***.

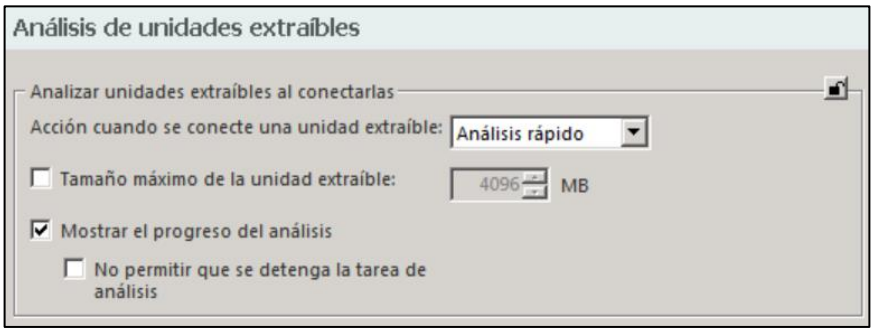
- **Plan de respuesta ante incidentes 02**
  - Evento: Acceso puertos USB infectados.

- Objetivo: Reducir el riesgo de infección de virus informáticos a través de dispositivos USB.
- Servicio afectado: Computadoras y laptops.
- Responsables: Equipo de respuesta ante incidentes.
    i. Coordinador de sistemas
    ii. Auxiliar de sistemas 1
    iii. Auxiliar de sistemas 2
- Descripción:
    i. Ingresar a la consola de antivirus con las credenciales respectivas.
    ii. En el módulo ***"dispositivos administrados"*** seleccionar el grupo ***"IN-USB"***.

    iii. Este grupo tiene como directiva el permitir el acceso de unidades extraíbles, así como también, un escaneo de la unidad insertada en el puerto USB.







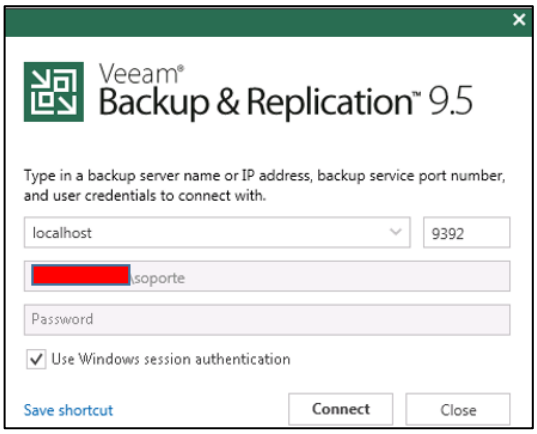
iv. Todas las computadoras y laptops que no pertenecen al grupo “IN USB” no tendrán acceso a dispositivos USB.
v. Se habilitará el puerto a demanda, es decir, cuando el usuario lo requiere y con fines laborales.

- **Plan de respuesta ante desastres 01**
    - Evento: Corrupción de servidor virtual.
    - Objetivo: Recuperar el servidor virtual después de un Ransomware ataque cibernético.
    - Servicio afectado: Directorio Activo, Bases de datos, Otros.
    - Responsables: Equipo de respuesta ante desastres.
        i. Coordinador de sistemas
        ii. Auxiliar de sistemas 1
        iii. Auxiliar de sistemas 2
    - Descripción:
        i. Existen varios tipos de ataques cibernéticos que pueden robar la información de la empresa. Por ejemplo, el ataque de tipo Ransomware restringe el acceso a los archivos y carpetas de un sistema operativo y solicita un pago para recuperar la información.
        ii. Como se observa en la imagen, el atacante muestra en pantalla un mensaje informando que los archivos han sido encriptados (manera de ocultar los datos mediante una llave para que otros no puedan interpretarlos).

