UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL TELETRABAJO EN LA EMPRESA BIOALIMENTAR

Trabajo de Graduación Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

ÁREA: Software

LÍNEA DE INVESTIGACIÓN: Sistemas Administradores de Recursos

AUTOR: Bryan Andrés Guerrón Chiluisa

TUTOR: Ing. David Omar Guevara Aulestia Mg.

Ambato - Ecuador

agosto - 2021

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL TELETRABAJO EN LA EMPRESA BIOALIMENTAR, desarrollado bajo la modalidad Proyecto de Investigación por el señor Bryan Andrés Guerrón Chiluisa, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, agosto 2021

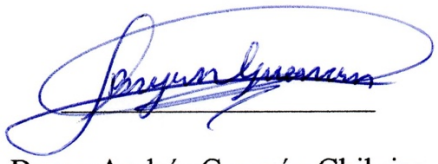
Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA

Ing. David Omar Guevara Aulestia Mg.
TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado: POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL TELETRABAJO EN LA EMPRESA BIOALIMENTAR es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2021



Bryan Andrés Guerrón Chiluisa

C.C. 1804398715

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Bryan Andrés Guerrón Chiluisa, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad de Proyecto de Investigación, titulado POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL TELETRABAJO EN LA EMPRESA BIOALIMENTAR, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, agosto 2021

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.
PRESIDENTA DEL TRIBUNAL

Firmado electrónicamente por:
FELIX OSCAR FERNANDEZ PENA

Ing. Félix Fernández, PhD
PROFESOR CALIFICADOR

Firmado electrónicamente por:
LEONARDO DAVID TORRES VALVERDE

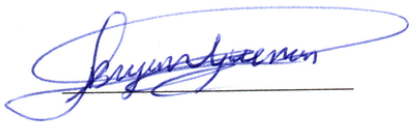
Ing. Leonardo Torres, Mg
PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, agosto 2021



Bryan Andrés Guerrón Chiluisa

C.C. 1804398715

AUTOR

DEDICATORIA

El presente trabajo está dedicado primeramente a Dios y a la Virgen que siempre me han acompañado dándome la sabiduría, la salud y la fuerza para seguir adelante día tras día.

A mi madre Alexandra que siempre me ha apoyado y ha estado conmigo en todo momento.

A mis abuelitas Piedad y Gregoria que, aunque ya no están, siempre me apoyaron y me dieron fuerza para seguir adelante y cumplir mis metas y sueños.

Finalmente, a los docentes, amigos y compañeros con los que compartí gratos momentos y de los cuales he aprendido muchas cosas.

Bryan Andrés Guerrón Chiluisa

AGRADECIMIENTOS

Gracias a Dios por darme la salud y la fuerza para continuar con lo que me he propuesto y no darme por vencido, por siempre acompañarme en cada paso que doy.

A mis padres por siempre apoyarme y mostrarme que en la vida siempre hay que luchar y no hay que dejarse vencer por las adversidades. A mis hermanos y sobrina por llenar mis días de alegría por sus palabras que me han dado fortaleza para seguir adelante.

A los docentes que cada día impartían sus conocimientos con gran esmero y dedicación con el fin de generar profesionales de calidad.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

En la actualidad debido a la pandemia causada por el COVID-19 muchas empresas se ven en la necesidad de incorporar nuevas maneras de trabajo para garantizar la continuidad del negocio y con ello no verse en la necesidad de despedir al personal o llegar a tal punto de cerrar sus puertas, como es el caso de algunas empresas en el Ecuador y en el mundo.

Gracias al avance de las tecnologías surgen nuevas maneras de garantizar la continuidad de las actividades de los empleados en las empresas, una de ellas es la realización del teletrabajo que permite la realización de las actividades de los empleados desde la comodidad de sus hogares o desde cualquier lugar.

Un problema al implementar el teletrabajo, que surgió durante la pandemia, fue la mala gestión y la apresurada implementación del teletrabajo sin tener en cuenta ciertos aspectos tales como: la infraestructura tecnológica de las empresas, equipos de trabajo sin configuraciones adecuadas y sin parches de seguridad, entre otros; que al no ser tomados en cuenta pueden significar un problema muy serio para las empresas.

Teniendo en cuenta los problemas generados a nivel de seguridad informática alrededor del mundo y en el Ecuador, por la mala implementación del teletrabajo se presenta el siguiente proyecto enfocado a la seguridad informática en el teletrabajo y las políticas que debe existir en el trabajo con el fin de garantizar una seguridad optima, así como la implementación correcta del teletrabajo en las empresas.

En el desarrollo del proyecto se realizaron diferentes evaluaciones para observar el estado actual en el que se encuentra la empresa Bioalimentar mediante el uso de herramientas como InsightVM, Zenmap, OWASP ZAP, entre otras, de igual manera se realizaron ataques de ingeniería social para poder observar cómo actúa el personal ante un ataque, y se aplicaron varias técnicas de Hacking Ético para validar las políticas desarrolladas y con ello comprobar la importante necesidad de políticas que sirvan de ayuda para una correcta implementación del teletrabajo en las empresas.

Palabras Clave: Seguridad informatica, politicas, hacking etico,ingenieria social, teletrabajo,COVID-19.

Abstract

At present due to the pandemic caused by the COVID-19 many companies are in the need to incorporate new ways of working to ensure business continuity and thus not be in the need to dismiss staff or reach the point of closing its doors, as is the case of some companies in Ecuador and in the world.

Thanks to the advance of technologies, new ways of guaranteeing the continuity of the activities of the employees in the companies arise, one of them is the telework that allows the realization of the activities of the employees from the comfort of their homes or from any place.

A problem when implementing telework, which arose during the pandemic, was the mismanagement and hasty implementation of telework without taking into account certain aspects such as: the technological infrastructure of the companies, work equipment without adequate configurations and without security patches, among others; that when not taken into account can mean a very serious problem for companies.

Taking into account the problems generated at the level of computer security around the world and in Ecuador, by the bad implementation of telework is presented the following project focused on computer security in telework and the policies that should exist in the work in order to ensure optimal security and the correct implementation of telework in companies.

In the development of the project different evaluations were made to observe the current state in which the company Bioalimentar is by using tools such as InsightVM, Zenmap, OWASP ZAP, among others, in the same way social engineering attacks were made to observe how the staff acts before an attack, and several techniques of Ethical Hacking were applied to validate the developed policies and thus verify the important need for policies that help for a correct implementation of teleworking in companies.

Keywords: Computer security, policies, ethical hacking, social engineering, teleworking, COVID-19.

INTRODUCCIÓN

El presente proyecto de investigación denominado “POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL TELETRABAJO EN LA EMPRESA BIOALIMENTAR” se encuentra dividido en los siguientes capítulos:

CAPÍTULO I. "MARCO TEÓRICO", se plantea un problema a investigar se establece la justificación y los objetivos que guiaran el desarrollo del proyecto.

