UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor:
Taco Paspuel Juan Pablo
Tutor:
Mg. Renato Mauricio Toasa Guachi PhD. Maryory Urdaneta Herrera

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Toasa Guachi Renato Mauricio con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.

Elaborado por: Taco Paspuel Juan Pablo, de C.I: 1722702527, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

Firma

APROBACIÓN DEL TUTOR

Yo, Urdaneta Herrera Maryory con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.

Elaborado por: Taco Paspuel Juan Pablo, de C.I: 1722702527, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

_____

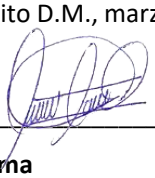
Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Juan Pablo Taco Paspuel con C.I: 1722702527, autor del proyecto de titulación denominado: Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2024



Firma

Tabla de contenidos

APROBACIÓN DEL TUTOR ii
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE iv
INFORMACIÓN GENERAL 1
Contextualización del tema 1
Problema de investigación 1
Objetivo general 2
Objetivos específicos 2
Vinculación con la sociedad y beneficiarios directos: 3
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO 4
1.1. Contextualización general del estado del arte 4
1.2. Proceso investigativo metodológico 5
1.2.1.- Enfoque de la investigación 5
1.2.1.- Tipos de investigación 6
1.2.4.- Población y muestra de estudio 6
1.2.4.- Recopilación de información 7
1.3. Análisis de resultados 7
CAPÍTULO II: PROPUESTA 18
2.1 Fundamentos teóricos aplicados 18
2.1.1. ISO 27002: 2013 18
2.1.2. Vulnerabilidades 19
2.2 Descripción de la propuesta 21
2.3 Propuesta de un plan de mitigación de riesgos 24
2.4 Validación de la propuesta 24
2.5 Matriz de articulación de la propuesta 25
2.6 Análisis de resultados. Presentación y discusión. 28
2.6.1. Estudio de la organización 28
2.6.2. Identificación y valoración de activos 30
2.6.3. Identificación de amenazas y estimación de riesgos 33
2.6.4. Identificación de vulnerabilidades 36
2.6.5. Cumplimiento de controles de la ISO 27002 40
CONCLUSIONES 44
RECOMENDACIONES 45

BIBLIOGRAFÍA 46

Índice de tablas

Tabla 1. Matriz de articulación 25

Tabla 2: Servidores 30

Tabla 3: Comunicaciones 30

Tabla 4: Computadoras 31

Tabla 5: Aplicaciones 33

Tabla 6: Servidores 33

Tabla 7: Computadoras 33

Tabla 8: Identificación de amenazas 34

Tabla 9: Valoración de riesgos 35

Tabla 10: Valoración de riesgos 35

Tabla 11: Criterios para evaluación de controles de la ISO 27002 40

Tabla 12: Evaluación de controles de la ISO 27002 41

Índice de figuras

Figura 1: Conocimiento del término seguridad informática. 8
Figura 2 Medidas implementadas en temas de seguridad informática 9
Figura 3 Medidas o herramientas para temas de seguridad informática en el último año 10
Figura 4 Incidente de seguridad informática 11
Figura 5 Incidentes de seguridad 12
Figura 6 Temas como Phisihing o Vishing en el último año 13
Figura 7 Capacitaciones recibidas referente a temas de seguridad informática 14
Figura 8 Política interna de seguridad informática. 15
Figura 9 Estructura de la propuesta 21
Figura 10 Organigrama Gerencia General. 29
Figura 11 Organigrama TI. 29
Figura 12 Vulnerabilidades servidor SAP-ERP. 36
Figura 13 Vulnerabilidades servidores 37
Figura 14 Vulnerabilidades pc contabilidad 39
Figura 15 Vulnerabilidades pc soporte de negocios 39
Figura 16 Resultado de evaluación de controles de la ISO 27002 42

INFORMACIÓN GENERAL

En la siguiente sección se propone un plan de mitigación de riesgos aplicado a la empresa DIBEAL Cía. Ltda., que permita la evaluación de los controles de ciberseguridad.

Contextualización del tema

Las TIC, cada vez más se han vuelto parte del diario vivir para mucha gente, con el transcurso de los años han evolucionado trayendo consigo beneficios en su aplicación en diversas áreas como; educación, entretenimiento, negocios, etc. (Moya, 2016).

En los últimos años se ha evidencia el aumento del uso de ordenadores y de redes de comunicación por parte de las diferentes organizaciones de nuestro medio, para la ejecución de sus actividades económicas, mediante la transferencia procesamiento y almacenamiento de información, que ha convertido a esta en uno de los activos más valiosos de las empresas, dicha información está siendo objeto de constante amenaza por parte de los ciberdelincuentes y puede estar vulnerable si no se toma las medidas de protección adecuadas (Cayambe, 2023).

El trabajo de investigación tiene como objetivo proponer un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL., para lo cual se identificará la situación actual de los controles de ciberseguridad existentes y evaluarlos, con la finalidad de identificar las vulnerabilidades existentes y proponer un plan de seguridad que ayude a mitigarlas. (Rouse, 2020)

Problema de investigación

DIBEAL CIA. LTDA., fue fundada en 1989, como importadora y distribuidora de productos de consumo. Durante tres décadas ha representado de manera exclusiva en Ecuador, marcas premium mundialmente reconocidas (DIBEAL, 2023).

Al ser una empresa del sector retail su giro de negocio hace muy necesario el uso de dispositivos electrónicos como ordenadores (desktop, laptops, servidores, etc.) y redes de comunicación para la utilización de un Enterprise Resource Planning (ERP) que con sus diferentes módulos (inventario, facturación electrónica, producción, etc.) permite gestionar varias áreas de la empresa.

Los dispositivos están interconectados en una red de área local con acceso a los diferentes servicios del ERP, de ahí que se identifican riesgos que puedan ser ocasionados por mal uso de los dispositivos asignados a los usuarios. Por otro lado, la red al no estar dividida por VLANS abre una brecha que puede ser explotada por un atacante, adicional se requiere evaluar el funcionamiento de la protección de seguridad perimetral que actualmente cuenta con un firewall.

Muchas empresas del sector retail como es el caso de DIBEAL, en la actualidad no cuentan con un método o herramienta que permita el análisis y evaluación de estado de los controles de TI, lo que abre brechas que están constantemente expuestas ante amenazas que hoy por hoy con el avance de la tecnología son más sofisticadas, este antecedente es el punto de partida para adaptar estrategias que ayudarán a gestionar los riesgos de seguridad informática y surge la siguiente interrogante.

¿Cómo un plan de mitigación de riesgos de análisis y medición de los controles de TI, podrá hacer seguro el ambiente tecnológico de la empresa DIBEAL?

Objetivo general

Proponer un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.

Objetivos específicos

- Realizar una investigación teórica referente a la evaluación de riesgos mediante la ISO 27002.
- Identificar vulnerabilidades y amenazas de seguridad informática a los que está expuesta la empresa mediante un diagnóstico de procesos críticos en la empresa DIBEAL.
- Proponer un plan de mitigación de riesgos basándose en la evaluación realizada con la Norma ISO 27002 y la identificación de vulnerabilidades.
- Valorar a través de criterio de especialistas el plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL

Vinculación con la sociedad y beneficiarios directos:

El presente trabajo está enmarcado en cubrir el objetivo de desarrollo sostenible (ODS) 9: "Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación" establecido por la Organización de Naciones Unidas (ONU).

Debido a que hoy en día para las organizaciones es vital la utilización de herramientas tecnológicas para la generación, procesamiento y almacenamiento de información utilizada para llevar a cabo sus diferentes operaciones sean estas administrativas, comerciales, financieras, etc. La mayoría de dicha información es de uso confidencial y debe estar resguardada con sus debidas seguridades.

Para el caso de DIBEAL, la información que maneja en su gran mayoría es de uso confidencial, es por esto que se hace muy necesario el desarrollo de un plan de mitigación de riesgos que permita evaluar los controles de seguridad vigentes.

Para llevar a cabo la evaluación de los controles se tomará como referencia la ISO 27002, mediante la gestión de vulnerabilidades, el resultado de este análisis nos ayudará a identificar posibles brechas de seguridad y tomar correcciones oportunas en los controles vigentes que requieran mejoras.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

A continuación, una breve descripción del proyecto propuesto.

1.1. Contextualización general del estado del arte

Debido al aumento de los delitos que se cometen por medio de un dispositivo informático, existe mayor demanda de profesionales que puedan analizar cualquier tipo de brecha que da lugar a que las instituciones o empresas se vean afectadas por riesgos de cibercrimen, el presente trabajo de titulación hace referencia a los mecanismos que se pueden aplicar para mitigar estos riesgos específicamente en la infraestructura y los riesgos a los que están expuestas varias instituciones del país, analizar estas brechas de seguridad y las herramientas para mitigarlas están enfocadas a la investigación (Cayambe, 2023).

La mitigación de riesgos en redes inalámbricas y las metodologías que se pueden implementar como medida a los riesgos que envuelven estas tecnologías ya que según un estudio realizado por Narváez (2023) menciona que las redes inalámbricas son uno de los eslabones más débiles por el cual se puede sufrir un ataque informático, esta información va de la mano con el actual trabajo de titulación.

Una de las tecnologías que están siendo más notorias en los últimos años es la IoT, que para su conectividad utiliza las redes LPWAN, la cual también comprende un punto de vulnerabilidad, la actual tesis ayuda a mitigar las posibles vulnerabilidades y amenazas que se pueden presentar basándose la normativa internacional ISO 27002 a través de la implementación de controles que esta normativa proporciona. (Espinosa, 2023)

Desde una perspectiva más general es importante tener en cuenta que son muy utilizadas las tecnologías de virtualización mediante entornos de hipervisores lo cual genera muchos beneficios en el aspecto económico de las empresas, pero esto también comprende varios riesgos de seguridad por diversos factores como la incorrecta configuración de las mismas, la no aplicación de claves seguras y la no atención de bloqueo de puertos que no son utilizados. (Quiroga, 2023)

Como parte de las herramientas que existen para la detección de posibles vulnerabilidades en los sistemas de una organización se encuentran las plataformas SIEM, que administran los registros generados por los diferentes equipos de seguridad perimetral, ya que recolecta toda la información generada por estos, la normaliza y correlaciona, esto permite

administrar de manera organizada todos los registros generados, este tipo de herramientas ayuda a combatir los ataques maliciosos tanto a hardware y software de manera integral. (Loachamín, 2023)

En la investigación realizada por Moya (2023) se detalla que "el conocimiento de la situación actual de la empresa permitió definir un punto de partida y, el análisis y la selección de los activos de información más importantes para la empresa, facilita la selección e implementación de controles adecuados" (p. 48). De ahí que se tiene como punto de partida el conocer la situación actual de la empresa de estudio para obtener mejores resultados y asi proceder a elaborar un plan de mitigación de riesgos acorde a la empresa de estudio.

El análisis procedente de la investigación realizada por Figueroa (2019) nos indica que "La implementación del plan de mitigación de riesgos permitiría mejorar la gestión de información en el departamento TIC" (p. 84). Esto indica que al implementarse un plan de mitigación de riesgos acorde a las necesidades de la institución se puede reducir errores, tiempo y recurso, para así garantizar una mejor gestión de la información.

1.2. Proceso investigativo metodológico

A continuación, se especifica el proceso que se ha realizado para el desarrollo del plan de seguridad aplicado a la empresa Dibeal Cia. Ltda.

1.2.1.- Enfoque de la investigación

Se considera una investigación con un enfoque cuantitativo ya que se van a obtener resultados en base a los datos recopilados para conocer sobre un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL. Según Hernández y otros (2014) "el enfoque cuantitativo es una forma estructurada de recopilar y analizar datos obtenidos de distintas fuentes, lo que implica el uso de herramientas informáticas, estadísticas, y matemáticas para obtener resultados" (p. 59).

1.2.1.- Tipos de investigación

Investigación Bibliográfica

Se considera una investigación de tipo bibliográfica tal como lo indica Hernández et al. (2014) "la investigación bibliográfica o revisión de la literatura proporcionan datos de primera mano" (p.27), de ahí se procedió con el análisis de varios documentos como libros, tesis, y artículos publicados, los cuales aportan con información técnica y conceptual para el desarrollo del proyecto titulado "Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL".

Investigación Descriptiva

También se considera una investigación de tipo descriptiva ya que "comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o procesos de los fenómenos" (Tamayo y Tamayo, 2003, p. 45). Mediante la investigación descriptiva se pretende hacer un análisis de los datos que se recopilarán con la aplicación de herramientas investigativas, que ayudarán a tener una comprensión clara sobre un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.

Investigación de Campo

Se buscará también obtener información de las áreas y personal relacionado a los procesos de mitigación de riesgos mediante la investigación de campo. Debido a que este tipo de investigación permite conocer directamente en la empresa DIBEAL como se encuentra la seguridad informática mediante la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades.

1.2.4.- Población y muestra de estudio

Se toma como población de estudio a la empresa DIBEAL la cual está conformada por 110 empleados distribuidos en las diferentes áreas. Como muestra en la presente investigación se considera un muestreo por conveniencia, aplicado a las jefaturas de las diferentes áreas de la empresa ya que ellos conocen y tienen acceso a la información considerada como confidencial.

1.2.4.- Recopilación de información

Para la recopilación de la información relacionada con la seguridad informática basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL se utiliza una revisión documental que permita conocer si se cumplen cada uno de los controles que indica la ISO 27002.

Como técnica de investigación se toma como referencia la encuesta la misma que permite conocer el estado actual de la empresa, así como el problema de investigación. Se realiza una encuesta a las jefaturas de las diferentes áreas de DIBEAL con el objetivo de saber su criterio sobre la situación actual de la empresa en lo que se refiere a seguridad informática, que en total son 15 personas, la información recopilada es de gran ayuda, ya que muestra una visión más amplia de cómo se está gestionando la seguridad informática, y la importancia que se da como organización a este tema. (ver Anexo 1). Finalmente se presentarán los resultados obtenidos.