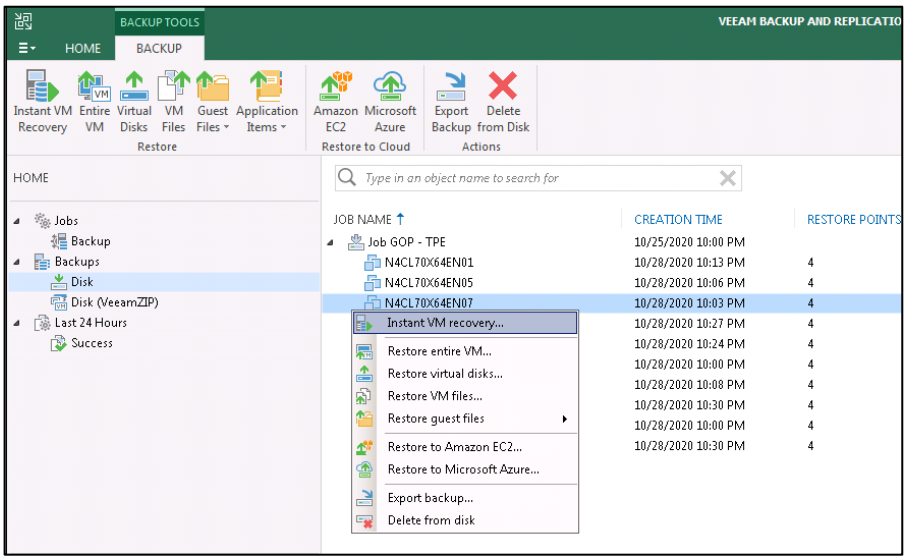
        iii. Asimismo, solicita el pago para recuperar los datos robados.

iv. Como medida de recuperación del servidor virtual ante este evento de ciberseguridad, es necesario utilizar la herramienta Veeam Backup en su modalidad de restauración de datos.

v. Ingresar al servidor de Backup y abrir la aplicación Veeam Backup.



vi. Ingresar al módulo ***"Home-Backups"***. Seleccionar la máquina virtual a recuperar y hacer click en la opción ***"Instant VM recovery"***.



vii. Finalizado el proceso, ingresar al servidor virtual y comprobar la recuperación total del servicio afectado.

Anexo 11: DE-01 Gestión de vulnerabilidades

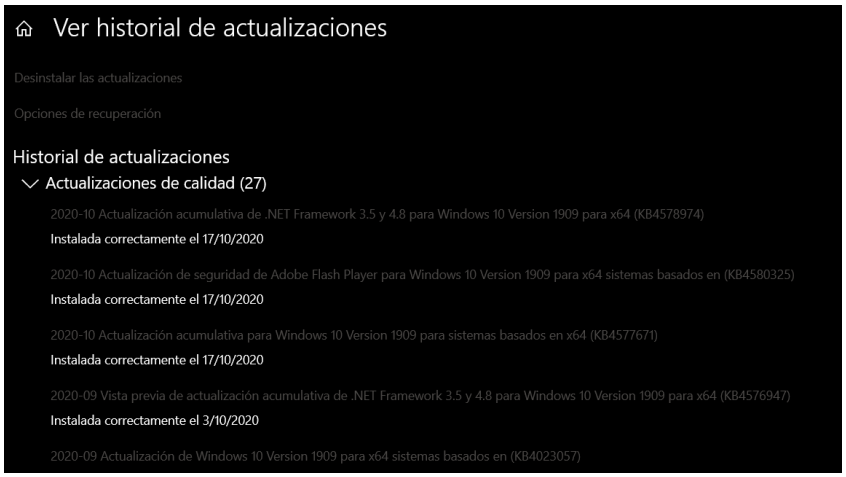
A continuación, se presenta el desarrollo del control de la empresa Xentic. Se elaboró el siguiente procedimiento que describe las tareas básicas de la gestión de vulnerabilidades en la empresa.

- El coordinador de sistemas es el responsable de la búsqueda de vulnerabilidades de los equipos tecnológicos de la empresa.
- Por el momento no se utilizará una herramienta de vulnerabilidades. Sin embargo, se realizarán las siguientes tareas con el fin de lograr el objetivo del control.
    - Con respecto a las computadoras y laptops, se instalarán progresivamente las actualizaciones de Windows Update. El servicio será ejecutado todos los días para garantizar la seguridad de los equipos.
    - Con respecto a los servidores, se instalarán progresivamente las actualizaciones de Windows Update. Se buscarán los últimos parches en la página del fabricante y aplicará de acuerdo con su criticidad.
    - Con respecto a los switches, se buscará las vulnerabilidades de la versión del equipo en la página del fabricante. Luego, se instalarán de acuerdo con su criticidad.
    - Con respecto a los demás equipos, se buscarán vulnerabilidades en las páginas oficiales de los fabricantes y se instalará de acuerdo con su criticidad.