CAPÍTULO II. "METODOLOGÍA", se reúne todas las técnicas y herramientas necesarias para el desarrollo del proyecto, además se define las etapas de que cubrirán el desarrollo del mismo.

CAPÍTULO III. "RESULTADOS Y DISCUSIÓN", se describe de manera precisa el desarrollo del proyecto sus características y funcionamiento haciendo énfasis en las partes fundamentales del desarrollo.

CAPÍTULO IV. "CONCLUSIONES Y RECOMENDACIONES", en esta sección se señalan las conclusiones y recomendaciones que se han encontrado a lo largo del desarrollo del proyecto.

CAPÍTULO I

MARCO TEÓRICO

1.1. Tema de investigación

POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL TELETRABAJO EN LA EMPRESA BIOALIMENTAR

1.2. Antecedentes investigativos

1.2.1. Contextualización del problema

Debido a la pandemia a causa del COVID-19, gran parte de empresas a nivel mundial se vieron afectadas, con lo que algunas tuvieron que cerrar sus puertas y otras adaptarse al medio y con ello la realización de teletrabajo, claro está solo en actividades que permitan su implementación; como apuntan varias fuentes a nivel mundial el incremento del teletrabajo ha sido significativo y de manera apresurada, además que ha sido en algunos casos improvisada y sin ningún tipo de consideración en cuanto a lo que es la ciberseguridad, lo cual ha traído consigo todo tipo de problemas en cuanto a lo que es protección de equipos, datos y garantías de privacidad entre otros [1].

El teletrabajo en diferentes países como Colombia ha significado involucrar ciertas condiciones tanto a nivel de seguridad de la información, la intimidad y los datos, al igual que otras, que necesariamente deben ser tomadas en cuenta al momento de implementar el teletrabajo, sin embargo últimamente a nivel mundial es muy difícil que se empleen de una manera adecuada debido a diferentes factores como el desconocimiento de herramientas así como la inadecuada implementación de políticas o la inexistencia de las mismas; las cuales garanticen la seguridad de las empresas al momento de la implementación de teletrabajo [2].

Con la llegada de COVID-19 los ciber atacantes han intensificado sus ataques deliberados hacia infraestructuras críticas, como es el caso de hospitales los cuales se vieron obligados a la realización de teletrabajo en ciertas áreas, pero no solo dichas infraestructuras recibieron ataques si no también empresas que por la implementación

apresurada y las inadecuadas medidas corporativas del trabajo a distancia fueron blanco de ciberataques y estafas. Los atacantes no han dudado en buscar puntos débiles en las diferentes empresas y entidades que han adoptado el teletrabajo con lo cual aumentaron su exposición, debido a multitud de aplicaciones, equipos y procedimientos de trabajo a distancia que no poseen las debidas seguridades. Otro factor a tener en cuenta es el tráfico de spam malicioso que se incrementó más del 6000% en el mes de abril de 2020 por lo que Google y Gmail se han visto en necesidad de filtrar y bloquear miles de millones de correo diarios en los cuales se trataba de suplantar la identidad de agencias, organizaciones, empresas, entre otras. Un hecho que marca Kasperky es la proliferación de ciberataques que desencadeno el teletrabajo sobre los protocolos de Microsoft para acceder al control remoto de los ordenadores de trabajo, aprovechando la confusión creada por el teletrabajo masivo con lo cual pasaron de miles por día a rozar el millón [3].

Ecuador en análisis realizados por la empresa ESET muestra diferentes ataques que han sufrido varias empresas ya sea por spam o por otro tipo de amenazas informáticas, todo esto en estudios realizados en los últimos años [4]; con ello y mediante el acuerdo ministerial en el cual afirma que "se mantendrá el teletrabajo emergente para todos los servidores cuya actividad lo permita y según las directrices de la máxima autoridad" [5], lo cual supone un riesgo para las empresas, la mala implementación del teletrabajo y políticas para la realización de la misma.

En la ciudad de Ambato, Bioalimentar una de las empresas más grandes del Ecuador con experiencia en la industria de balanceados que cuenta con aproximadamente 400 empleados en la ciudad de Ambato de los cuales 170 se encuentran en teletrabajo en distintas áreas como es el área de Compras, Comunicación, Contabilidad, Créditos y Cobranzas, Dirección Organizacional, Desarrollo Organizacional, Dirección de Marketing y Eventos, Gerencia de Procesos Comerciales, Dirección de Mercadeo, Gestión de Talento Humano, Dirección de Tecnologías de la Información, por mencionar las más importantes; con ello surge la necesidad de conocer las amenazas y vulnerabilidades que conlleva la realización apresurada del teletrabajo, con lo sucedido con la pandemia del COVID-19 donde es de suma importancia proteger la información que es manejada desde el teletrabajo, ya sea información financiera o

elaboración de nuevos productos, además de tener en cuenta los propios sistemas de la empresa y las seguridades que poseen, los servidores, el correo institucional, dispositivos IoT que pueden verse comprometidos y con ellos afectar gravemente a la empresa, mediante piratería de ordenadores, irrupción en sistemas de la empresa, captura de credenciales, ransomware y otros medios; por lo tanto, es necesario tener políticas bien definidas que sirvan de apoyo para mejorar el nivel de seguridad en la empresa que ayuden a prevenir y en caso de incidentes, así como la actuación de manera adecuada frente a incidentes; además de lograr la continuidad del negocio, todo ello mediante una documentación que sea de respaldo para las políticas planteadas como es el caso del plan de acción, el plan de contingencia y continuidad de negocio; mediante un análisis completo en la parte de sistemas de la empresa se pretende lograr políticas acordes a las necesidades de la empresa.

1.2.2. Fundamentación teórica

Políticas de seguridad informática

Las políticas de seguridad describen las actividades que son necesarias realizar, en qué momento y lugar, quienes serán los responsables de la ejecución y cuáles serán los controles que se aplicarán para supervisar la correcta ejecución. En este sentido, las políticas describen que debe protegerse [6].

Una política de seguridad define como una organización se ocupará de algún aspecto de seguridad como puede ser el caso del comportamiento del usuario final, las respuestas ante incidentes o para problemas o incidentes específicos. De igual forma se pueden crear para hacer frente a los requisitos reglamentarios [7].

Mecanismos de seguridad

Los mecanismos de seguridad son aquellos mecanismos que está diseñados para detectar, prevenir o recobrarse de un ataque de seguridad. Implementan varios servicios básicos de seguridad además de especificar como deben ser ejecutados los controles [8].

Se dividen en tres grupos [9]:

Prevención

Se centra en evitar desviaciones con respecto a las políticas de seguridad de una organización o institución. En el caso de incumplir en una de ellas se puede proceder con una sanción.