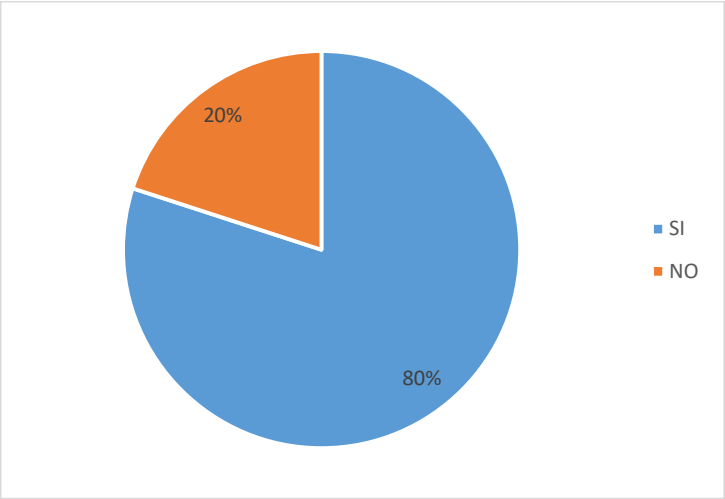
1.3. Análisis de resultados

A continuación, se presentan los resultados obtenidos al aplicar la encuesta a las jefaturas de la empresa DIBEAL con el objetivo de saber su criterio sobre la situación actual de la empresa en lo que se refiere a seguridad informática:

Pregunta 1: ¿Conoce usted acerca del término seguridad informática?

Figura 1:

Conocimiento del término seguridad informática.



Nota. La figura muestra el nivel de conocimiento del término seguridad informática. (Elaboración propia)

Análisis e interpretación de resultados:

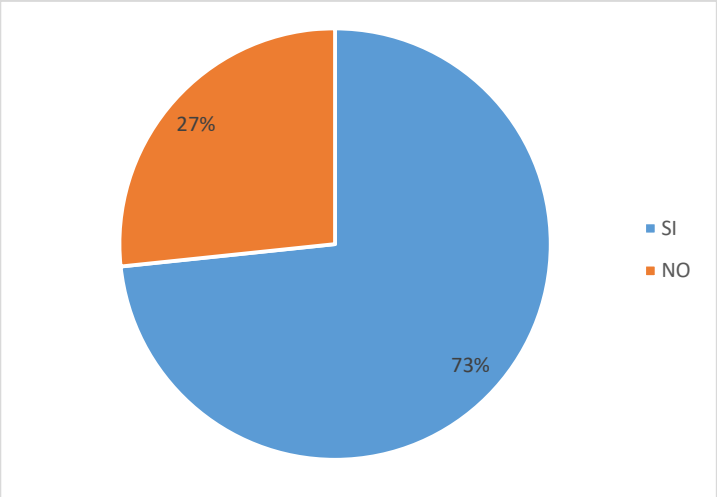
Al indagar sobre el nivel de conocimiento del término seguridad informática se obtuvo que 12 personas que corresponde al 80% de los encuestados SI conocen el término Seguridad informática, mientras que 3 personas que corresponden al 20% No lo conoce, como se muestra en la figura1.

La mayor parte de personas encuestadas afirman conocer sobre la seguridad informática sin embargo a pesar de ello cometen errores que ponen en riesgo la seguridad de la empresa ya que almacenan y comparten una gran cantidad de información personal en línea. De ahí que conocer sobre seguridad informática aplicada de una manera adecuada ayuda a proteger datos sensibles de la empresa contra el robo y la utilización indebida.

Pregunta 2: ¿Conoce si en la empresa se han tomado medidas o implementado herramientas para temas de seguridad informática en el último año?

Figura 2

Medidas implementadas en temas de seguridad informática



Nota. La figura muestra el nivel de conocimiento sobre las medidas implementadas en temas de seguridad informática. (Elaboración propia)

Análisis e interpretación de resultados:

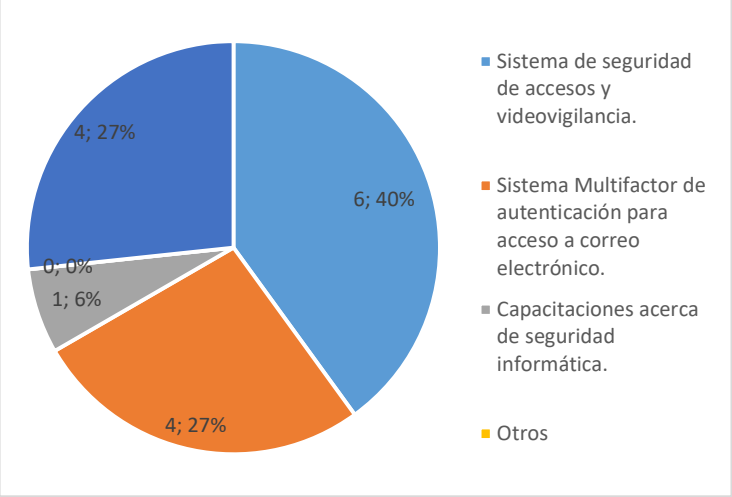
La figura muestra que 11 personas que corresponde al 73% de los encuestados SI conocen que se han implementado medidas en temas de Seguridad informática mientras que 4 personas que corresponden al 27% No, como se muestra en la figura 2.

En la empresa se han implementado temas de seguridad informática y esto ha sido del completo conocimiento de los empleados sin embargo no han implementado estas en sus labores cotidianas y esto se refleja en la manera en la que almacenan y comparten la información personal en línea. De ahí que conocer sobre seguridad informática ayuda a proteger datos sensibles como números de tarjetas de crédito, contraseñas, información médica y otros datos personales contra el robo y la utilización indebida.

Pregunta 3: ¿Conoce si en la empresa se han tomado medidas o implementado herramientas para temas de seguridad informática en el último año?

Figura 3

Medidas o herramientas para temas de seguridad informática en el último año.



Nota. La figura muestra Medidas o herramientas para temas de seguridad informática en el último año. (Elaboración propia)

Análisis e interpretación de resultados:

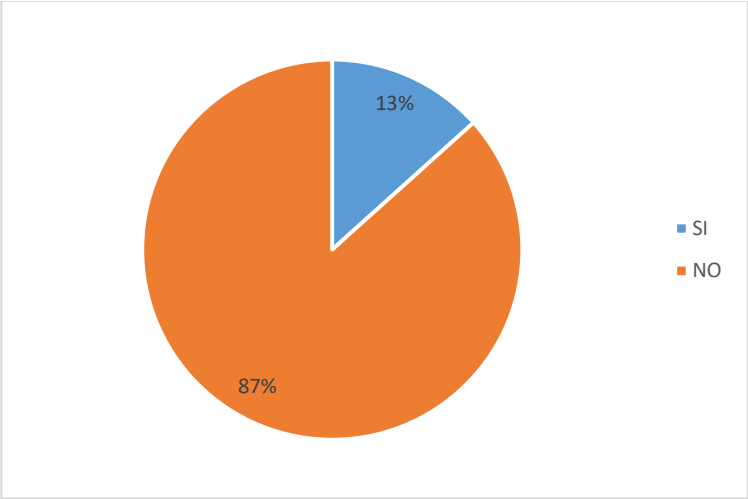
Según los datos obtenidos se muestra que 6 personas que corresponde al 40% de los encuestados conocen de la implementación de un sistema de seguridad de acceso y video vigilancia, 4 personas que corresponde al 27% conocen de la implementación de un sistema Multifactor de autenticación para acceso a cuenta de correo electrónico, 1 personas que corresponde al 6% de los encuestados ha recibido capacitaciones acerca de seguridad informática, mientras que 4 personas que corresponden al 27% No aplicaron con su comentario para esta pregunta por qué en la pregunta anterior su respuesta fue negativa, como se muestra en la figura 3.

Tan solo el 6% de empleados han recibido capacitaciones sobre seguridad informática como medida de seguridad, de ahí que se refleja el uso de contraseñas débiles y varias falencias en el manejo de información considerada como crítica para la empresa.

Pregunta 4: ¿Se ha suscitado algún tipo de incidente de seguridad informática en la empresa en el último año?

Figura 4

Incidente de seguridad informática



Nota. La figura muestra los incidentes relacionados con seguridad informática. (Elaboración propia)

Análisis e interpretación de resultados:

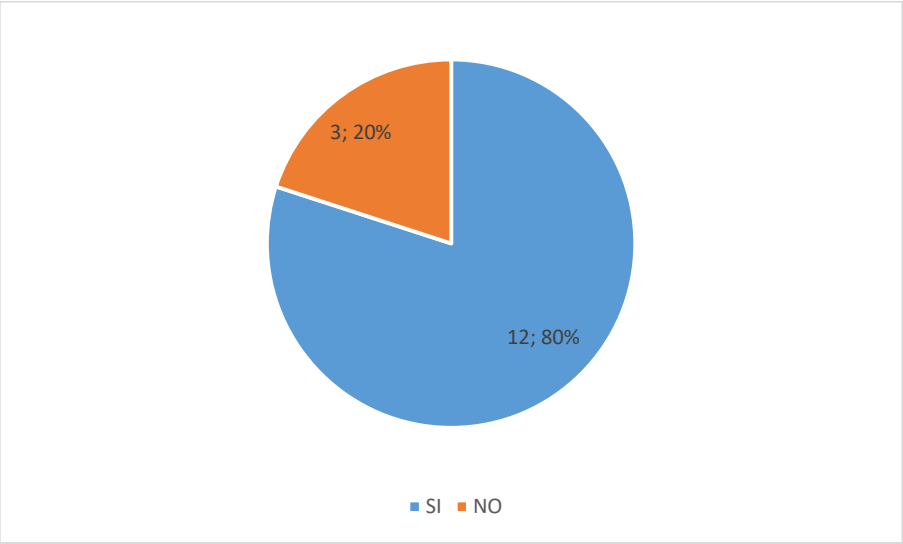
De la encuesta realiza se obtuvo como resultados los datos de la figura 4 en la que se muestra que 2 personas que corresponde al 13% de los encuestados SI conocen de algún tipo de incidente de Seguridad informática ocurrido en la empresa mientras que 13 personas que corresponden al 87% desconocen que se haya suscitado algún evento de seguridad informática en la empresa, como se muestra en la figura 4.

Los datos muestran que más de la mitad de empleados no han experimentado incidentes relacionados con seguridad informática el último año, sin embargo, los pocos incidentes registrados pueden significar un grave riesgo para la empresa ya que se puede comprometer información considerada como crítica para cada uno de los procesos que se realizan en la empresa.

Pregunta 5: ¿Si recibe un mensaje de correo electrónico de dudosa procedencia y contiene links para abrir otras páginas web y usted considera que no es seguro, sabe a qué área debe reportar dicho incidente?

Figura 5

Incidentes de seguridad



Nota. La figura muestra los datos relacionados con incidentes de seguridad informática. (Elaboración propia)

Análisis e interpretación de resultados:

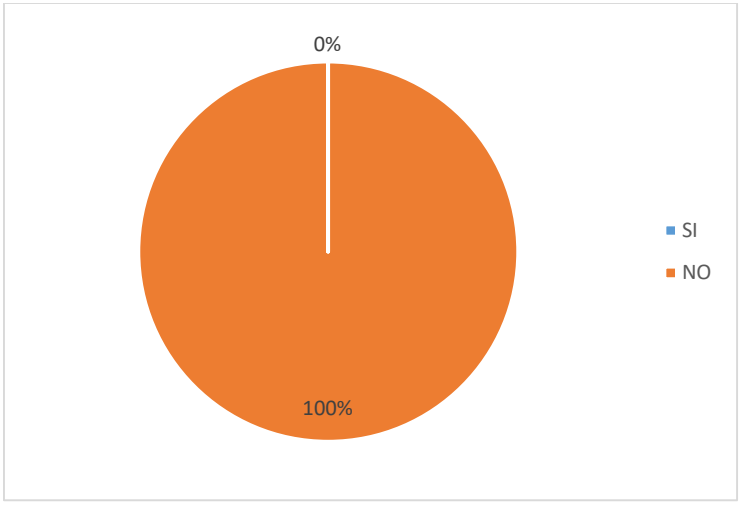
La figura muestra que 12 personas que corresponde al 80% de los encuestados SI conocen a que departamento deben reportar algún evento de correo sospechosos recibidos en la empresa mientras que 3 personas que corresponden al 20% No, como se muestra en la figura 5.

La emisión de correos de dudosa procedencia que contiene links para abrir otras páginas web es cotidiana, de ahí que es importante capacitar a los empleados para que puedan reconocer aquellos correos considerados como no seguros, además es importante que los empleados sepan a quien poderse dirigir para reportar estos incidentes y así evitar que más compañeros puedan ser víctimas de ciberdelincuentes.

Pregunta 6: ¿Ha recibido algún tipo de recomendación o consejos a seguir a través del correo empresarial de temas como Phisihing o Vishing en el último año?

Figura 6

Temas como Phisihing o Vishing en el último año



Nota. La figura muestra algún tipo de recomendación o consejos a seguir a través del correo empresarial de temas como Phisihing o Vishing en el último año. (Elaboración propia)

Análisis e interpretación de resultados:

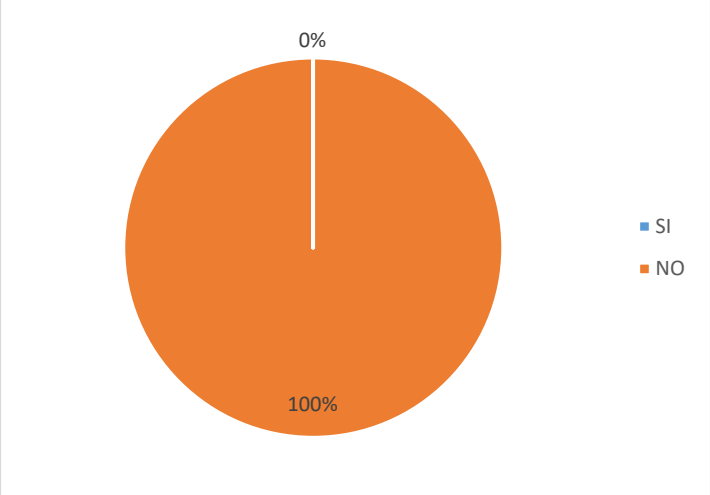
Al indagar sobre si han recibido algún tipo de recomendación o consejos a seguir a través del correo empresarial de temas como Phisihing o Vishing en el último año se muestra que 15 personas que corresponde al 100% de los encuestados NO han recibido ningún tipo de recomendación por medio de correo institucional, como se muestra en la figura 6.