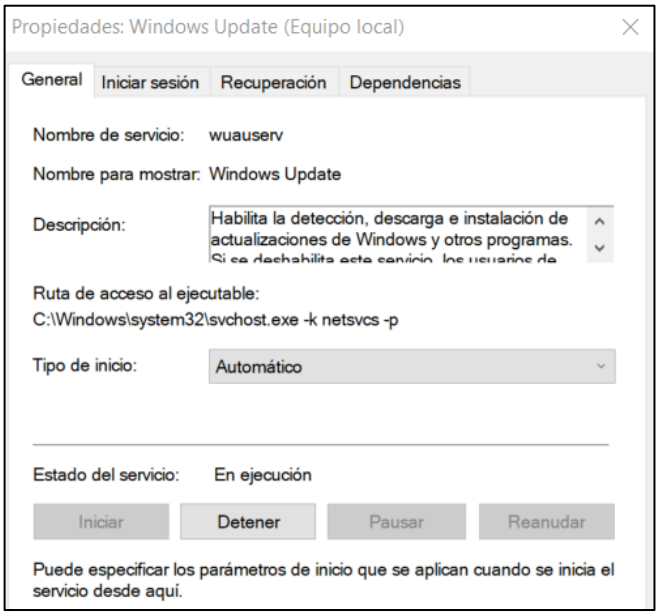
A continuación, se presenta unas capturas de la instalación de los parches de seguridad de Windows Update en computadoras y servidores de la empresa.

- Computadora Windows 10 – Coordinador de sistemas
    - Búsqueda de actualizaciones

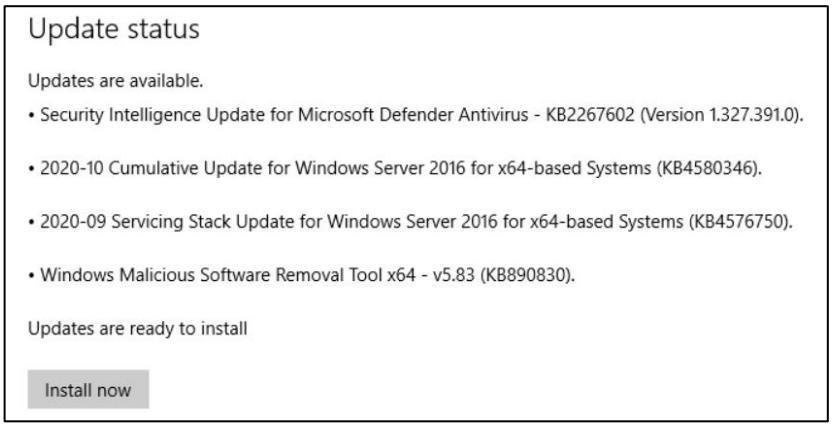
    - Actualizaciones instaladas



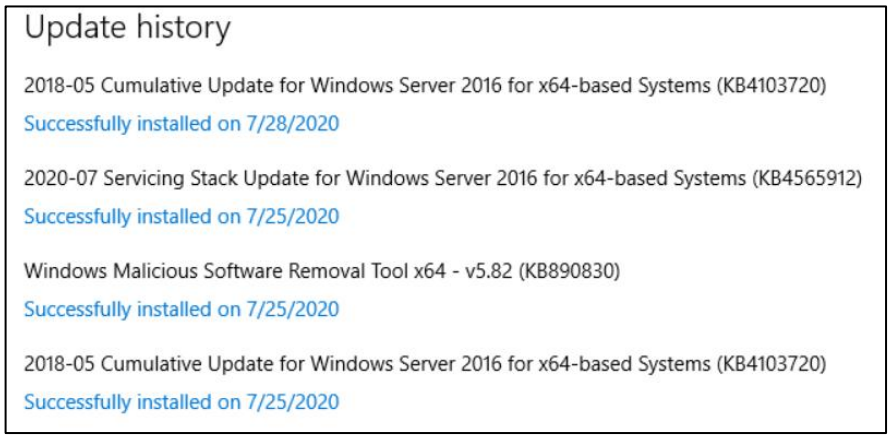
    - Propiedades del servicio Windows Update