Detección

Comprende la parte de detectar las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema, vulnerabilidades, amenazas que puedan comprometer a la organización o institución.

Recuperación

Se aplica cuando se ha detectado una violación de seguridad para recuperar su normal funcionamiento dentro de la organización o institución.

Seguridad de la Información

Son medidas y controles que aseguren la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información como puede ser software, firmware, información que se procesa, se almacena y comunica entre otras que son de suma importancia o muy sensible [10].

Confidencialidad

Garantiza que la información que sea transmitida o almacenada en un sistema informático solo tendrá que ser leída por el destinatario. En caso de que el mensaje sea interceptado o llegue a otro destinatario no se podrá acceder al contenido del mensaje original. Por lo tanto, se pretende garantizar la confidencialidad de la información transmitida por las redes de comunicaciones [10].

Integridad

Se encarga de garantizar que la información no ha sido modificada desde el momento de su creación y durante la transmisión a través de la red. De este modo, es posible conocer si se ha agregado o eliminado algún tipo de información [10].

Disponibilidad

Es una cuestión de suma importancia para garantizar el cumplimiento de los objetivos, ya que es necesario el diseño de un sistema muy robusto frente ataques como para garantizar el correcto funcionamiento, de manera que pueda estar permanentemente a disposición del usuario. También se debe tener en cuenta la recuperación de los sistemas frente a fallos o incidentes de seguridad, así como desastres naturales. De igual manera no sirve de nada los demás servicios si el sistema no se encuentra disponible [10].

Pandemia

Proviene de pan que significa "todos" y demos "pueblo". La palabra se usa comúnmente para referirse a una epidemia generalizada de enfermedades contagiosas en todo el mundo, en un país, uno o más continentes, cruza fronteras internacionales y generalmente afecta a un grupo de personas, ocurre cuando surge un nuevo virus para el cual existe poca o ninguna inmunidad entre la población humana [11].

Problemas Económicos

Se define los problemas económicos como la escasez de los recursos finitos de una economía por lo que son insuficientes para satisfacer todos los deseos y necesidades humanos, por lo que es necesario la asignación de recursos o la producción de los mismos [12].

Formas de Trabajo

Las formas de trabajo se refieren a la manera en que se realizara el trabajo y el cumplimiento de actividades del contratado ya sea presencial, freelance, mediante teletrabajo entre otras [13].

Teletrabajo

Es la forma de organizar y realizar el trabajo a distancia desde cualquier sitio que se disponga, generalmente de un computador y conexión a internet, ya sea desde el domicilio del trabajador o en lugares o establecimientos ajenos al empleador [14].

Malware

Es software creado por un ciberdelincuente o hacker que es utilizado ya sea como virus informático, software espía, troyanos que se puede emplear para la interrupción o daño de computadoras, puede ser utilizado a través de un archivo adjunto de correo electrónico no solicitado o en una descarga de apariencia legitima [15,16].

Tipos de Malware

Virus

Programa de autorreplicación que se puede adherir a cualquier archivo limpio, se puede propagar por un sistema informático infectando a otros archivos con código malicioso desarrollado por atacante [17].

Troyanos

Es un tipo de malware que se hace pasar por software legítimo. Los atacantes engañan a los usuarios para que instalen troyanos en sus computadoras, donde pueden causar algunos daños al usuario así como recopilar datos sensibles del mismo [17].

Spyware

Son programas que registran en secreto lo que el usuario realiza, recopilando información que los atacantes puedan hacer uso posteriormente. Ejemplo: Un software espía que obtiene datos de las tarjetas de crédito [15].

Ransomware

Es un tipo de malware que bloquea o cifra los datos de un usuario, que viene acompañado de una amenaza de que serán borrados o no podrán acceder a los mismos hasta que se pague una cantidad de dinero [15].

Adware

Es un software publicitario utilizado para la propagación de malware en la red [18].

Botnets

Conjunto de computadoras infectadas con malware que los atacantes emplean para la realización de tareas en línea sin el permiso del usuario.

Inyección SQL

Ataque cibernético que es utilizado para robo y toma de control de base de datos. Es aprovechada debido a las vulnerabilidades que presentan ciertas aplicaciones basadas en base de datos en las cuales se inserta una declaración SQL que permita tener acceso a información confidencial [18].

Suplantación de Identidad

También conocido como phishing, se produce cuando un atacante envía información a las victimas mediante correo electrónico asegurando ser una empresa legitima que necesita información confidencial para hacerles llegar algo o a cambio de cierto producto [15].

Man in the Middle

Conocida también como ataque de hombre en el medio, es un tipo de ataque en el que un atacante intercepta la comunicación entre dos personas para poder robar la información. Ejemplo: Una red wifi insegura en la cual se puedan interceptar las comunicaciones entre dispositivos y la red [15].

Ataque de Denegación de Servicios (DoS)

Se produce cuando un atacante realiza demasiadas solicitudes a un sistema informático que termina saturando las redes y servidores con tráfico. Eso impide que la organización o empresa pueda acceder al sistema y realice sus funciones [18].

Ingeniería Social

Consiste en la manipulación psicológica de las personas para poder obtener información confidencial, de igual manera se superpone con el phishing.

Defacement

Consiste en inyectar datos maliciosos en una página web para con ello proporcionar información engañosa o vergonzosa para el propietario del sitio. Puede ser simplemente inyectar un marcador HTML en el sitio o la utilización de scripts para inyectar contenido muy elaborado [19].

1.3. Objetivos

1.3.1. General

Determinar políticas de seguridad informática que reduzcan las amenazas para la realización del teletrabajo en la empresa Bioalimentar.

1.3.2. Específicos

- Analizar el estado actual y seguridades adoptadas para el teletrabajo en la empresa Bioalimentar.
- Determinar herramientas de seguridad que ayuden a la detección de vulnerabilidades y a una mejor realización de teletrabajo.
- Definir políticas de seguridad informática para la realización de teletrabajo en la empresa Bioalimentar.
- Validar políticas mediante el uso de técnicas de Hacking Ético.

CAPÍTULO II

METODOLOGÍA

2.1. Materiales

Los materiales empleados para la recolección de información son:

- Entrevista semiestructurada
- Encuesta

La entrevista está orientada hacia las medidas y seguridades que posee la empresa para la realización de teletrabajo, realizada a un representante del departamento de TI. Consta de las siguientes preguntas:

1. ¿Cuál es la infraestructura que presenta la empresa en cuanto a seguridad informática?
2. ¿Qué características presentan los sistemas que se manejan en la empresa?
3. ¿La empresa posee políticas de seguridad?
4. ¿La empresa posee VPN propias o de terceros?
5. ¿Posee en la VPN algún log de actividad en caso de que haya un accidente informático?
6. ¿Para el teletrabajo la empresa brinda un equipo al empleado?
7. ¿Como la empresa se asegura de que no ha sido sustraída información por algún empleado?
8. ¿La empresa cuenta con un plan de contingencia y de continuidad del negocio en caso de que suceda algún incidente informático?
9. ¿Cada que tiempo se realizan copias de seguridad de la información?
10. ¿Existe algún tipo de cifrado en los equipos en caso de que se extravié algún equipo de la empresa?
11. ¿Se ha informado sobre medidas de seguridad a tener en cuenta al momento de realizar teletrabajo?