Las personas encuestadas afirman no haber recibido capacitaciones sobre temas como Phisihing o Vishing en el último año, de ahí que resulta importante capacitar a los empleados para que verifiquen siempre la autenticidad del remitente antes de hacer clic en enlaces o proporcionar información. También es importante que sepan reconocer enlaces de correos electrónicos sospechosos.

Pregunta 7: ¿Ha recibido capacitaciones referentes a seguridad de informática en el último año?

Figura 7

Capacitaciones recibidas referente a temas de seguridad informática



Nota. La figura muestra el nivel de conocimiento del término seguridad informática. (Elaboración propia)

Análisis e interpretación de resultados:

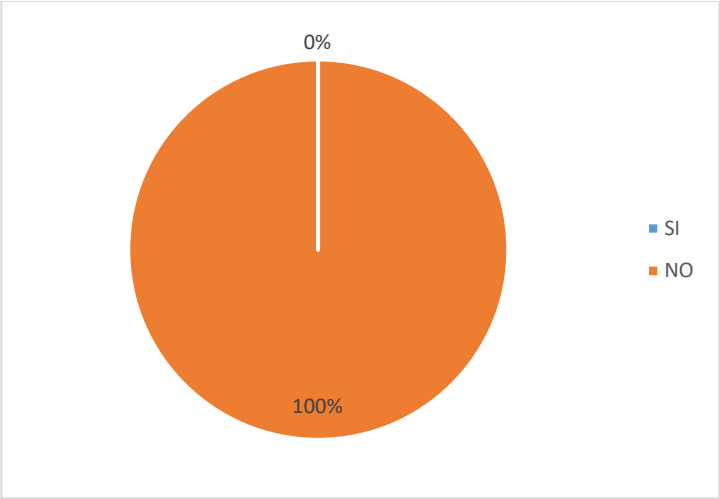
La figura muestra que 15 personas que corresponde al 100% de los encuestados NO han recibido ningún tipo de capacitaciones de temas de seguridad informática por parte de la organización como se muestra en la figura 7.

La mayor parte de personas encuestadas afirman conocer sobre la seguridad informática sin embargo a pesar de ello cometen errores que ponen en riesgo la seguridad de la empresa ya que almacenan y comparten una gran cantidad de información personal en línea. De ahí que conocer sobre seguridad informática aplicada de una manera adecuada ayuda a proteger datos sensibles de la empresa contra el robo y la utilización indebida.

Pregunta 8: ¿Conoce si en la empresa existe alguna política interna sobre seguridad informática?

Figura 8

Política interna de seguridad informática.



Nota. La figura muestra el nivel de conocimiento del término seguridad informática. (Elaboración propia)

Análisis e interpretación de resultados:

La figura muestra que 15 personas que corresponde al 100% de los encuestados su respuesta fue NO, porque no conocen si existe alguna política interna referente a seguridad informática, como se muestra en la figura 8.

En la empresa no existen políticas claras relacionadas con políticas de seguridad informática de ahí que resulta de gran importancia tener políticas claras que ayuden a proteger los activos críticos de la organización, como datos confidenciales, propiedad intelectual, información del cliente y otros recursos digitales esenciales para el funcionamiento adecuado de la misma.

Luego se procedió a hacer un análisis general de los datos obtenidos que se detalla a continuación:

Políticas de seguridad

La empresa Dibeal Cia. Ltda. actualmente no tiene un manual de políticas de seguridad informática, sin embargo, tiene implementados algunos controles que permiten limitar el acceso no autorizado a la información, pero estos no se encuentran debidamente documentados.

Organización de la seguridad de la información

Actualmente no se cuenta con un departamento dedicado a la seguridad informática sin embargo como departamento de TI se han considerado estos temas y se ha evaluado herramientas adicionales que puedan ayudar a mejorar este aspecto.

El departamento de TI al estar encargado de los diferentes procesos dentro de la organización (Soporte n1, n2, etc.), como ya mencionamos anteriormente no cuenta con personal dedicado al monitoreo de las herramientas que se han implementado, por lo que, mientras no se reporte algún tipo de incidente por parte de los usuarios, se asume que todo marcha bien.

Seguridad Física

Debido al giro de negocio de la empresa se ha implementado un sistema de video vigilancia y control de acceso a las diferentes áreas incluyendo el Data Center por medio de lectores biométricos.

En caso de cortes eléctricos en el sector para garantizar la continuidad del negocio se encuentra implementado un total 5 UPS que están conectados a los diferentes Racks con una duración de hasta 2 horas de batería, adicional cuenta con un generador eléctrico que se acciona automáticamente después de un minuto de detectar que no existe energía eléctrica en la red.

En cuanto al mantenimiento de los equipos que hacen parte del Data Center, al carecer de documentación, no se tiene definido un cronograma de mantenimiento preventivo lo que podría con el tiempo provocar daño de los mismos.

Controles de acceso

Para el acceso a los computadores personales y aplicaciones utilizadas en la organización se han establecido el uso de contraseñas seguras que son custodiadas por cada

usuario, las mismas que deben tener un mínimo de 8 caracteres y deben contener al menos una letra mayúscula, caracteres numéricos y especiales.

Gestión de incidentes en la seguridad de la información

En caso de existir un incidente de seguridad informática el jefe de sistemas es la persona que se encarga de disponer de las acciones a seguir ya que no se cuenta con un procedimiento formal cuando se trata de este tema.

Años atrás la empresa fue víctima de un ataque de ransonware donde se vio afectada la data de la misma, actualmente los constantes ataque de phishing hace vulnerable el servicio de correo electrónico.

Como medida preventiva se empezó a hacer uso de la regla 3, 2, 1 para la realización de respaldos donde se tiene 3 copias de los datos delicados que posee la empresa en al menos 2 diferentes medios de almacenamiento

CAPÍTULO II: PROPUESTA

A continuación, se detalla el desarrollo del plan y los resultados obtenidos.

2.1 Fundamentos teóricos aplicados

Para el desarrollo del plan de seguridad informática basado en la evaluación de los controles de la ISO 27002, que permita la identificación de vulnerabilidades: Caso empresa DIBEAL; se procede a hacer una investigación teórica referente a la evaluación de riesgos mediante la ISO 27002.

2.1.1. ISO 27002: 2013

La ISO 27002:2013 cuenta con 14 dominios, 35 objetivos de control y 114 controles los mismos que pretenden ser una referencia para las organizaciones dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Mediante este estándar se tiene las directrices para la "gestión de seguridad de la información específicas de la industria y la organización, teniendo en cuenta sus entornos de riesgo de seguridad de la información específicos" (NTE INEN-ISO/IEC 27002, 2013).

La ISO/IEC 27002 se encuentra estructurada en dieciocho secciones la cual empieza desde la sección cero en la cual se encuentran los "antecedentes y contexto" de la normativa, luego se encuentra la parte uno en la que se encuentra el objeto en la que la "Norma Internacional proporciona directrices para normas organizacionales de seguridad de la información y para las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles" (NTE INEN-ISO/IEC 27002, 2013, p. 1).

La parte dos contiene las "referencias normativas", por otro lado, la parte tres hace referencia a los "términos y definiciones", la parte cuatro da a conocer la "estructura" en la que se indica que la "norma contiene 14 cláusulas de control de la seguridad que en su conjunto contienen un total de 35 categorías principales de seguridad y 114 controles" (NTE INEN-ISO/IEC 27002, 2013)

Dentro de este marco, en la sección cinco se detalla las "políticas de seguridad de la información" las cuales tienen como objetivo orientar y apoyar en la dirección de la seguridad de la información tomando en cuenta los objetivos del negocio y las leyes establecidas. La sección seis indica la "organización de la seguridad de la información" cuyo objetivo es

“establecer un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización” (NTE INEN-ISO/IEC 27002, 2013)

La sección siete hace referencia a la “seguridad ligada a los recursos humanos” cuyo objetivo es “asegurar que los empleados y contratistas entiendan sus responsabilidades y que sean aptos para los roles” en los cuales se desempeñan (NTE INEN-ISO/IEC 27002, 2013, p. 11). Siguiendo ese orden la parte ocho indica la “gestión de activos” y tiene como objetivo identificar los activos y definir responsabilidades.

Por su parte la sección nueve hace referencia al “control de acceso”, y en la diez se considera la “criptografía”, en la once la “seguridad física y del ambiente” que tiene como objetivo “evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de información y la información de la organización” (NTE INEN-ISO/IEC 27002, 2013, p. 36). La parte doce hace referencia a la “seguridad de las operaciones” en la que se tiene como objetivo “asegurar la operación correcta y segura de las instalaciones de procesamiento de información” (NTE INEN-ISO/IEC 27002, 2013, p. 44).

En la sección trece se hace referencia a la “seguridad de las comunicaciones”, en la sección catorce se hace referencia la “adquisición, desarrollo y mantenimiento de los sistemas de información”, en la quince la “relación con los proveedores”, en la 16 la “gestión de incidentes de seguridad de la información” cuyo objetivo es “garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades” (NTE INEN-ISO/IEC 27002, 2013, p. 76).

Finalmente, en la sección diecisiete se detallan los “aspectos de seguridad de la información en la gestión de continuidad del negocio” y en la sección dieciocho se establece el cumplimiento cuyo objetivo es “evitar los incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con los requisitos de seguridad” (NTE INEN-ISO/IEC 27002, 2013, p. 83).

2.1.2. Vulnerabilidades

Las vulnerabilidades del sistema son debilidades en el software o hardware de un servidor o cliente que pueden ser explotadas por un intruso determinado para obtener acceso a una red o cerrarla. Donald Pipkin (2000) define la vulnerabilidad del sistema como “una

condición, una debilidad o ausencia de un procedimiento de seguridad o controles técnicos, físicos o de otro tipo que podrían ser explotados por una amenaza" (p. 56).

Defectos de diseño

Los dos componentes principales de un sistema informático, el hardware y el software, suelen tener defectos de diseño. Los sistemas de hardware son menos susceptibles a fallas de diseño que sus contrapartes de software debido a su menor complejidad, lo que los hace más fáciles de probar; número limitado de posibles insumos y resultados esperados, lo que nuevamente facilita la prueba y verificación; y la larga historia de la ingeniería de hardware. Pero incluso con todos estos factores respaldando la ingeniería de hardware, debido a la complejidad de los nuevos sistemas informáticos, los defectos de diseño siguen siendo comunes. (Fernández Fernández, 2015)

Pero los mayores problemas de vulnerabilidad de seguridad del sistema se deben a fallas en el diseño del software. Varios factores causan fallas en el diseño del software, incluido el hecho de pasar por alto los problemas de seguridad en su conjunto. Sin embargo, tres factores principales contribuyen en gran medida a los fallos en el diseño del software: factores humanos, complejidad del software y fuentes de software confiables. (Cayambe, 2023)

Factores humanos

En la categoría del factor humano Pipkin (2000) indica que se tiene vulnerabilidades debido a:

1. Lapsos de memoria y fallas de atención: por ejemplo, se suponía que alguien había eliminado o agregado una línea de código, probado o verificado, pero no lo hizo por simple olvido.
2. Apresurarse a terminar: El resultado de la presión, generalmente por parte de la gerencia, para sacar el producto al mercado, ya sea para reducir los costos de desarrollo o para cumplir con el plazo del cliente, puede causar problemas.
4. Exceso de confianza y uso de algoritmos no estándar o no probados: antes de que los pares prueben completamente los algoritmos, se incluyen en la línea de productos porque parecen haber funcionado en algunas pruebas.
5. Malicia: Los desarrolladores de software, como cualquier otro profesional, tienen personas maliciosas en sus filas. Se sabe que errores, virus y gusanos se incrustan y

descargan en el software, como es el caso del software troyano, que se inicia solo en una ubicación determinada.

2.2 Descripción de la propuesta

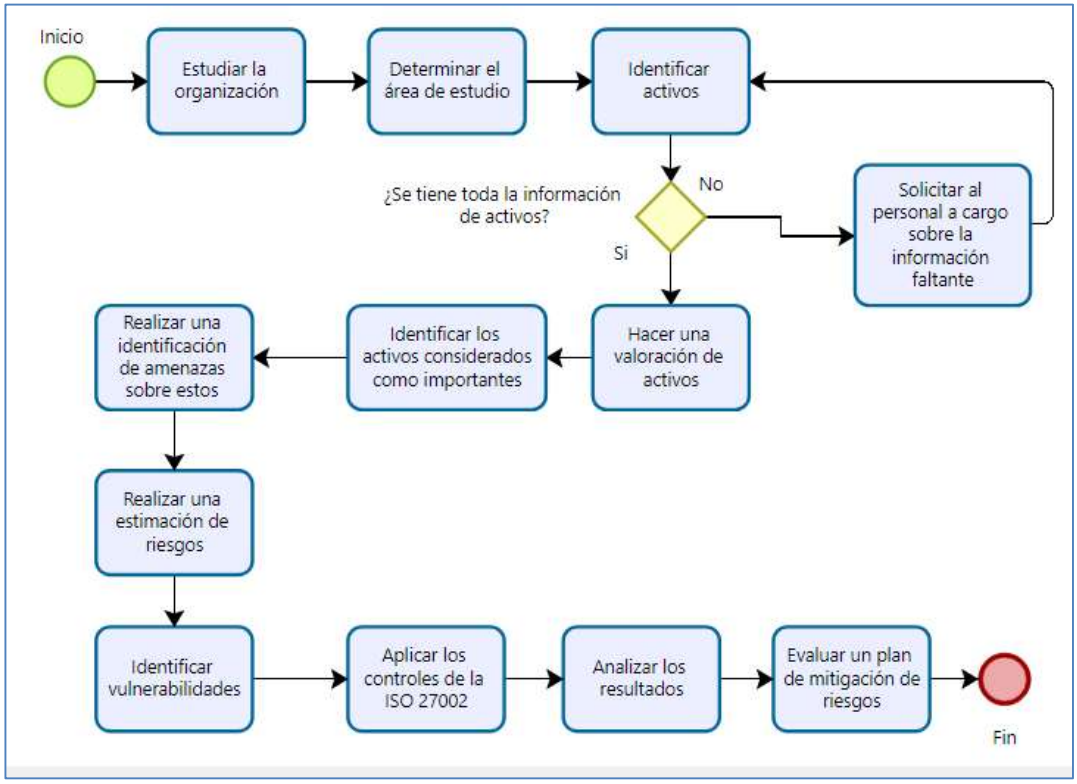
A continuación, se hace una descripción detallada de el plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.

a. Estructura general

Para realizar el plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL. Se estructuró su desarrolló tal como se muestra en la figura 9 en la cual se detalla cada paso a realizarse para el correcto desarrollo de la propuesta.