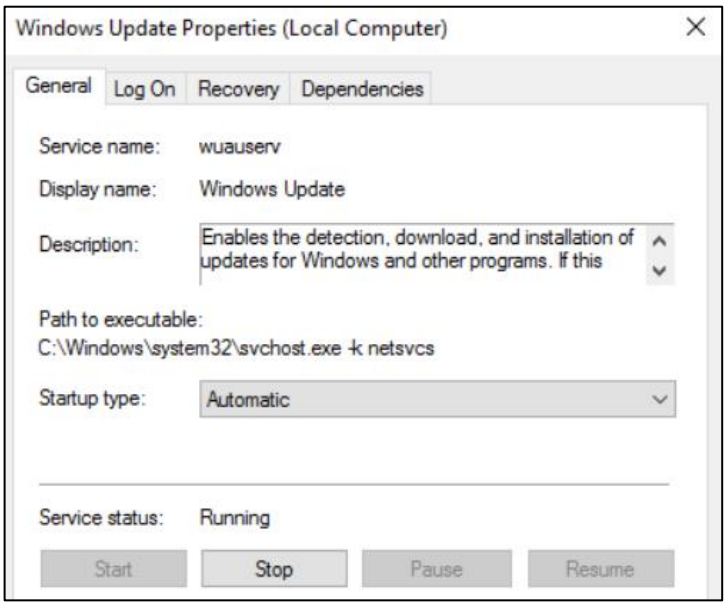
- Servidor Windows Server 2016 – Controlador de Dominio
    - Búsqueda de actualizaciones



    - Actualizaciones instaladas



    - Propiedades del servicio Windows Update



Anexo 12: Auditoría interna

A continuación, se presenta el resultado de la auditoría interna que se realizó en la empresa Xentic

Entrevistado: John Rentería / Cargo: Coordinador de sistemas

Control	Consultas	Respuestas	Observaciones	Recomendaciones	Cumplimiento (%)
ID-01 Política de ciberseguridad	¿La empresa ha desarrollado un documento de política de ciberseguridad que identifique objetivos y compromisos aprobada por la gerencia? ¿La política de ciberseguridad es difundida y comunicada a los colaboradores de la empresa?	*"Se elaboró y aprobó la Política de Ciberseguridad. Asimismo, el documento fue enviado a los colaboradores de la empresa."*	El documento siguió las pautas descritas en la plantilla elaborada en la tesis	Se recomienda una constante revisión de los lineamientos y compromisos del documento.	100%
ID-02 Inventario de hardware y software	¿Existe un inventario de los activos de hardware y software de la empresa? ¿Existe un procedimiento que controle los cambios del inventario? ¿Existe una lista blanca de software y aplicaciones?	*"La instalación del programa Lansweeper permitió la identificación de los activos de hardware y software. El procedimiento es claro y preciso, así como también la identificación de aplicaciones autorizadas en la empresa"*	El inventario se encuentra actualizado y contiene las columnas base de la plantilla elaborada en la tesis	Se recomienda mantener en constaste actualización el inventario respectivo	100%
ID-03 Matriz de roles y responsabilidades	¿Se tiene identificado los roles y responsabilidades de ciberseguridad en la empresa? ¿Existe un documento donde estén registrados los roles y responsabilidades?	*"El oficial de ciberseguridad y los equipos está conformados por el personal del área de sistemas. El documento de la matriz está elaborado con los roles y responsabilidades respectivas"*	La matriz de la empresa se basa en la plantilla elaborada en la tesis	Se recomienda analizar nuevos roles y responsabilidades en la matriz respectiva	100%
ID-04 Plan de riesgos	¿Existe un plan de riesgos? ¿El plan realiza la valoración, evaluación y tratamiento de riesgos?	*"La valoración de activos, evaluación y tratamiento de riesgos fueron elaborados de acuerdo con los lineamientos sugeridos en el framework propuesto"*	Las tablas y matrices usadas en el plan de riesgos de la empresa se basan en las plantillas propuestos en la tesis	Se recomienda identificar nuevas amenazas para los activos de hardware y software de manera regular	100%