La encuesta está orientada hacia las personas que realizaron y realizan teletrabajo en la empresa Bioalimentar para conocer el estado actual de la empresa en cuanto a las seguridades informáticas. Consta de las siguientes preguntas:

1. ¿Conoce los riegos y amenazas informáticas que existen al momento de realizar teletrabajo?
    - Si
    - No
    - Tal vez
2. ¿La empresa en la que trabaja han implementado algún tipo de mecanismos de seguridad informática para la realización de teletrabajo?
    - Si
    - No
    - Tal vez
3. Para el teletrabajo emplea un equipo:
    - Propio
    - De la empresa
4. ¿El equipo que emplea para el teletrabajo es de uso exclusivo para cosas de la empresa?
    - Si
    - No
    - Tal vez
5. ¿Cuál es la velocidad de conexión que posee?
    - 0 a 15 Mbps
    - 15 Mbps a 30 Mbps
    - 30 Mbps a 45 Mbps
    - Mas de 45 Mbps
6. ¿Cuál es su proveedor de servicio de internet?
    - Tvcable
    - CNT
    - Netlife
    - Puntonet
    - Claro
    - Otro

7. ¿Los equipos empleados para la realización de teletrabajo se encuentran actualizados?
    - Si
    - No
    - Tal vez
8. Las unidades de almacenamiento como son: discos duros, pendrives, que contienen información de la empresa. ¿Cuentan con algún tipo de cifrado o algún tipo de protección en caso de pérdida de los mismos?
    - Si
    - No
    - Tal vez
9. ¿Emplea contraseñas robustas en lo dispositivos y sistemas de la empresa?
    - Si
    - No
    - Tal vez
10. ¿El equipo donde realiza teletrabajo cuenta con un antivirus actualizado y que además funcione adecuadamente?
    - Si
    - No
    - Tal vez
11. Para compartir archivos entre miembros de la empresa lo hace mediante:
    - Drive
    - Mega
    - WhatsApp
    - Mesenger
    - WeTransfer
    - Sistemas de la empresa
    - Otro

12. ¿En el caso de un incidente de seguridad informática conoce que se debe hacer y con quien debe comunicarse?
    - Si
    - No
    - Tal vez
13. ¿Cree usted que es de suma importancia tener en cuenta políticas de seguridad informática que ayuden a una mejor realización del teletrabajo reduciendo las amenazas y riesgos en la empresa?
    - Si
    - No
    - Tal vez

2.2. Métodos

2.2.1. Modalidad de la investigación

Investigación de Campo

La investigación será de campo debido a que se pretende obtener información correspondiente a las seguridades que presenta en la parte informática la empresa directamente con las personas expertas en el área.

Investigación Bibliográfica

La investigación será de carácter bibliográfico ya que se tomará como apoyo para investigación de libros, documentos científicos, tesis en el ámbito de la seguridad informática, revistas, leyes, que proporcionen información relevante que servirá de base y de fundamentación para el presente trabajo.

2.2.2. Población y muestra

En la presente investigación se trabajará con un total de 50 personas que consta de un grupo de profesionales de los diferentes departamentos de la empresa Bioalimentar que realizan teletrabajo. En la Tabla 2.1 se muestra los departamentos, así como el número de personas a ser encuestadas en cada departamento y el porcentaje que representan de la población total.

Tabla 2.1 Población de Estudio

Elaborado por: Investigador

Población	Número	Porcentaje
Departamento de Compras	3	6.00%
Departamento de Comunicación	1	2.00%
Departamento de Contabilidad	6	12.00%
Departamento de Crédito y Cobranza	2	4.00%
Departamento de Dirección Comercial	5	10.00%
Gerencia Administrativa	1	2.00%
Gerencia Comercial	1	2.00%
Departamento de Gestión de TI	4	8.00%
Logística	1	2.00%
Departamento de Mercadeo	1	2.00%
Departamento de Negocio Nutrición Humana	2	4.00%
Departamento de Nutrición Animal	4	8.00%
Departamento de Planificación de Producción	3	6.00%
Departamento de Publicidad	4	8.00%
Departamento de Seguridad Industrial	5	10.00%
Departamento de Talento Humano	5	10.00%
Tesorería	2	4.00%
Total	50	100%

2.2.3. Recolección de información

La recolección de información para la investigación se realizará mediante entrevista y encuesta. Ya que es de suma importancia la información clara y precisa se realizará la entrevista a un ingeniero en la parte de Gestión de Tecnologías de la Información de la empresa, así como la aplicación de una encuesta al personal de diferentes áreas de la empresa que realizan teletrabajo. En la Tabla 2.2 se encuentra de manera detallada como se realizará la recolección de información.

Tabla 2.2 Recolección de Información.

Elaborado por: Investigador

Peguntas Básicas	Explicación
¿Para qué?	Para lograr cumplir los objetivos de la investigación.
¿De qué personas u objetos?	Departamento de Comunicación Departamento de Contabilidad Departamento de Crédito y Cobranza Departamento de Dirección Comercial Departamento de Gestión de TI
¿Sobre qué aspectos?	Políticas de seguridad informática y el teletrabajo.
¿Quién, Quienes?	Investigador: Bryan Andrés Guerrón Chiluisa
¿Cuándo?	Las primeras 2 semanas posteriores a la aprobación del proyecto.
¿Donde?	Bioalimentar
¿Cuántas veces?	Una o dos veces hasta obtener la información correcta
¿Qué técnicas de recolección?	Encuesta Entrevista
¿Con que?	Cuestionario Guía de Entrevista
¿En qué situación?	Cuando tengan disponibilidad los entrevistados y encuestados.

2.2.4. Procesamiento y análisis de datos

Para el procesamiento y análisis de la información se aplicaron los siguientes procedimientos:

Procesamiento de Información

1. Elaboración y estructuración de cuestionario para entrevista y encuesta.
2. Realización de entrevista y encuesta a personal de la empresa.
3. Revisión de la información recogida mediante las diferentes técnicas empleadas y limpieza de información de ser el caso.
4. Clasificación de la información obtenida en base a criterios relacionados con el tema de investigación.
5. Tabulación de la información obtenida.
6. Estudio de la información obtenidos para la presentación de los resultados.
7. Presentación de la información tanto escrita como tabular o gráfica.