Figura 9

Estructura de la propuesta



b. Explicación del aporte

Con la presente investigación se pretende elaborar un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL, para lo cual se sigue cada uno de los pasos mostrados a continuación:

Estudio de la organización: En este paso se identifica la organización de estudio para ello se empieza conociendo su fundación, reseña histórica, giro del negocio, misión, visión. Debido a que estos aspectos son importantes; ya que permiten conocer el giro de negocio y de esta manera relacionarse con cada uno de los procesos que se desarrollan dentro de la organización con la finalidad de identificar las áreas más sensibles en las que se maneje la información considerada como importante.

Determinar el área de estudio: Una vez identificada la organización de estudio se procede a determinar cuál es el área en la que se maneja los procesos relacionados con información sensible y que a la vez necesitan ser protegidos para de esta manera evitar pérdidas o que se comprometa el funcionamiento adecuado de la empresa DIBEAL.

Identificación de activos: Una vez determinada el área de estudio se procedió a identificar los activos más importantes que se utilizan para el almacenamiento de la información, los cuales se dividirán en servidores, comunicaciones, computadoras y aplicaciones.

Valoración de activos: Para la valoración de activos se procede a hacerlo a través de juicio de expertos los cuales conocen el funcionamiento de cada equipo dentro de la organización, así como la información que se maneja dentro de la organización.

Identificar activos considerados como importantes para el estudio: Una vez realizada la valoración de activos se identifican los bienes informáticos considerados como críticos que necesitan ser resguardados.

Identificación de amenazas: Luego de identificar los activos más importantes para el estudio se procede a identificar las amenazas en cada uno de ellos tomando como referencia los criterios mostrados en la ISO 27005 relacionada con los diferentes tipos de amenazas.

Estimación de riesgos: En el orden de ideas presentado e identificadas las amenazas se procede a hacer la estimación de riesgos, considerando una escala de alto, medio y bajo.

Identificación de vulnerabilidades: Para la identificación de vulnerabilidades se toma como referencia el uso de la herramienta Nessus, ya que esta herramienta proporciona un escáner de fácil uso y un informe completo de vulnerabilidades categorizada como altas, medias, bajas y de información.

Aplicación de controles de la ISO 27002: Para evaluar los controles de la ISO 27002 se procede a hacer una revisión técnica en conjunto con el jefe del área de TI, para lo cual se hace una valoración en cuanto a cumplimiento.

Plan de mitigación de riesgos: El plan de mitigación de riesgos estará centrado en la protección de activos considerados como importantes para el estudio, así como en la mitigación de vulnerabilidades y la generación de posibles soluciones para evitar que afecten el correcto funcionamiento de la empresa.

c. Estrategias y/o técnicas

Para la elaboración de el plan de mitigación de riesgos en la empresa DIBEAL se lo hace de la siguiente manera:

Identificación de activos: Se identifican los activos considerados como importantes para la organización.

Identificación de riesgos: Se procede a hacer un análisis exhaustivo para identificar todos los posibles riesgos relacionados con los activos relacionados como importantes para el estudio.

Utilización de herramientas: Se utiliza Nessus como herramienta de apoyo ya que esta permite la identificación de vulnerabilidades.

Categorización de riesgos: Se agrupa los riesgos en categorías para facilitar la gestión y la asignación de recursos.

Evaluación de riesgos: Se evalúa la probabilidad de que ocurra cada riesgo y el impacto potencial en el proyecto.

Priorización de riesgos: Se prioriza los riesgos según su impacto y probabilidad, para centrar los esfuerzos en los más críticos.

Desarrollo de estrategias de mitigación: Finalmente se diseña estrategias específicas para abordar cada riesgo identificado.

2.3 Propuesta de un plan de mitigación de riesgos

El plan de mitigación de riesgos basándose en la evaluación realizada con la Norma ISO 27002 y la identificación de vulnerabilidades, para la empresa DIBEAL se encuentra detallado en el Anexo 4.

2.4 Validación de la propuesta

Para la validación de la propuesta se toma como referencia el juicio de expertos es por esta razón que se contactó con el Ing. Oscar Ramos el mismo que desempeña el puesto de jefe de TI en la empresa DIBEAL, el cual considero que el proyecto tiene un impacto alto ya que el alcance de la propuesta ayuda a generar valor para la empresa, en cuanto a aplicabilidad, conceptualización, actualidad, calidad técnica, factibilidad y pertinencia se consideró muy adecuada de ahí que se obtuvo una puntuación de 35 lo que indica que la propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades es válida y viable de realizar. (Anexo 5)

Por otro lado, el Ing. Kevin Vera el cual desempeña el cargo de especialista Networking en Netby Condulting considero que el proyecto es viable dando la calificación de muy adecuado en cuanto a impacto, conceptualización, actualidad y calidad técnica. Mientras que considero bastante adecuado la aplicabilidad, factibilidad y pertinencia. Como recomendación considera que se podría tomar como guía casos de éxito y aplicar buenas prácticas. Dando una puntuación de 32 para lo cual se considera como un instrumento válido y se prosigue con el desarrollo del plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002. (Anexo 6)

2.5 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados, como se muestra en la tabla 1.

Tabla 1.

Matriz de articulación

Ejes o partes principales del proyecto		Sustento teórico	Sustento metodológico	Estrategias/ técnicas	Descripción de resultados	Instrumentos aplicados
1	Controles de la ISO 27002	La ISO 27002 cuenta con 14 dominios, 35 objetivos de control y 114 controles los mismos que pretenden ser una referencia para las organizaciones dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). (NTE INEN-ISO/IEC 27002, 2013)	Enfoque cualitativo	Investigación bibliográfica	Ayuda a sustentar conocimiento previos y necesarios para entender la propuesta	Revisión Documental

3	Reconocimiento de la empresa	El reconocimiento del lugar de estudio es la familiarización o identificación de un lugar específico (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014).	Enfoque cualitativo	Investigación de campo	Ayuda a conocer el problema de estudio ya que se investiga en el lugar donde se está desarrollando	Ficha de Observación
5	Valoración de activos	Es un proceso para la gestión de la seguridad de la información mediante el cual se puede tomar decisiones en una organización (Quiroga, 2023).	Enfoque cuantitativo	Observación	Permite el reconocimiento de los activos considerados como primordiales dentro de la organización.	Ficha de Observación
2	Vulnerabilidades	Una vulnerabilidad es considerada como una debilidad en un sistema determinado que puede comprometer la seguridad (Cayambe, 2023).	Enfoque cuantitativo	Investigación bibliográfica	Ayuda a identificar las vulnerabilidades para generar un plan de mitigación de riesgos enfocado en la mitigación de riesgos.	Herramienta para análisis de código

4	Plan de seguridad informática	Es un documento detallado que establece las políticas, procedimientos, controles y medidas que una organización implementará para proteger sus activos (Cayambe, 2023).	Enfoque cualitativo	Investigación bibliográfica	Ayuda a sustentar conocimiento previos y necesarios para entender la propuesta	Revisión Documental

2.6 Análisis de resultados. Presentación y discusión.

A continuación, se procede a realizar el estudio de la organización con la finalidad de conocer el giro de negocio para lo cual se empieza con una reseña histórica tal y como se presenta a continuación:

2.6.1. Estudio de la organización

Dibeal Cia. Ltda fue fundada en 1989 prestando servicios en "importación, comercialización y distribución de productos de consumo". La empresa ha tenido gran acogida debido a que representa de manera exclusiva en Ecuador, marcas premium mundialmente reconocidas. Se caracteriza por ofrecer buena calidad y también debido a su aporten al mercado ecuatoriano mediante la diversidad y cultura gastronómica. Los productos que la empresa comercializa son ideales para "hogares, restaurantes, bares, hoteles, tiendas especializadas, supermercados, etc.". (Dibeal, 2023)

A continuación se presenta la misión y visión de la empresa Dibeal.

Misión

"Brindar a nuestros clientes y consumidores productos de excelente calidad, comprometiéndonos a la búsqueda continua de productos innovadores que aporten al mercado ecuatoriano diversidad y cultura gastronómica.". (Dibeal, 2023)

Visión

"Ser la empresa de referencia ineludible en Ecuador, para representar las marcas internacionales más reconocidas; ofreciendo una variedad de productos que nos permitan anticiparnos a los deseos de nuestros clientes y consumidores, con eficacia y dinamismo.". (Dibeal, 2023)

Estructura organizacional

A continuación, se presenta la estructura organizacional empezando por el organigrama de la gerencia general tal como se detalla en la figura 9, también se presenta el organigrama del área de TI figura 10 y figura 11; de la empresa Dibeal:

Figura 10

Organigrama Gerencia General.

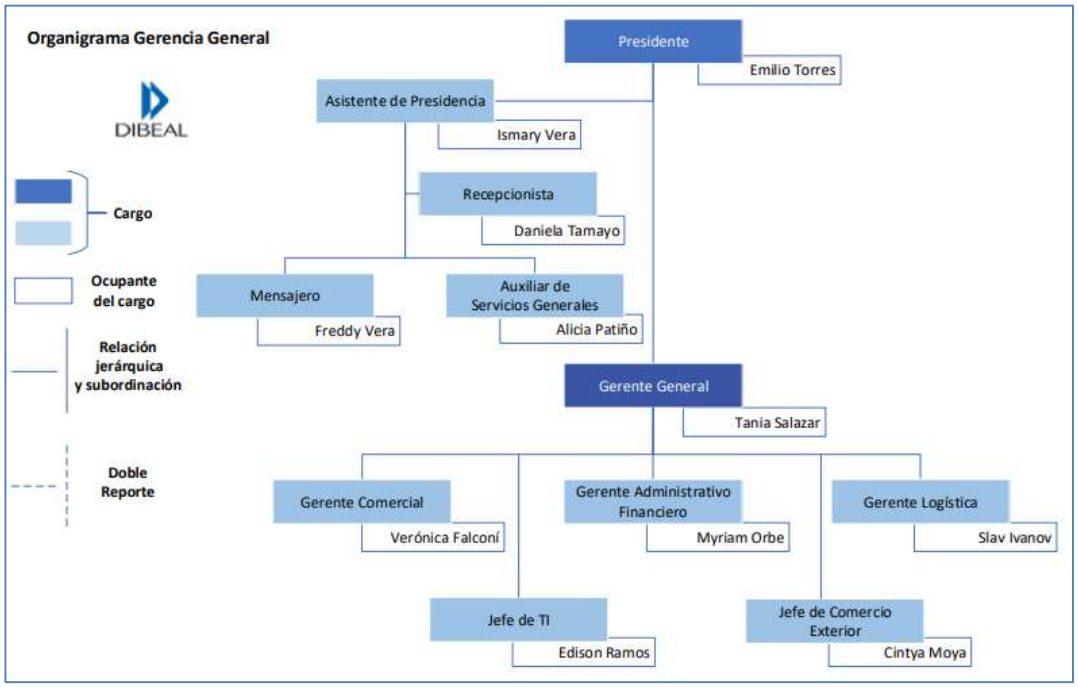
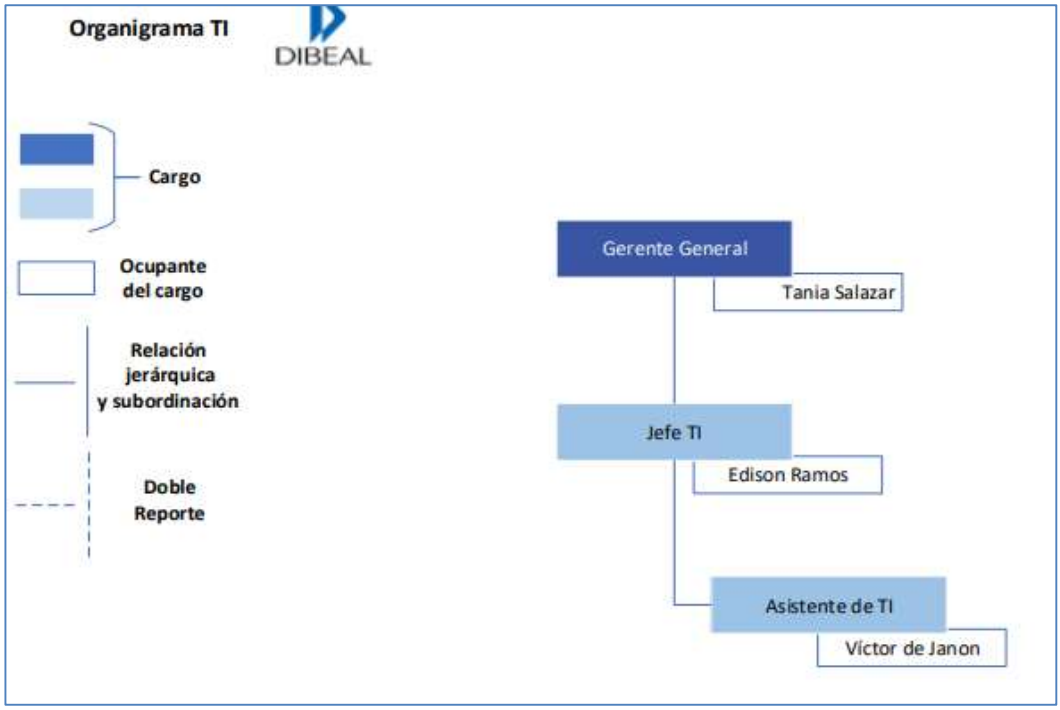


Figura 11

Organigrama TI.