Control	Consultas	Respuestas	Observaciones	Recomendaciones	Cumplimiento (%)
PR-01 Gestión de cuentas de usuarios y contraseñas	¿Existe un inventario de cuentas y contraseñas de usuarios? ¿Existen restricciones en la elaboración de contraseñas?	"En estos momentos, existe un archivo Excel con las cuentas de usuarios de los sistemas. Las credenciales contemplan los requerimientos del control"	Existen algunos usuarios que se desconoce la contraseña respectiva.	Se recomienda eliminar estos usuarios, caso contrario, intentar cambiar o recuperar las contraseñas respectivas	100%
PR-02 Gestión de la red empresarial	¿Se realiza una segmentación lógica y física en la red empresarial? ¿Existen redes virtuales VLAN para dividir los segmentos de red? ¿Todos los puertos de red de los switches se encuentran habilitados?	"La red de la empresa se encuentra segmentada por Switches y redes virtuales (VLANs), así mismo, los puertos no utilizados del Switch se encuentran deshabilitados siguiendo las recomendaciones del control"	-	-	100%
PR-03 Plan de concientización y capacitación	¿Existen planes de concientización y capacitación de ciberseguridad para los colaboradores? ¿Cuál es la frecuencia de las capacitaciones? ¿Cuándo fue la última capacitación?	"Se elaboró un cronograma para el mes de noviembre y diciembre que permitirá capacitar al personal. La frecuencia es aprox. cada 20 días y la última charla fue el pasado 7 de Nov"	Se deberá planificar el cronograma del año 2021	Se recomienda dictar las capacitaciones en horario de oficinas y remotamente	100%
PR-04 Gestión de copias de seguridad	¿Se realiza copias de seguridad (backup) de los archivos de los equipos, sistemas, aplicaciones o servicios? ¿Utilizan una herramienta automatizada o labor manual para realizar la copia de seguridad? ¿Cuál es la frecuencia de backup? ¿Existen duplicados de las copias de seguridad como medida preventiva?	"Se implementó la herramienta Veeam Backup (versión gratuita) y nos permite ejecutar copias de seguridad y restauración de archivos de las máquinas virtuales de nuestra empresa. Las tareas de Backup son aplicadas todos los días y existe una copia adicional en un disco externo"	-	Se recomienda ejecutar pruebas de recuperación de archivos cada mes para validar la integridad de los datos	100%

Control	Consultas	Respuestas	Observaciones	Recomendaciones	Cumplimiento (%)
PR-05 Plan de respuesta ante incidentes y plan de recuperación ante desastres	¿Existe un plan de respuesta ante incidentes de ciberseguridad? ¿Existe un plan de recuperación ante desastres de ciberseguridad? ¿El plan de recuperación ante desastres se encuentra disponible y cuenta con una copia de seguridad?	"Se elaboraron algunos planes de incidentes y desastres ante un evento de ciberseguridad. Se tiene como objetivos, desarrollar más planes para preparar a los equipos y estar capacitados ante cualquier situación. Los planes están disponibles para cada integrante del área de sistemas"	Existen una cantidad mínima de planes ante incidentes y desastres de seguridad cibernética	Se recomienda aumentar el número de procedimientos y planes de ciberseguridad	100%
DE-01 Gestión de vulnerabilidades	¿Se realiza una búsqueda de vulnerabilidades de los activos? ¿Cuál es la frecuencia del proceso de búsqueda de vulnerabilidades? ¿Existe un procedimiento que describa las actividades de la búsqueda vulnerabilidades?	"Siguiendo las pautas del control, se realiza la búsqueda de vulnerabilidades de los equipos informáticos de la empresa de forma manual. La frecuencia es cada dos semanas y el procedimiento menciona los pasos puntales de la búsqueda e instalación de parches de seguridad"	El proceso de búsqueda es manual y podría causar errores humanos	Se recomienda utilizar una herramienta Open Source para que realice esta actividad con el objetivo de automatizar el control	100%