Análisis de Información

1. Análisis de los resultados, destacando tendencias o relaciones fundamentales que existen con los objetivos.
2. Interpretación de resultados con el apoyo de la parte del marco lógico y bibliografía adicional de ser el caso.
3. Comprobación de objetivos y verificación de datos obtenidos
4. Establecimiento de conclusiones y recomendaciones.

CAPITULO III

RESULTADOS Y DISCUSIÓN

3.1. Análisis y discusión de los resultados

Para la realización del proyecto se realizó la recolección de información mediante entrevista y encuesta, los resultados obtenidos servirán de base para determinar el estado actual de la empresa y qué aspectos tener en cuenta en la investigación.

Entrevista dirigida al Departamento de Gestión de TI

Mediante la entrevista dirigida a uno de los encargados de la gestión de la TICs, se presentan las siguientes preguntas realizadas con la respectiva respuesta.

Nombre del entrevistado: Ing. Gabriel Eduardo Santamaria Galarza

Fecha: 10/12/2020

Plataforma para la reunión: Microsoft Teams

1. **¿Cuál es la infraestructura que presenta la empresa en cuanto a seguridad informática?**

   Responde. – La empresa cuenta con dos proveedores de internet (ISP) de fibra óptica, en caso de que una falle se puede continuar trabajando; de igual manera se cuenta con Firewalls que son gestionados por terceros, además se manejan perfiles de navegación para el acceso al internet que tienen que ser activados manualmente dependiendo de la función que realice dentro de la empresa, también pueden obtener acceso a una red que no esté tan limitada; además de contar con hostpot que ayudan en la gestión de la red mediante la autenticación, de igual manera se emplea VPNs vía vigilancia y otra por lugar geográfico.

2. **¿Qué características presentan los sistemas que se manejan en la empresa?**

   Responde. – Algunos sistemas son de terceros por lo que la gestión y la seguridad es gestionada por ellos, de igual manera están gestionados para que solo se tenga acceso desde ciertos países que están gestionados con un LDAP.

3. **¿La empresa posee políticas de seguridad?**

   Responde. – No se encuentra escritas solo existen políticas de inocuidad y ad hoc que realiza la empresa, pero no están documentadas.

4. **¿La empresa posee VPN propias o de terceros?**

   Responde. – Las VPNs que posee la empresa es un hardware como servicio, en el cual se puede configurar por el personal de la empresa y la gestión es realizada por la empresa contrada.

5. **¿Posee algún tipo log de actividad la VPN en caso de que haya un accidente informático?**

   Responde. – No, lo que posee es un log de conexiones, donde guarda la información de que usuario se conectó y a qué hora además que sitio.

6. **¿Para el teletrabajo la empresa brinda un equipo al empleado?**

   Responde. – Sí, la empresa brinda un equipo que cuenta con todas las configuraciones necesarias y unido al LDAP además de contar con un antivirus empresarial.

7. **¿Como la empresa se asegura de que no ha sido sustraída información por algún empleado?**

   Responde. – La empresa tiene lo que es una carta de confidencialidad en donde se especifica las sanciones y ámbitos legales en los cuales se vería involucrado en caso de que se sustraiga información, además de tener configurados los dispositivos de entrada y salida para que no se sustraiga información.

8. **¿La empresa cuenta con un plan de contingencia y de continuidad del negocio en caso de que suceda algún incidente informático?**

   Responde. – Existen procesos y contratos que se realizarían en caso de un desastre, pero no se encuentra documentado.

9. **¿Se realiza algún tipo de copias de seguridad de la información?**

   Responde. – No existe copia de hardware lo que se maneja es una política ad hoc de que se emplee Office 365 para el manejo de información.

10. **¿Existe algún tipo de cifrado en los equipos en caso de que se extravié algún equipo de la empresa?**

    Responde. – No, solo las de Windows 10 y se emplea Office 365 con un tera de almacenamiento para que los empleados guarden y gestión en esa plataforma la información.

11. **¿Se ha informado sobre medidas de seguridad a tener en cuenta al momento de realizar teletrabajo?**

    Responde. – Si al momento del ingreso se les da una inducción sobre las medidas de seguridad y tips de sentido común, como que no respondan correo de personas que no conocen, entre otras cosas que deben tener en cuenta, y en ciertos momentos mediante el chat corporativo cosas como no compartir tus credenciales ni datos bancarios, pero no una actualización de los conocimientos que se les da cuando ingresan.

12. **¿Se ha impartido charlas o cursos de las configuraciones que deben tener los routers de las personas que realizan teletrabajo?**

    Responde. – No en la parte de domicilio no se ha realizado.

Encuesta realizada a los empleados que realizan teletrabajo en la empresa

La encuesta consta de preguntas en el ámbito de la seguridad informática que son necesarias para tener en cuenta ciertos aspectos en la investigación, la aplicación de la encuesta va dirigida a 50 profesionales que pertenecen a la empresa Bioalimentar y que se encuentran realizando teletrabajo.

Fecha: 07/01/2020

1. **¿Conoce los riegos y amenazas informáticas que existen al momento de realizar teletrabajo?**

Figura 3.1: Pregunta: ¿Conoce los riegos y amenazas informáticas que existen al momento de realizar teletrabajo?

Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.1 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 18 empleados (36%) indicaron que si conocen los riesgos y amenazas que existen en la realización del teletrabajo, 24 empleados (48%) indicaron que no conocen, mientras que 8 empleados (16%) indicaron que tal vez. De los resultados obtenidos se puede evidenciar que una gran parte de empleados que corresponde al 48%, no tiene conocimientos de las amenazas y riesgos informáticos que existen en el teletrabajo.

2. **¿La empresa en la que trabaja han implementado algún tipo de mecanismos de seguridad informática para la realización de teletrabajo?**

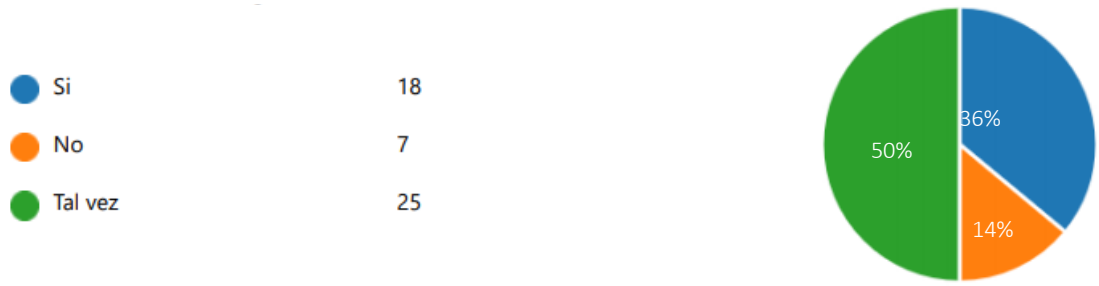


Figura 3.2: Pregunta: ¿La empresa en la que trabaja han implementado algún tipo de mecanismos de seguridad informática para la realización de teletrabajo?
Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.2 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 18 empleados (36%) indicaron si, que la empresa ha implementado algún tipo de mecanismo de seguridad informática para la realización de teletrabajo, 7 empleados (14%) indicaron no, mientras que 25 empelados (50%) indicaron que tal vez. De los resultados obtenidos se puede evidenciar que la mitad de los empleados encuestados que corresponde al 50%, no conocen si se ha implementado o no mecanismo de seguridad informática en el ámbito del teletrabajo.