2.6.2. Identificación y valoración de activos

Una vez analizado el giro de negocio se procede a identificar y valorar los activos más importantes que se utilizan para el almacenamiento de la información, los cuales se dividirán en servidores (tabla 2), comunicaciones (tabla 3), computadoras (tabla 4) y aplicaciones (tabla 5).

Tabla 2:

Servidores

SERVIDORES	MARCA	PROCESADOR	MEMORIA	DISCO	SISTEMA OPERATIVO
SERVIDOR SAP ANTIGUO	IBM	Intel (R) Xeon (R) CPU E5-2620 V2	70 GB	500-500-200-200-1TB-2TB	WINDOWS SEREVER 2016
SERVIDOR VARIOS APLICATIVOS	IBM	Intel (R) Xeon (R) CPU E5-2620 V2	64 GB	1TB-200 GB-130 GB-2TB-1TB-1.5TB	WINDOWS SEREVER 2016
MOBILVENDOR	DELL	Intel (R) Xeon (R) CPU E3-11 2225 V5	40 GB	1 TB - 2 TB	WINDOWS SEREVER 2016
FACTURACION ELECTRONICA ANTIGUO	HP	Core I5	8 GB	500 GB	
ACTIVE DIRECTORY ANTIGUO	HP	Xeon (R) 1.6	8 GB	1 TB	
SERVIDOR SAP ACTUAL	LENOVO	Xeon 10 Core	96 GB	480 GB x 4	LINUX
MONITOR-DATACENTER	LG	S/N	S/N	S/N	S/N
NAS	SYSNOLOGY			6 discos 2 Teras	
NAS	WD			4 TB	

Tabla 3:

Comunicaciones

TIPO	MARCA
SWITCH	ARUBA
SWITCH	ARUBA
MONITOR	LG

SWITCH	ARUBA
ACESS POINT	ARUBA
ACESS POINT	ARUBA
ACESS POINT	ARUBA
ACESS POINT	ARUBA
ACESS POINT	ARUBA
UPS	TRIPLITE
UPS	TRIPLITE
SWITCH	HP
FIREWALL	FORTINET

Tabla 4:

Computadoras

PC/MONITOR /PORTATIL	MARCA	MODELO	SERIE	PROCESADOR	MEMORIA	DISCO	APLICACIONES	INFORMACIÓN
PORTATIL	HP	PROBOOK 440	5CD307 8BGL	CORE I7	16 GB	500 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar, MobilVendor	Facturación electrónica, datos clientes, carpetas compartidas información financiera
PORTATIL	HP	PROBOOK 440 G9	5CD307 8BFF	CORE I7	16 GB	500 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar, MobilVendor	Facturación electrónica, datos clientes, carpetas compartidas información financiera
PORTATIL	HP	PROBOOK 440 G9	5CD307 0ZTW	CORE I7	16 GB	1Tb SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar, MobilVendor	Facturación electrónica, datos clientes, carpetas compartidas información financiera
PORTATIL	HP	PROBOOK 440 G9	5CD307 8BGB	CORE I7	16 GB	500 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar, MobilVendor	Facturación electrónica, datos clientes, carpetas compartidas información financiera
PORTATIL	HP	PROBOOK 440 G9	5CD307 8BFP	CORE I7	16 GB	500 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa	Facturación electrónica, datos clientes, carpetas compartidas

							Estándar, MobilVendor	información financiera
PORTATIL	LENOVO	ThinkPad E15	PF49K8VF	CORE I7	16 GB	480 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar, MobilVendor	Facturación electrónica, datos clientes, carpetas compartidas información financiera, comercial
PORTATIL	LENOVO	ThinkBook 15,6 Pulgadas	LR0ET6LR	CORE I7	16 GB	480 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar	Facturación electrónica, datos clientes, carpetas compartidas información personal interno
PORTATIL	LENOVO	ThinkPad E14	SL10W47313	CORE I7	16 GB	480 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar	Facturación electrónica, datos clientes, carpetas compartidas información jurídicos
PORTATIL	LENOVO	E590	PF49KDHX	CORE I7	16 GB	480 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar	Facturación electrónica, datos clientes, carpetas compartidas información financiera
PORTATIL	HP	ENVY	8CG8517FMK	CORE I7	16 GB	512 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar	Facturación electrónica, datos clientes, carpetas compartidas información financiera
PORTATIL	LENOVO	V330	MP1HB4HQ	CORE I7	20 GB	500 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar	Facturación electrónica, datos clientes, carpetas compartidas información financiera
PORTATIL	DELL	INSPIRON	G3G7G13	CORE I5	16 GB	480 GB	ERP SAP Business One Client, Microsoft 365 Empresa Estándar	Facturación electrónica, datos clientes, carpetas compartidas información financiera, comercial, contable

PORTATIL	LEN OVO	V330	CORE I7	20 GB	480 GB SSD	ERP SAP Business One Client, Microsoft 365 Empresa Estándar	Facturación electrónica, datos clientes, carpetas compartidas información financiera, comercial, contable

Tabla 5:

Aplicaciones

Aplicación	Tipo de Licencia
ERP SAP Business One Client	Administrativa, Financiera, Logística
Office 365	Microsoft 365 Empresa Estándar, Exchange Online (plan 1)
MobilVendor	Web, Móvil

Para la valoración de activos se procede a hacerlo a través de juicio de expertos de ahí que se identifica que los activos más importantes para la organización son los que se presentan a continuación en la tabla 6 y tabla 7:

Tabla 6:

Servidores

SERVIDORES	DIRECCIÓN IP
SERVIDOR SQL	192.168.0.28
SERVIDOR AMBIENTE DE PRUEBAS	192.168.0.108
SERVIDOR SAP ACTUAL	192.168.0.20
TERMINAL SERVER	192.168.0.211

Tabla 7:

Computadoras

PC/MONITOR/PORTATIL	IP	INFORMACIÓN
PORTATIL1	192.168.0.114	Soporte de negocio
PORTATIL2	192.168.0.116	Gerencia Comercial
PORTATIL3	192.168.0.111	Contabilidad

2.6.3. Identificación de amenazas y estimación de riesgos

Luego de haber realizado la valoración de activos se encontró los bienes informáticos considerados como críticos que necesitan ser resguardados, de ahí que se procede a identificar las amenazas que se agrupan en diferentes categorías como se detalla en la tabla 8.

Tabla 8:

Identificación de amenazas

Criterio	Código	Valor
Daño físico	DF 1	Fuego
	DF 2	Daño por agua
	DF 3	Accidente importante
	DF 4	Destrucción del equipo o los medios
Compromiso de la información	CI1	Hurto de medios o documentos
	CI2	Hurto de equipo
	CI3	Recuperación de medios reciclados o desechados
	CI4	Divulgación
	CI5	Datos provenientes de fuentes no confiables
	CI6	Manipulación con hardware
	CI7	Manipulación con software
Fallas técnicas	FT1	Falla del equipo
	FT2	Mal funcionamiento del equipo
	FT3	Mal funcionamiento del software
	FT4	Incumplimiento en el mantenimiento del sistema de información
Nivel de datos y redes	ND1	Manejo inadecuado de datos críticos (modificar, borrar, etc.)
	ND2	Transmisión no cifrada de datos críticos
	ND3	Dependencia de servicio técnico externo
	ND4	Red inalámbrica expuesta al acceso no autorizado
	ND5	Acceso electrónico no autorizado a sistemas externos
	ND6	Acceso electrónico no autorizado a sistemas internos
Acciones no autorizadas	ANA1	Uso no autorizado del equipo
	ANA2	Copia fraudulenta del software
	ANA3	Uso de software falso o copiado
	ANA4	Corrupción de los datos
	ANA5	Procesamiento ilegal de los datos
Compromiso de las funciones	CF1	Error en el uso
	CF2	Abuso de derechos
	CF3	Falsificación de derechos
	CF4	Negación de acciones
	CF5	Incumplimiento en la disponibilidad del personal
Factor humano	FH1	Destrucción de información
	FH2	Divulgación ilegal de información
	FH3	Ganancia monetaria
	FH4	Alteración no autorizada de los datos

Nota: En la tabla se muestran los diferentes tipos de amenazas. Tomado de ISO 27005 (2011).

Con las amenazas identificadas anteriormente se procede a hacer la valoración de riesgos, para ello se toma como referencia la valoración detallada en la tabla 9 y tabla 10, que se toma como referencia de la ISO 27005.

Tabla 9:

Valoración de riesgos

Criterio	Valor
Riesgo bajo	1
Riesgo medio	2
Riesgo alto	3

Nota. En la tabla se muestran la escala para realizar la valoración de riesgos. Tomado de ISO 27005 (2011).

Tabla 10:

Valoración de riesgos

Criterio	Código	Servidor SQL	Servidor AP	Servidor SAP	Terminal server	Portátil 1	Portátil 2	Portátil 3
Daño físico	DF 1	2	1	1	1	1	1	1
	DF 2	2	2	2	2	2	2	2
	DF 3	2	1	2	1	2	1	2
	DF 4	2	1	1	1	2	1	1
	Promedio	**2**	**1.25**	**1.5**	**1.25**	**1.75**	**1.25**	**1.5**
Compromiso de la información	CI1	3	3	3	3	3	3	3
	CI2	1	1	1	1	3	3	3
	CI3	1	2	3	2	2	1	2
	CI4	3	3	2	3	2	3	2
	CI5	3	2	3	2	3	2	3
	CI6	3	3	2	3	3	3	3
	CI7	3	3	2	3	3	3	3
	Promedio	**2.43**	**2.43**	**2.28**	**2.43**	**2.71**	**2.57**	**2.71**
Fallas técnicas	FT1	3	3	3	2	2	2	2
	FT2	1	1	1	1	2	3	2
	FT3	1	2	2	2	2	2	2
	FT4	2	2	2	2	3	3	3
	Promedio	**1.75**	**2**	**2**	**1.75**	**2.25**	**2.5**	**2.25**
Nivel de datos y redes	ND1	3	3	3	3	3	3	3
	ND2	3	3	3	3	3	3	3
	ND3	2	2	2	2	1	1	1
	ND4	2	2	2	2	3	3	2
	ND5	1	2	3	3	3	3	3
	ND6	2	2	2	2	3	2	3
	Promedio	**2.17**	**2.33**	**2.5**	**2.5**	**2.67**	**2.5**	**2.67**
Acciones no autorizadas	ANA1	2	2	2	3	3	3	3
	ANA2	1	1	1	1	2	2	2
	ANA3	1	1	1	1	3	3	3
	ANA4	3	3	3	3	3	3	3
	ANA5	1	1	1	1	1	1	1
	Promedio	**1.6**	**1.6**	**1.6**	**1.8**	**2.4**	**2.4**	**2.4**
Compromiso de las funciones	CF1	3	3	3	3	3	3	3
	CF2	1	1	1	1	1	1	1
	CF3	1	1	1	1	1	1	1
	CF4	1	1	1	1	1	1	1
	CF5	2	1	2	1	2	2	1
	Promedio	**1.6**	**1.4**	**1.6**	**1.4**	**1.6**	**1.6**	**1.4**

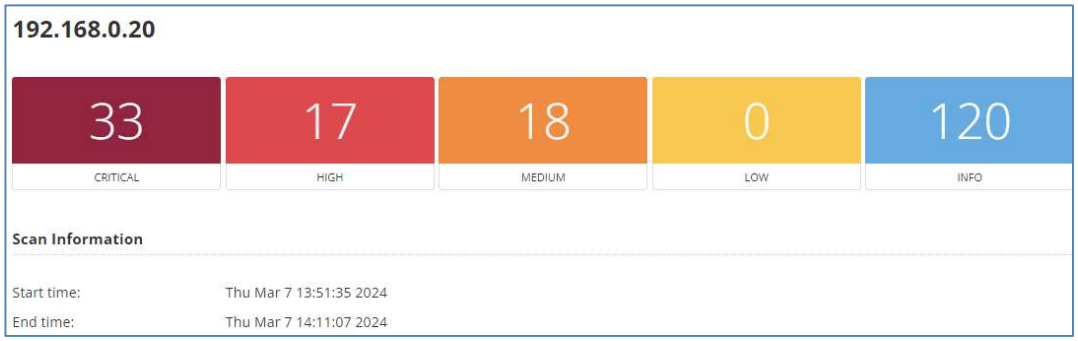
	FH1	2	2	2	2	3	3	3
Factor	FH2	3	3	3	3	3	3	3
humano	FH3	1	1	1	1	1	1	1
	FH4	3	3	3	3	3	3	3
	Promedio	**2.25**	**2.25**	**2.25**	**2.25**	**2.5**	**2.5**	**2.5**

2.6.4. Identificación de vulnerabilidades

De acuerdo a los datos obtenidos se encontró que existe mayor riesgo relacionado con compromiso de la información, nivel de datos y redes y factor humano. Una vez determinados los activos más importantes e identificados los riesgos se procede a hacer un análisis de vulnerabilidades mediante la herramienta Nessus, los resultados se muestran a continuación en la figura 12:

Figura 12

Vulnerabilidades servidor SAP-ERP.