3. **Para el teletrabajo emplea un equipo:**

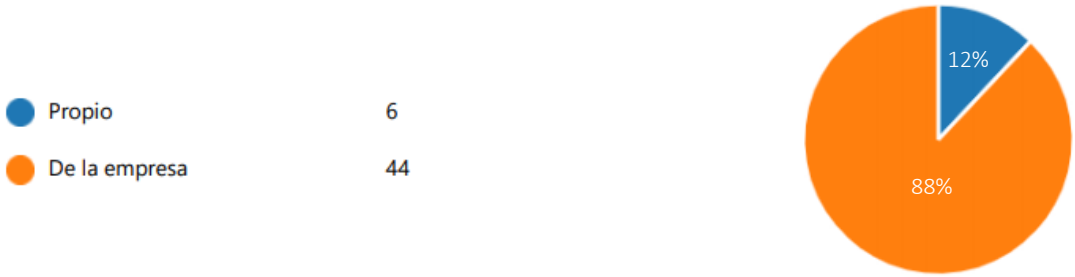


Figura 3.3: Pregunta: Para el teletrabajo emplea un equipo: Propio o de la Empresa.
Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.3 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 44 empleados (88%) indicaron que emplean un equipo de la empresa para la realización de teletrabajo, mientras que 6 empleados (12%) indicaron que emplean un equipo propio. De los resultados obtenidos se puede evidenciar que 44 empleados que corresponde al 88%, emplean un equipo de la empresa para la realización de teletrabajo, con lo cual la empresa puede tener un mejor control sobre los empleados y lograr una mejor seguridad en la empresa.

4. **¿El equipo que emplea para el teletrabajo es de uso exclusivo para cosas de la empresa?**

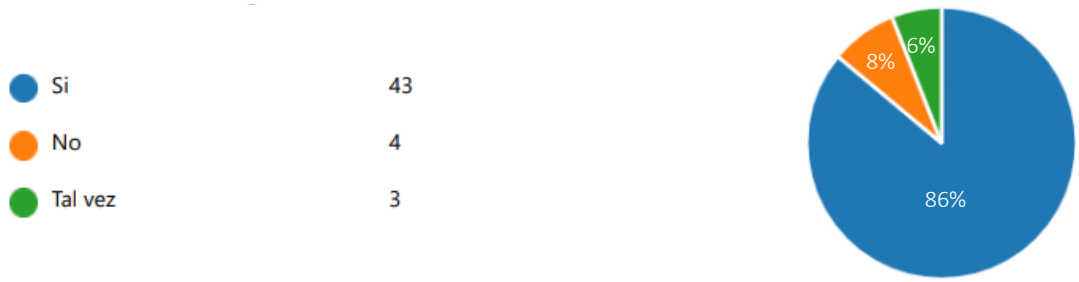


Figura 3.4: Pregunta: ¿El equipo que emplea para el teletrabajo es de uso exclusivo para cosas de la empresa?
Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.4 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 43 empleados (86%) indicaron que su equipo es de uso exclusivo para actividades de la empresa, 4 empleados (8%) indicaron que no es de uso exclusivo para

actividades de la empresa, mientras que 3 empleados (6%) indicaron que tal vez emplean el equipo tanto para actividades empresariales como para otras. De los resultados obtenidos se puede evidenciar que 43 empleados que corresponde al 86%, dan uso exclusivo de los equipos a actividades de la empresa, un aspecto positivo que aumenta la seguridad de la empresa y que debe extenderse hacia todo el personal que realiza teletrabajo dentro de la empresa.

5. ¿Cuál es la velocidad de conexión que posee?

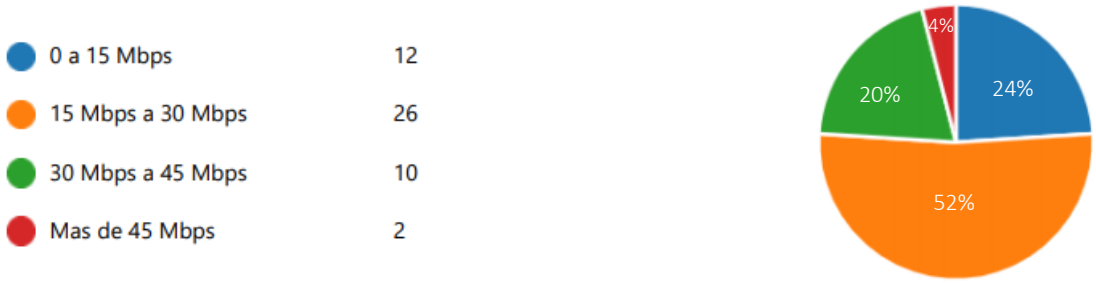


Figura 3.5: Pregunta: ¿Cuál es la velocidad de conexión que posee?
Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.5 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 12 empleados (24%) indicaron que poseen una conexión entre 0 a 15 Mbps, 26 empleados (52%) indicaron que poseen una conexión entre 15 Mbps a 30 Mbps, 10 empleados (20%) indicaron que poseen una conexión entre 30 Mbps a 45 Mbps, mientras que 2 empleados (4%) indicaron que poseen una conexión de más de 45 Mbps. De los resultados obtenidos se puede evidenciar que 26 empleados que corresponde al 52%, poseen una conexión de 15 Mbps a 30 Mbps, que no puede ser muy buena para la realización de teletrabajo si se comparte con otros miembros dentro del domicilio.

6. ¿Cuál es su proveedor de servicio de internet?