Los datos indican que el servidor web remoto se ve afectado por múltiples vulnerabilidades. La versión de Apache https instalada en el host remoto es anterior a la 2.4.41. Por lo tanto, se ve afectado por múltiples vulnerabilidades como se menciona en el aviso 2.4.41, incluidas las siguientes:

- Se informó “un problema limitado de secuencias de comandos entre sitios que afectaba a la página de error mod_proxy. Un atacante podría provocar que el enlace de la página de error” (Nessus, 2023) tenga un formato incorrecto y, en su lugar, apunte a una página de su elección. Esto solo sería explotable cuando un servidor estuviera configurado con el proxy habilitado, pero estuviera mal configurado de tal manera que se mostrara la página de error de proxy. (CVE-2019-10092)

- Algunas implementaciones de “HTTP/2 son vulnerables al almacenamiento en búfer de datos interno sin restricciones” (Nessus, 2023), lo que podría provocar una denegación de servicio. El atacante abre la ventana HTTP/2 para que el par pueda enviar sin restricciones; sin embargo, dejan la ventana TCP cerrada para que el interlocutor no pueda escribir (muchos de) los bytes en el cable. Luego, el atacante envía un flujo de solicitudes para un objeto de respuesta grande. Dependiendo de cómo los servidores pongan en cola las respuestas, esto puede consumir exceso de memoria, CPU o ambos. (CVE-2019-9517)

Del análisis de los hosts se obtuvo la siguiente información mostrada en la figura 13:

Figura 13

Vulnerabilidades servidores

Del análisis del sevidor SQL (192.168.0.28) se obtuvo como resultado que existen vulnerabilidades relacionadas con información. Mientras que del servidor de ambientes de pruebas se encontro una vulnerabilidad alta 6 medias y 40 relacionadas con la información. Entre los principales hallazgos se tiene que “no es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de intermediario contra el servidor SMB” (Nessus, 2023).

Tambien se encontró que “no se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación” (Nessus, 2023):

- En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. (Nessus, 2023)
- En segundo lugar, la cadena de certificados “puede contener un certificado que no sea válido en el momento del análisis. Esto puede ocurrir cuando el análisis se realiza antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado”.
- En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. “Las firmas incorrectas se pueden solucionar haciendo que su emisor vuelva a firmar el certificado con la firma incorrecta. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utilizó un algoritmo de firma que Nessus no admite o no reconoce” (Nessus, 2023).

“Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques de intermediario contra el host remoto” (Nessus, 2023).

Tambien se encontró que el servicio remoto admite el uso del cifrado RC4. “El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene fallas en la generación de un flujo pseudoaleatorio de bytes” (Nessus, 2023), de modo que se introduce una amplia variedad de pequeños sesgos en el flujo, lo que disminuye su aleatoriedad.

“Si el texto sin formato se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante puede obtener muchos (es decir, decenas de millones) de textos cifrados, es posible que pueda derivar el texto sin formato” (Nessus, 2023).

Figura 14

Vulnerabilidades pc contabilidad

Luego de realizar el Scanner de vulnerabilidades se encontró que en la PC de contabilidad (figura 14) hay una vulnerabilidad media y 35 relacionadas con la información las mismas que indican que “no es necesario firmar en el servidor SMB remoto. De ahí que un atacante remoto no autenticado puede aprovechar esto para realizar ataques de intermediario contra el servidor SMB” (Nessus, 2023).

También se encontró que fue posible enumerar nombres de CPE que coincidían en el sistema remoto. Es decir que, al utilizar la información obtenida de un escaneo de Nessus, este complemento informa coincidencias de CPE (Enumeración de plataforma común) para varios productos de hardware y software que se encuentran en un host.

Figura 15

Vulnerabilidades pc soporte de negocios

Al realizar el scanner en el pc de soporte de negocios (figura 15) se encontró que existe un alta, cinco medias, y cuarenta y uno relacionadas con la información. De lo que se tiene que “el servicio remoto admite el uso de cifrados SSL de potencia media. Es decir que el host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media” (Nessus, 2023). Nessus considera de potencia media cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el conjunto de cifrado 3DES.

Además, que no se puede confiar en el certificado SSL para este servicio. “No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas diferentes,

en las que se puede romper la cadena de confianza, como se indica a continuación" (Nessus, 2023):

- "En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida" (Nessus, 2023) .
- "En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento del análisis" (Nessus, 2023).
- "En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas incorrectas se pueden solucionar haciendo que su emisor vuelva a firmar el certificado con la firma incorrecta" (Nessus, 2023).

"Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques" (Nessus, 2023) de intermediario contra el host remoto.

2.6.5. Cumplimiento de controles de la ISO 27002

Para evaluar los controles de la ISO 27002 se procede a hacer una revisión técnica en conjunto con el jefe del área de TI (Anexo 3) de lo que se encontró los datos presentados en la tabla 11 para lo cual se procede a hacer una validación de cada control de acuerdo a la siguiente tabla 12:

Tabla 11:

Criterios para evaluación de controles de la ISO 27002

Criterio Cumplimiento	Abreviatura	Valor
Cumple en su totalidad	CT	5
Cumple significativamente	CS	4
Cumple parcialmente	CP	3
Cumple mínimamente	CM	2
No cumple	NC	1

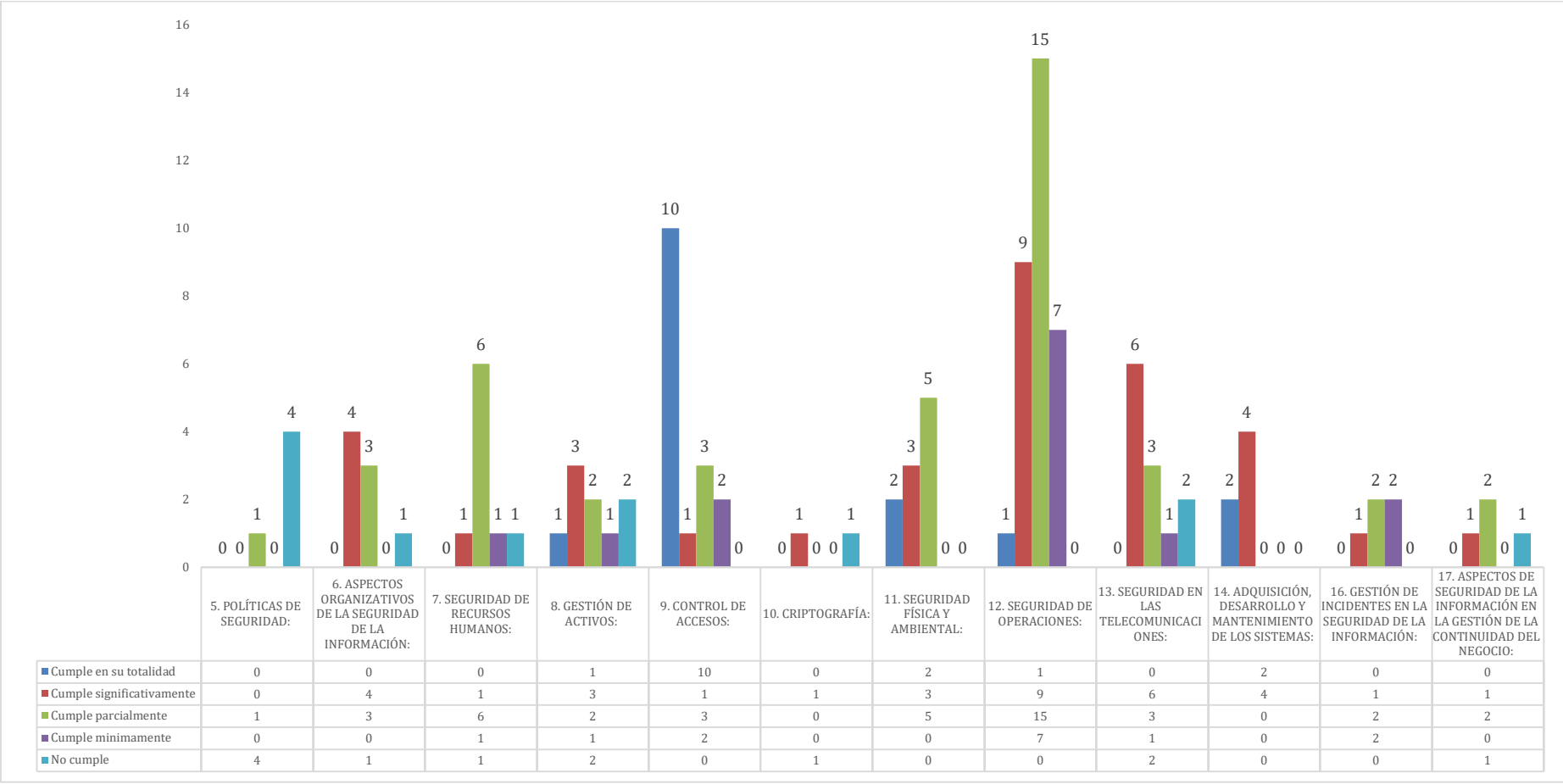
Tabla 12:

Evaluación de controles de la ISO 27002

	CT	CS	CP	CM	NC
5. Políticas de seguridad:	0	0	1	0	4
6. Aspectos organizativos de la seguridad de la información:	0	4	3	0	1
7. Seguridad de recursos humanos:	0	1	6	1	1
8. Gestión de activos:	1	3	2	1	2
9. Control de accesos:	10	1	3	2	0
10. Criptografía:	0	1	0	0	1
11. Seguridad física y ambiental:	2	3	5	0	0
12. Seguridad de operaciones:	1	9	15	7	0
13. Seguridad en las telecomunicaciones:	0	6	3	1	2
14. Adquisición, desarrollo y mantenimiento de los sistemas:	2	4	0	0	0
16. Gestión de incidentes en la seguridad de la información:	0	1	2	2	0
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio:	0	1	2	0	1

Figura 16

Resultado de evaluación de controles de la ISO 27002



	5. POLÍTICAS DE SEGURIDAD:	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN:	7. SEGURIDAD DE RECURSOS HUMANOS:	8. GESTIÓN DE ACTIVOS:	9. CONTROL DE ACCESOS:	10. CRIPTOGRAFÍA:	11. SEGURIDAD FÍSICA Y AMBIENTAL:	12. SEGURIDAD DE OPERACIONES:	13. SEGURIDAD EN LAS TELECOMUNICACIONES:	14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS:	16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN:	17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO:
Cumple en su totalidad	0	0	0	1	10	0	2	1	0	2	0	0
Cumple significativamente	0	4	1	3	1	1	3	9	6	4	1	1
Cumple parcialmente	1	3	6	2	3	0	5	15	3	0	2	2
Cumple minimamente	0	0	1	1	2	0	0	7	1	0	2	0
No cumple	4	1	1	2	0	1	0	0	2	0	0	1

En la evaluación de controles (figura 16) se encontró que en cuanto a políticas de seguridad no se cumple con los controles adecuadamente ya que tan solo el 20% cumplen los cumplen parcialmente y el restante 80% no lo hacen.

Por otro lado, en cuanto a aspectos organizativos de la seguridad de la información se encontró que el 50% no cumple o cumple parcialmente, en la seguridad de recursos humanos se tiene que el 89% cumple parcialmente, mínimamente o no lo hace.

En cuanto a gestión de activos se tiene que el 55% cumple parcialmente, mínimamente o no lo hace. Al evaluar el control de acceso se encontró que el 62% se cumplen en su totalidad y otro 32% lo hacen parcialmente o mínimamente. La seguridad de las operaciones no se cumple con un 52%.

Una vez realizado el estudio de la organización, la valoración de activos, la identificación de amenazas y vulnerabilidades se procedió a evaluar los controles de la ISO 27002 para así proponer un plan de mitigación de riesgos que se detalla en el anexo 4.

CONCLUSIONES

Luego de hacerse el estudio en la empresa DIBEAL se concluyó que es importante proponer un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, ya que esto ayuda a reducir la probabilidad de que ocurran eventos adversos, así como a minimizar su impacto en caso de que se produzcan y mejorar la capacidad de la entidad para gestionar situaciones de riesgo de manera efectiva. Además, un plan de mitigación de riesgos permite identificar y proteger los activos y recursos críticos de una entidad, para así tomar medidas con la finalidad de protegerlos y evitar pérdidas.

Al realizar una investigación teórica de la ISO 27002 se encontró que esta normativa cuenta con 14 dominios, 35 objetivos de control y 114 controles los mismos que pretenden ser una referencia para las organizaciones dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

De acuerdo a los datos obtenidos se encontró que existe mayor riesgo relacionado con compromiso de la información, nivel de datos y redes y factor humano. Entre las principales vulnerabilidades se tienen que el servidor web remoto se ve afectado por múltiples vulnerabilidades. La versión de Apache https instalada en el host remoto es anterior a la 2.4.41. Del análisis del servidor SQL (192.168.0.28) se obtuvo como resultado que existen vulnerabilidades relacionadas con la información. Mientras que del servidor de ambientes de pruebas se encontró una vulnerabilidad alta seis medias y cuarenta relacionadas con la información. Entre los principales hallazgos se tiene que no es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques en el servidor SMB.

De la evaluación de los controles de la ISO 27002 se encontró que en cuanto a políticas de seguridad no se cumple con los controles adecuadamente ya que tan solo el 20% los cumplen parcialmente y el restante 80% no lo hacen. Por otro lado, en cuanto a aspectos organizativos de la seguridad de la información se encontró que el 50% no cumple o cumple parcialmente, en la seguridad de recursos humanos se tiene que el 89% cumple parcialmente, mínimamente o no lo hace. En la gestión de activos se tiene que el 55% cumple parcialmente, mínimamente o no lo hace. Al evaluar el control de acceso se encontró que el 62% se cumplen en su totalidad y otro 32% lo hacen parcialmente o mínimamente. La seguridad de las operaciones no se cumple con un 52%.