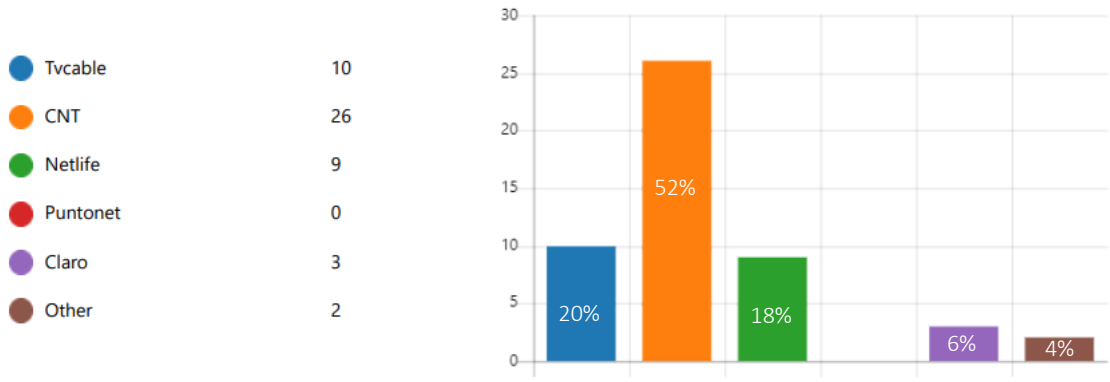


Figura 3.6: Pregunta: ¿Cuál es su proveedor de servicio de internet?

Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.6 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 10 empleados (20%) indicaron que su proveedor de servicio de Internet es Tvcable, 26 empleados (52%) indicaron que su proveedor de servicio de Internet es CNT, 9 empleados (18%) indicaron que su proveedor de servicio de Internet es Netlife, 3 empleados (6%) indicaron que su proveedor de servicio de Internet es Claro, mientras que 2 empleados (4%) indicaron que poseen otro proveedor de Internet. De los resultados obtenidos se puede evidenciar que 26 empleados que corresponde al 52%, el proveedor de servicio de Internet es CNT; es de suma importancia para la realización correcta de las actividades en el teletrabajo contar con un proveedor de Internet que no tenga antecedentes de problemas de conectividad y de seguridad que pueden ser un problema en la seguridad de la empresa.

7. **¿Los equipos empleados para la realización de teletrabajo se encuentran actualizados?**

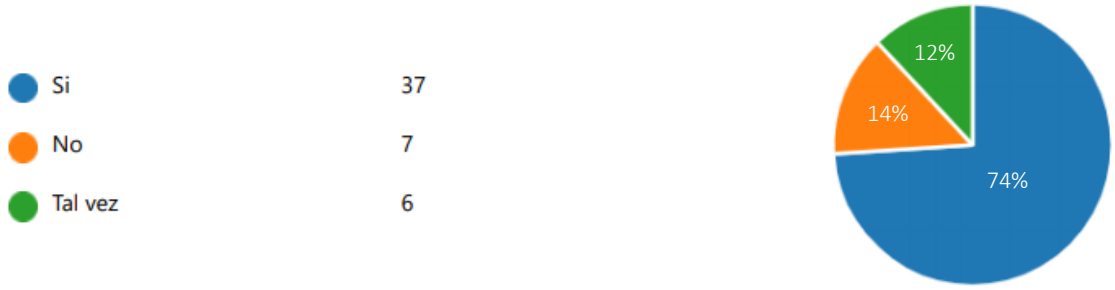


Figura 3.7: Pregunta: ¿Los equipos empleados para la realización de teletrabajo se encuentran actualizados?
Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.7 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 37 empleados (74%) indicaron que los equipos empleados para el teletrabajo se encuentran actualizados, 7 empleados (14%) indicaron no se encuentran actualizados, mientras que 6 empleados (12%) indicaron que tal vez se encuentren actualizados. De los resultados obtenidos se puede evidenciar que 37 empleados que corresponde al 74%, los equipos empleados para la realización de teletrabajo se encuentran actualizados, con lo cual se podría evitar ciertos ataques que hagan uso de vulnerabilidades de software no actualizado, pero se podría ver comprometida la seguridad de la empresa por el resto del personal que no posee actualizado sus equipos.

8. **Las unidades de almacenamiento como son: discos duros, pendrives, que contienen información de la empresa. ¿Cuentan con algún tipo de cifrado o algún tipo de protección en caso de pérdida de los mismos?**

Figura 3.8: Pregunta: Las unidades de almacenamiento como son: discos duros, pendrives, que contienen información de la empresa. ¿Cuentan con algún tipo de cifrado o algún tipo de protección en caso de pérdida de los mismos?
Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.8 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 16 empleados (32%) indicaron que las unidades de almacenamiento que poseen si cuentan con algún tipo protección en caso de perdida, 22 empleados (44%) indicaron no cuentan con ningún tipo de protección, mientras que 12 empleados (24%) indicaron que tal vez cuentan con algún tipo de protección. De los resultados obtenidos se puede evidenciar que 22 empleados que corresponde al 44%, cuentan con algún tipo de protección en las unidades de almacenamiento en caso de pérdida de los mismos, lo cual es una buena práctica de seguridad, pero el resto del personal en caso de que se extravié una unidad de almacenamiento podría comprometer la seguridad de la empresa al extraviar información de alto valor.

9. ¿Emplea contraseñas robustas en los dispositivos y sistemas de la empresa?

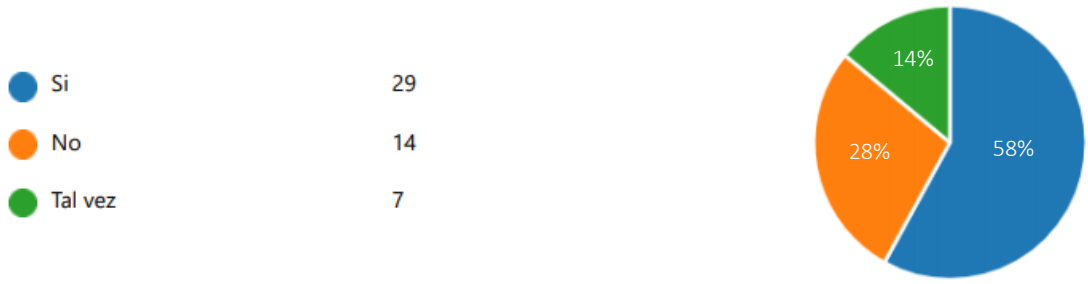


Figura 3.9: Pregunta: ¿Emplea contraseñas robustas en los dispositivos y sistemas de la empresa?

Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.9 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 29 empleados (58%) indicaron que emplean contraseñas robustas en los diferentes sistemas y dispositivos de la empresa, 14 empleados (28%) indicaron no emplean una contraseña robusta, mientras que 7 empleados (14%) indicaron que tal vez emplean contraseñas robustas. De los resultados obtenidos se puede evidenciar que 29 empleados que corresponde al 58%, emplean contraseñas robustas tanto en los sistemas como en los dispositivos de la empresa, un aspecto positivo a tener en cuenta, pero un problema es la gestión de las contraseñas y otro es que el resto del personal no emplee contraseñas robustas, así como el desconocimiento del resto del personal sobre lo que es considerado como una contraseña robusta que cumpla con los estándares de seguridad.