RECOMENDACIONES

Luego de hacerse el estudio en la empresa DIBEAL se recomienda implementar cada una de las recomendaciones mostradas en el plan de mitigación de riesgos para así evitar que se comprometa la información y seguridad de la empresa.

La ISO 27002 proporciona controles para la implementación de un Sistema de Gestión de Seguridad de la Información de una manera adecuada de ahí que se recomienda realizar un estudio en el cual se investigue en cuanto a implementación de cada control y nivel de madurez.

Para la valoración de activos se lo hizo de acuerdo al juicio de experto de ahí que se propone que se haga una valoración de activos mediante la ISO 27005 ya que esta normativa proporciona todo el proceso.

De la evaluación de los controles de la ISO 27002 se encontró que en gran parte de controles no se cumplen de ahí que se recomienda un trabajo en el cual se implanten cada uno de los controles que faltan para que la empresa cuente con un Sistema de Gestión de Seguridad de la Información (SGSI) adecuado.

BIBLIOGRAFÍA

Cayambe, J. E. (Marzo de 2023). *Repositorio Digital Universidad Israel.* http://repositorio.uisrael.edu.ec/handle/47000/3562

CIS. (Mayo de 2021). *https://www.cisecurity.org/*. https://learn.cisecurity.org/control-download

Dibeal. (2023). *Página web*. https://www.dibeal.com/quienes-somos/

DIBEAL. (2023). *www.dibeal.com*. https://www.dibeal.com/quienes-somos/

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2014). *Metodologìa de la investigación (6a. ed.).* McGraw-Hill. https://academia.utp.edu.co/grupobasicoclinicayaplicadas/files/2013/06/Metodolog%C3%ADa-de-la-Investigaci%C3%B3n.pdf

Moya, E. J. (10 de Agosto de 2016). *revistapublicando.org.* https://revistapublicando.org/revista/index.php/crv/article/view/175

Narváez, D. F. (Marzo de 2023). *Repositorio digital Universidad Israel.* http://repositorio.uisrael.edu.ec/handle/47000/3561

NTE INEN-ISO/IEC 27002. (2013). *Tecnologías de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información.* INEN. https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27002.pdf

Pipkin, D. (2000). *Information Security: Protecting the Global Enterprise.* Upper Saddle River, NJ: Prentice Hall PTR.

Quiroga, C. B. (Marzo de 2023). *Repositorio Digital Universidad Israel.* http://repositorio.uisrael.edu.ec/handle/47000/3612

Rouse, M. (21 de Mayo de 2020). *www.techopedia.com*. https://www.techopedia.com/definition/28830/nist-800-53

Tamayo, M., y Tamayo. (2003). *El proceso de la investigación científica.* Limusa, Noriega editores. https://www.gob.mx/cms/uploads/attachment/file/227860/El_proceso__de_la_investigaci_n_cient_fica_Mario_Tamayo.pdf

ANEXOS

Anexo 1. Encuesta realizada a los usuarios

ENCUESTA CONSIDERACIONES DE LA SEGURIDAD INFORMÁTICA EN DIBEAL

Le invitamos a participar en esta encuesta que tiene como objetivo descubrir el conocimiento que usted tiene de seguridad informática y como evidencia su aplicación en la empresa.

Su participación es anónima y sus respuestas nos ayudarán a comprender mejor la situación actual de la empresa con respecto a este tema.

Marque con una (x) su respuesta.

1. ¿Conoce usted acerca del término seguridad informática?

   SI ☐ NO ☐

2. ¿Conoce si en la empresa se han tomado medidas o implementado herramientas para temas de seguridad informática en el último año?

   SI ☐ NO ☐

3. De ser Si su respuesta menciónelo(s)

   ☐ Sistema de seguridad de accesos y videovigilancia.

   ☐ Sistema Multifactor de autenticación para acceso a correo electrónico.

   ☐ Capacitaciones acerca de seguridad informática.

   ☐ Otros:

   _____

4. ¿Se ha suscitado algún tipo de incidente de seguridad informática en la empresa en el último año?

   SI ☐ NO ☐

5. ¿Si recibe un mensaje de correo electrónico de dudosa procedencia y contiene links para abrir otras páginas web y usted considera que no es seguro, sabe a qué área debe reportar dicho incidente?

   SI ☐ NO ☐

6. ¿Ha recibido algún tipo de recomendación o consejos a seguir a través del correo empresarial de temas como Phisihing o Vishing en el último año?

   SI ☐ NO ☐

7. ¿Ha recibido capacitaciones referentes a seguridad de informática en el último año?

   SI ☐ NO ☐

8. ¿Conoce si en la empresa existe alguna política interna sobre seguridad informática?

   SI ☐ NO ☐

Anexo 2 Resultado de la encuesta

No. Encuesta	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8
Encuesta 1	SI	SI	1	SI	SI	NO	NO	NO
Encuesta 2	NO	NO	n/a	NO	NO	NO	NO	NO
Encuesta 3	SI	SI	2	NO	SI	NO	NO	NO
Encuesta 4	SI	SI	2	NO	SI	NO	NO	NO
Encuesta 5	SI	SI	2	NO	SI	NO	NO	NO
Encuesta 6	SI	SI	1	NO	SI	NO	NO	NO
Encuesta 7	NO	NO	n/a	NO	NO	NO	NO	NO
Encuesta 8	SI	SI	1	NO	SI	NO	NO	NO
Encuesta 9	SI	SI	1	NO	SI	NO	NO	NO
Encuesta 10	SI	SI	1	NO	SI	NO	NO	NO
Encuesta 11	SI	NO	n/a	NO	SI	NO	NO	NO
Encuesta 12	NO	NO	n/a	NO	NO	NO	NO	NO
Encuesta 13	SI	SI	1	NO	SI	NO	NO	NO
Encuesta 14	SI	SI	2	SI	SI	NO	NO	NO
Encuesta 15	SI	SI	3	NO	SI	NO	NO	NO

Anexo 3. Resultado de ISO 27002

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

El presente instrumento de investigación tiene como objetivo: "Proponer un plan mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL".

INSTRUCCIONES:

Conteste con la mayor objetividad a las preguntas formuladas.

Recuerde que la evaluación es anónima.

Se evalúa de acuerdo al cumplimiento con la siguiente escala:

Criterio Cumplimiento	Valor
Cumple en su totalidad	5
Cumple significativamente	4
Cumple parcialmente	3
Cumple mínimamente	2
No cumple	1

PREGUNTAS	Cumplimiento
5. POLÍTICAS DE SEGURIDAD:	
¿Existen documento(s) de políticas de seguridad de Sistema de Información?	1
¿Existe normativa relativa a la seguridad del Sistema de Información?	1
¿Existen procedimientos relativos a la seguridad de Sistema de Información?	1
¿Existe un responsable de las políticas, normas y procedimientos?	3
¿Existen controles regulares para verificar la efectividad de las políticas?	1
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN:	

¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?	3
¿Existe un responsable encargado de evaluar la adquisición y cambios de Sistema de Información?	4
¿Participan la Dirección y las áreas de la Organización en temas de seguridad?	4
¿Existen condiciones contractuales de seguridad con terceros y outsourcing?	4
¿Existen criterios de seguridad en el manejo de terceras partes?	3
¿Existen programas de formación en seguridad para los empleados, clientes y terceros?	3
¿Existe un acuerdo de confidencialidad de la información que se accede?	4
¿Se revisa la organización de la seguridad de forma periódica por una empresa externa?	1
7. SEGURIDAD DE RECURSOS HUMANOS:	
¿Se tienen definidas responsabilidades y roles de seguridad?	3
¿Se tiene en cuenta la seguridad en la selección y baja del personal?	3
¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?	4
¿Se imparte la formación adecuada de seguridad y tratamiento de activos?	3
¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?	2
¿Se recogen los datos de los incidentes de forma detallada?	3
¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?	3
¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?	3
¿Existe un proceso disciplinario de la seguridad de la información?	1
8. GESTIÓN DE ACTIVOS:	
¿Existen un inventario de activos actualizado?	4
¿El Inventario contiene activos de datos, software, equipos y servicios?	3
¿Se dispone de una clasificación de la información según la criticidad de la misma?	2
¿Existe un responsable de los activos?	5
¿Existen procedimientos para clasificar la información?	1
¿Existen procedimientos de etiquetado de la información?	1
¿Existen procedimientos para el manejo de activos?	4
¿Se realiza gestión en medios extraíbles?	4
¿Existen procedimientos para la transferencia de medios físicos?	3
9. CONTROL DE ACCESOS:	
¿Existe una política de control de accesos?	2
¿Existe una política de uso de los servicios de red?	2
¿Existe un procedimiento formal de registro y baja de accesos?	3
¿Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario?	5
¿Existe una gestión de los privilegios de usuarios?	5
¿Existe una revisión de los derechos de acceso de los usuarios?	5
¿Existe el uso del password?	5
¿Se controla el uso de información secreta de autenticación?	5
¿Existe restricción de acceso a la información?	5
¿Se han establecido procedimientos para el inicio de sesión seguros?	5
¿Existe un control de acceso al código fuente del programa?	5
¿Existe una autenticación de usuarios en conexiones externas?	5

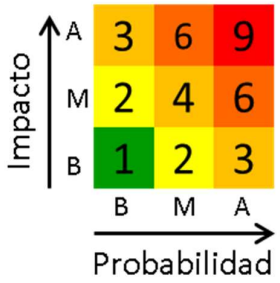
¿Existe un control de la conexión de redes?	5
¿Existen procedimientos de log-on al terminal?	3
¿Se ha incorporado medidas de seguridad a la computación móvil?	3
¿Está controlado el teletrabajo por la organización?	5
10. CRIPTOGRAFÍA:	
¿Existen políticas sobre el uso de controles criptográficos?	1
¿Se realizan procedimientos adecuados para la gestión de claves?	4
11. SEGURIDAD FÍSICA Y AMBIENTAL:	
¿Existe perímetro de seguridad física (una pared, puerta con llave)?	5
¿Existen controles físicos de entrada?	5
¿Existe un área segura cerrada, aislada y protegida de eventos naturales?	3
¿En las áreas seguras existen controles adicionales al personal propio y ajeno?	3
¿La ubicación de los equipos está de tal manera para minimizar accesos innecesarios?	4
¿Existen protecciones frente a fallos en la alimentación eléctrica?	4
¿Existe seguridad en el cableado frente a daños e intercepciones?	3
¿Se asegura la disponibilidad e integridad de todos los equipos?	4
¿Existe algún tipo de seguridad para los equipos retirados o ubicados en el exterior?	3
¿Se incluye la seguridad en equipos móviles?	3
12. SEGURIDAD DE OPERACIONES:	
¿Existen procedimientos operativos documentados?	4
¿Se realiza gestión de cambio?	3
¿Existe Gestión de capacidad?	3
¿Se han definido separación de los entornos de desarrollo, prueba y operación?	3
¿Existen controles contra malware?	4
¿Se han establecido parámetros para realizar copia de seguridad de la información?	4
¿Existe un registro de eventos?	3
¿Se realizan procedimientos para la protección de la información de registro?	3
¿Se realizan controles para la instalación de software en sistemas operativos?	3
¿Existen restricciones en la instalación de software?	5
¿Existen controles de auditoría de sistemas de información?	4
¿Existe Gestión de vulnerabilidades técnicas?	3
¿Se definen y establecen los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas?	2
¿Se supervisan las vulnerabilidades?	3
¿Se aplican parches?	4
¿Se han identificado los recursos de información que se utilizaran para vulnerabilidades?	3
¿Los recursos de información se actualizan basándose en los cambios del inventario?	3
¿Existe un cronograma para reaccionar a las notificaciones de vulnerabilidades relevantes?	2
¿Existen procedimientos para riesgos asociados y acciones a ser tomadas?	2
¿Si está disponible un parche (patch), los riesgos asociados con la instalación del parche (patch) son evaluados?	4
¿Se prueban y evalúan los parches antes de ser instalados?	3
Si no está disponible ningún parche:	

¿Existen procedimientos para bajar servicios o funcionalidades relacionadas con la vulnerabilidad?	2
¿Se adaptan o agregan controles de acceso, por ejemplo: cortafuegos (firewalfs), en los bordes de la red?	4
¿Se aumenta el seguimiento para descubrir ataques reales?	4
¿Se fomenta conciencia de la vulnerabilidad?	3
¿Existe un registro de auditoría para todos los procedimientos emprendidos?	2
¿Se supervisa y evalúa con regularidad el proceso de gestión de vulnerabilidades técnicas para asegurar su eficacia y eficiencia?	2
¿Existe una gestión de los sistemas de riesgo alto?	3
¿La vulnerabilidad técnica está alineada con las actividades de gestión de incidentes?	2
¿Existen procedimientos técnicos si ocurre un incidente?	3
¿Existen procedimientos para vulnerabilidades identificadas?	3
¿Se evalúan los riesgos relacionados con la vulnerabilidad conocida y se definen las acciones de investigación y correctivas adecuadas?	4
13. SEGURIDAD EN LAS TELECOMUNICACIONES:	
¿Todos los procedimientos operativos identificados en la política de seguridad están documentados?	1
¿Están establecidas responsabilidades para controlar los cambios en equipos?	3
¿Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?	4
¿Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas?	3
¿Existe una segregación en redes?	4
¿Existen políticas y procedimientos de transferencia de información?	1
¿Existen controles contra software maligno?	4
¿Se realizar copias de backup de la información?	4
¿Existen logs para las actividades realizadas por los operadores y administradores?	3
¿Se ha establecidos controles para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)?	2
¿Existen medidas de seguridad en el comercio electrónico?	4
¿Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada?	4
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS:	
¿Se asegura que la seguridad está implantada en los Sistemas de Información?	4
¿Existe seguridad en las aplicaciones?	5
¿Existe seguridad en los ficheros de los sistemas?	5
¿Existe seguridad en los procesos de desarrollo, testing y soporte?	4
¿Existen controles de seguridad para los resultados de los sistemas?	4
¿Existe la gestión de los cambios en los Sistemas Operativos?	4
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN:	
¿Se comunican los eventos de seguridad?	4
¿Se comunican las debilidades de seguridad?	3
¿Existe definidas las responsabilidades antes un incidente?	2
¿Existe un procedimiento formal de respuesta?	2
¿Existe la gestión de incidentes?	3

¿Existen procesos para la gestión de la continuidad?	3
¿Existe un plan de continuidad del negocio y análisis de impacto?	3
¿Existe un diseño, redacción e implantación de planes de continuidad?	2
¿Existe un marco de planificación para la continuidad del negocio?	2
¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?	1

Anexo 4: Plan de mitigación de riesgos empresa DIBEAL

VALOR	NIVEL DEL RIESGO
6 a 9	Alto
3 y 4	Medio
1 y 2	Bajo



Matriz de Riesgos	
Proyecto:	Plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL
Fecha de inicio:	
Fecha de fin:	

No. de	Fuente	Riesgo Consecuencia	Impacto (A/M/B)	Probabilidad (A/M/B)	Evaluación Valor (1 al 9)	Evaluación Nivel (A/M/B)	Respuesta
1	*El servidor web remoto se ve afectado por múltiples vulnerabilidades.*	*La versión de Apache https instalada en el host remoto es anterior a la 2.4.41. Por lo tanto, se ve afectado por múltiples vulnerabilidades como se menciona en el aviso 2.4.41, incluidas las siguientes:*	*M*	*M*	*4*	*Medio*	*Actualice a la versión 2.4.41 de Apache o posterior.*

		- Se informó un problema limitado de secuencias de comandos entre sitios que afectaba a la página de error mod_proxy. Un atacante podría provocar que el enlace de la página de error tenga un formato incorrecto y, en su lugar, apunte a una página de su elección. Esto solo sería explotable cuando un servidor estuviera configurado con el proxy habilitado, pero estuviera mal configurado de tal manera que se mostrara la página de error de proxy. (CVE-2019-10092) *- Los envíos muy tempranos de HTTP/2 (2.4.20 a 2.4.39), por ejemplo, configurados con H2PushResource, podrían provocar una sobrescritura de la memoria en el grupo de solicitudes de envío, lo que provocaría fallos. La memoria copiada es la de los valores del encabezado del enlace push configurados, no los datos proporcionados por el cliente. (CVE-2019-10081)* *- Algunas implementaciones de HTTP/2 son vulnerables al almacenamiento en búfer de datos interno sin restricciones, lo que podría provocar una denegación de servicio. El atacante abre la ventana HTTP/2 para que el par pueda enviar sin restricciones;* *sin embargo, dejan la ventana TCP cerrada para que el interlocutor no pueda escribir (muchos de) los bytes en el cable. Luego, el atacante envía un flujo de solicitudes para un objeto de respuesta grande. Dependiendo de cómo los servidores pongan en cola las respuestas, esto puede consumir exceso de memoria, CPU o ambos. (CVE-2019-9517)*					
2	*El servidor web remoto se ve afectado por una vulnerabilidad de desbordamiento del búfer.*	*La versión de Apache https instalada en el host remoto es anterior a la 2.4.52. Por lo tanto, se ve afectado por una falla relacionada con mod_lua al manejar contenido multiparte. Un cuerpo de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer en el analizador multiparte mod_lua (r:parsebody() llamado desde scripts Lua). El equipo https de Apache no tiene conocimiento de ningún exploit para esta vulnerabilidad, aunque podría ser posible crear uno.*	*A*	*A*	*9*	*Alto*	*Actualice a la versión 2.4.52 de Apache o posterior.*

3	*El servidor web remoto se ve afectado por una vulnerabilidad de denegación de servicio o falsificación de solicitudes del lado del servidor.*	*La versión de Apache https instalada en el host remoto es igual o superior a 2.4.7 y anterior a 2.4.52.* *Por lo tanto, se ve afectado por una falla relacionada con actuar como proxy directo.* *Un URI diseñado enviado a https configurado como un proxy directo (ProxyRequests activado) puede causar un bloqueo (desreferencia de puntero NULL) o, para configuraciones que combinan declaraciones de proxy directo e inverso, puede permitir que las solicitudes se dirijan a un punto final declarado de Unix Domain Socket (Falsificación de solicitudes del lado del servidor).*	*A*	*A*	7	*Alto*	*Actualice a la versión 2.4.52 de Apache o posterior.*
4	*El servidor web remoto está afectado por una vulnerabilidad.*	*La versión de Apache https instalada en el host remoto es anterior a la 2.4.49. Por lo tanto, se ve afectado por una vulnerabilidad como se menciona en el registro de cambios 2.4.49.* *- Una ruta uri de solicitud diseñada puede hacer que mod_proxy reenvíe la solicitud a un servidor de origen elegido por el usuario remoto. (CVE-2021-40438)*	*A*	*M*	4	*Medio*	*Actualice a la versión 2.4.49 de Apache o posterior.*
5	*Es posible acceder a un recurso compartido de red.*	*El host remoto tiene uno o más recursos compartidos de Windows a los que se puede acceder a través de la red con las credenciales proporcionadas.* *Dependiendo de los derechos compartidos, puede permitir que un atacante lea/escriba datos confidenciales.*	*A*	*A*	7	*Alto*	*Para restringir el acceso en Windows, abra el Explorador, haga clic derecho en cada recurso compartido, vaya a la pestaña "Compartir" y haga clic en "Permisos".*
6	*El servidor VNC remoto no requiere autenticación.*	*El servidor VNC instalado en el host remoto permite que un atacante se conecte al host remoto ya que no se requiere autenticación para acceder a este servicio.* *** El servidor VNC a veces envía al usuario conectado al inicio de sesión XDM* *** pantalla. Desafortunadamente, Nessus no puede identificar esta situación.* *** En tal caso, no es posible avanzar más sin una autorización válida.* *** Las credenciales y esta alerta pueden ignorarse.*	*A*	*A*	7	*Alto*	*Deshabilite el tipo de seguridad Sin autenticación.*

7	*El servidor web remoto se ve afectado por una vulnerabilidad de denegación de servicio.*	*Según su banner, la versión de Apache que se ejecuta en el host remoto es 2.4.x anterior a 2.4.35. Se ve, por tanto, afectado por la siguiente vulnerabilidad:* *- Al enviar tramas de CONFIGURACIÓN continuas de tamaño máximo, una conexión HTTP/2 en curso podría mantenerse ocupada y nunca expiraría. Se puede abusar de esto para un DoS en el servidor. Esto sólo afecta a un servidor que tenga habilitado el protocolo h2.*	*A*	*M*	6	*Medio*	*Actualice a la versión 2.4.35 de Apache o posterior.*
8	*No es necesario firmar en el servidor SMB remoto.*	*No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de intermediario contra el servidor SMB.*	*A*	*M*	6	*Medio*	*Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de política 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'. En Samba, la configuración se llama "firma del servidor". Consulte los enlaces 'ver también' para obtener más detalles.*
9	*El servidor SSH remoto es vulnerable a un ataque de truncamiento del prefijo mitm.*	*El servidor SSH remoto es vulnerable a una debilidad de truncamiento del prefijo de intermediario conocida como Terrapin. Esto puede permitir que un atacante remoto, intermediario, eluda las comprobaciones de integridad y degrade la seguridad de la conexión.* *Tenga en cuenta que este complemento solo busca servidores SSH remotos que admitan ChaCha20-Poly1305 o CBC con Encrypt-then-MAC y no admitan las contramedidas estrictas de intercambio de claves. No busca versiones de software vulnerables.*	*A*	*M*	6	*Medio*	*Póngase en contacto con el proveedor para obtener una actualización de las estrictas contramedidas de intercambio de claves o deshabilite los algoritmos afectados.*

10	*No se puede confiar en el certificado SSL para este servicio.*	*No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación:* *- En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.* *- En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento del análisis. Esto puede ocurrir cuando el análisis se realiza antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado.* *- En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas incorrectas se pueden solucionar haciendo que su emisor vuelva a firmar el certificado con la firma incorrecta. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utilizó un algoritmo de firma que Nessus no admite o no reconoce.* *Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques de intermediario contra el host remoto.*	*A*	*M*	6	*Medio*	*Compre o genere un certificado SSL adecuado para este servicio.*
11	*El certificado SSL del servidor remoto ya caducó.*	*Este complemento verifica las fechas de vencimiento de los certificados asociados con servicios habilitados para SSL en el destino e informa si alguno ya ha expirado.*	*A*	*M*	6	*Medio*	*Compre o genere un nuevo certificado SSL para reemplazar el existente.*

12	*La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.*	*La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque de intermediario contra el host remoto.* *Tenga en cuenta que este complemento no busca cadenas de certificados que terminen en un certificado que no esté autofirmado, pero que esté firmado por una autoridad certificadora no reconocida.*	*A*	*M*	6	*Medio*	*Compre o genere un certificado SSL adecuado para este servicio.*
13	*El servicio remoto cifra el tráfico utilizando una versión anterior de TLS.*	*El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS, como 1.2 y 1.3, están diseñadas contra estos defectos y deben usarse siempre que sea posible.* *A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales navegadores web ni con los principales proveedores.* *PCI DSS v3.2 requiere que TLS 1.0 esté completamente deshabilitado antes del 30 de junio de 2018, excepto para los terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que se puede verificar que no son susceptibles a ningún exploit conocido.*	*A*	*M*	6	*Medio*	*Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.*

14	*El servicio XDMCP se está ejecutando en el host remoto.*	*El servicio X Display Manager Control Protocol (XDMCP) permite a un usuario de Unix obtener de forma remota un inicio de sesión gráfico X11 y, por lo tanto, actuar como un usuario local en el host remoto. Si un atacante puede obtener un nombre de usuario y una contraseña válidos, este servicio podría usarse para obtener más acceso al host remoto. Un atacante también puede utilizar este servicio para montar un ataque de diccionario contra el host remoto e intentar iniciar sesión de forma remota.* *Tenga en cuenta que XDMCP es vulnerable a ataques de intermediario, lo que facilita a los atacantes robar las credenciales de usuarios legítimos haciéndose pasar por el servidor XDMCP. Además de esto, XDMCP no es un protocolo cifrado, lo que permite a un atacante capturar las pulsaciones de teclas ingresadas por el usuario.*	*M*	*M*	*6*	*Medio*	*Deshabilite el servicio XDMCP, si no lo utiliza, y no permita que este servicio se ejecute a través de Internet.*
15	*El servidor web remoto no aplica HSTS.*	*El servidor HTTPS remoto no aplica la seguridad de transporte estricta de HTTP (HSTS). HSTS es un encabezado de respuesta opcional que se puede configurar en el servidor para indicarle al navegador que solo se comunique a través de HTTPS. La falta de HSTS permite ataques de degradación, ataques de intermediarios que eliminan SSL y debilita las protecciones contra el secuestro de cookies.*	*M*	*A*	*2*	*Bajo*	*Configure el servidor web remoto para utilizar HSTS.*

16	*Es posible determinar la hora exacta establecida en el host remoto.*	*El host remoto responde a una solicitud de marca de tiempo ICMP. Esto permite a un atacante saber la fecha establecida en la máquina objetivo, lo que puede ayudar a un atacante remoto no autenticado a derrotar los protocolos de autenticación basados en el tiempo.* *Las marcas de tiempo devueltas por máquinas que ejecutan Windows Vista/7/2008/2008 R2 son deliberadamente incorrectas, pero generalmente están dentro de los 1000 segundos de la hora real del sistema.*	*B*	*B*	*2*	*Bajo*	*Filtre las solicitudes de marca de tiempo ICMP (13) y las respuestas de marca de tiempo ICMP salientes (14).*
17	*Es posible obtener el SID del host remoto.*	*Al emular la llamada a LsaQueryInformationPolicy(), fue posible obtener el SID (Identificador de seguridad) del host.* *Luego, el SID del host se puede utilizar para obtener la lista de usuarios locales.*	*B*	*B*	*2*	*Bajo*	*Puede evitar búsquedas anónimas del SID del host configurando la configuración del registro 'RestrictAnonymous' en un valor apropiado.*
18	*El recurso compartido remoto contiene archivos relacionados con Office.*	*Este complemento se conecta a los recursos compartidos SMB accesibles de forma remota e intenta encontrar archivos relacionados con Office (como .doc, .ppt, .xls, .pdf, etc.).*	*B*	*B*	*2*	*Bajo*	*Asegúrese de que los archivos que contienen información confidencial tengan controles de acceso adecuados establecidos.*

Anexo 5: Validación de la propuesta, especialista 1

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: OSCAR EDISON RAMOS GONZALEZ

Título obtenido
INGENIERO EN SISTEMAS DE LA INFORMACION
Cédula de Identidad
1710808385
E- mail
eramos@dibeal.com
Institución de Trabajo
DIBEAL CIA. LTDA.
Cargo
JEFE TI
Años de experiencia en el área
30 Años

1

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	X				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	**X**				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	**X**				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	**X**				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	**X**				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	**X**				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total						

Observaciones:

_____
_____

Recomendaciones

_____
_____

Lugar, fecha de validación: Quito, 07 de marzo del 2024

Firma del especialista

Anexo 6: Validación de la propuesta, especialista 2

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Kevin Estuardo Vera Jaramillo

Título obtenido
INGENIERO EN SISTEMAS
Cédula de Identidad
1721067369
E- mail
kverajaramillo@gmail.com
Institución de Trabajo
NETBY CONSULTING
Cargo
ESPECIALISTA NETWORKING
Años de experiencia en el área
2

1

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		*X*			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	*X*				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	*X*				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	*X*				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*		*X*			
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*		*X*			
Total		*20*	*12*			

Observaciones:

Propuesta que agrega valor con gran proyección a futuros procesos.

Recomendaciones

Guiarse en casos de éxito y aplicar buenas prácticas.

Lugar, fecha de validación: Quito, 07 de marzo del 2024

Firma del especialista