10. ¿El equipo donde realiza teletrabajo cuenta con un antivirus actualizado y que además funcione adecuadamente?

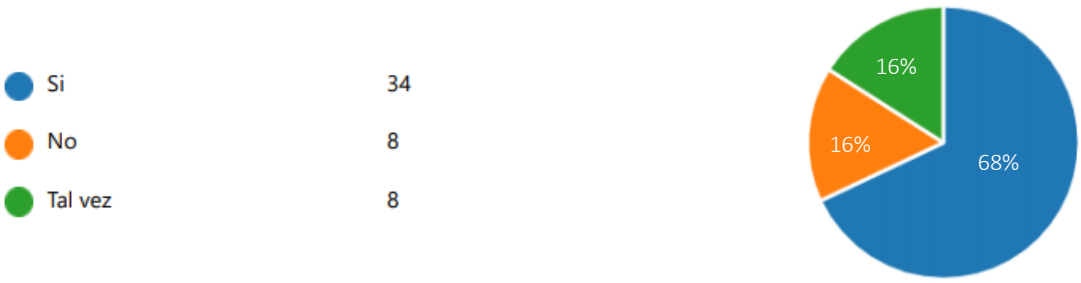


Figura 3.10: Pregunta: ¿El equipo donde realiza teletrabajo cuenta con un antivirus actualizado y que además funcione adecuadamente?
Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.10 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 34 empleados (68%) indicaron que cuentan con un antivirus actualizado y además que funciona adecuadamente, 8 empleados (16%) indicaron que no cuentan con un antivirus actualizado y además que funcione adecuadamente, mientras que 8 empleados (16%) indicaron que tal vez. De los resultados obtenidos se puede evidenciar que 34 empleados que corresponde al 68%, cuentan con un antivirus que se encuentra actualizado y que además funciona adecuadamente; un aspecto de seguridad muy importante, pero el resto del personal entrevistado afirma que no cuenta con un antivirus actualizado o desconoce del estado actual de su antivirus, lo cual puede significar un problema muy grave en cuanto a la seguridad ya que puede significar que en algún momento se encontró o se encuentra infectado el equipo donde se realiza teletrabajo y podría estarse filtrando información de la empresa.

11. Para compartir archivos entre miembros de la empresa lo hace mediante:

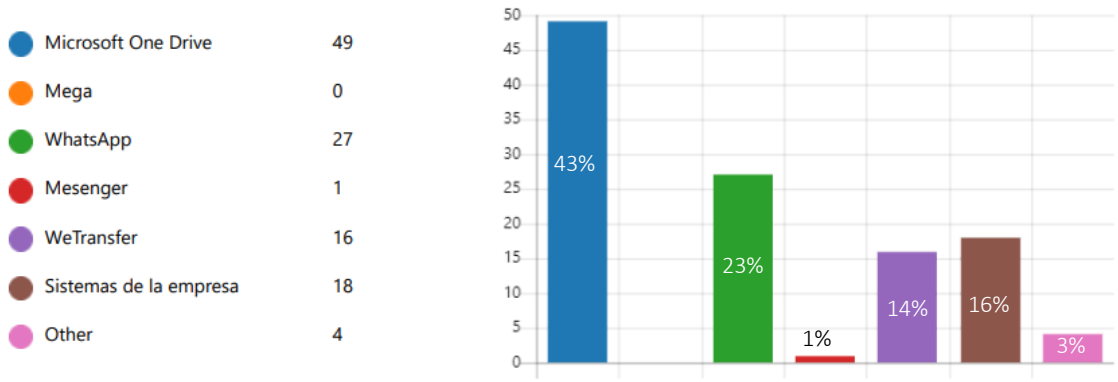


Figura 3.11: Pregunta: Para compartir archivos entre miembros de la empresa lo hace mediante.

Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.11 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, el 43% de los empleados indicaron que comparten archivos mediante la cuenta empresarial de Microsoft One Drive, el 23% de los empleados indicaron que de igual manera comparten archivos mediante WhatsApp, el 1% de los empleados indicaron que comparten archivos mediante Messenger, el 14% de los empleados indicaron que de igual manera emplean WeTransfer para compartir archivos, el 16% de los empleados emplean Sistemas de la empresa para compartir archivos, mientras que 4% empleados indicaron que lo realizan por otros medios. De los resultados obtenidos se puede evidenciar que los principales medios para compartir información son: Microsoft One Drive, WhatsApp, Sistemas de la empresa, WeTransfer, en ese orden; lo cual es muy importante tener en cuenta al momento de compartir por medios que no sean parte de la empresa como WhatsApp o WeTransfer, ya que puede significar un riesgo en la seguridad de la empresa.

12. ¿En el caso de un incidente de seguridad informática conoce que se debe hacer y con quien debe comunicarse?

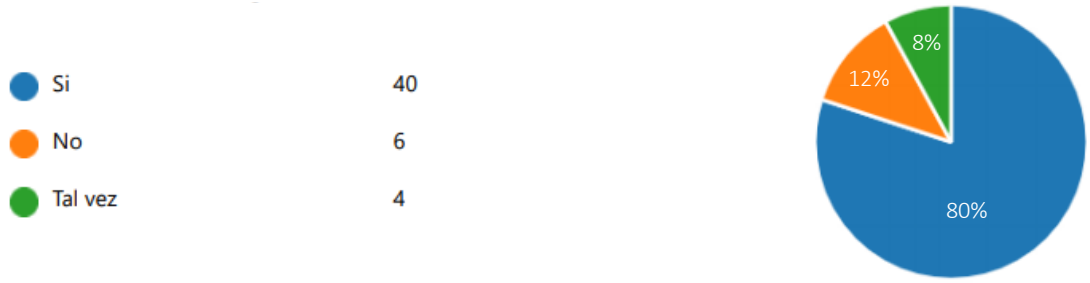


Figura 3.12: ¿En el caso de un incidente de seguridad informática conoce que se debe hacer y con quien debe comunicarse?

Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.12 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 40 empleados (80%) indicaron que conocen que deben hacer ante un incidente de seguridad informático y a quien deben informar, 6 empleados (12%) indicaron que no conocen que se debe hacer ante un incidente de seguridad informático y a quien se debe informar, mientras que 4 empleados (8%) indicaron que tal vez. De los resultados obtenidos se puede evidenciar que 40 empleados que corresponde al 80%, conocen que se debe realizar si sucede un incidente de seguridad informática y a quien deben comunicarlo, pero un porcentaje mínimo de empleados no conocen que se debe realizar ni a quien deben comunicar, por lo que es de suma importancia educar al personal ante posibles incidentes.

13. **¿Cree usted que es de suma importancia tener en cuenta políticas de seguridad informática que ayuden a una mejor realización del teletrabajo reduciendo las amenazas y riesgos en la empresa?**

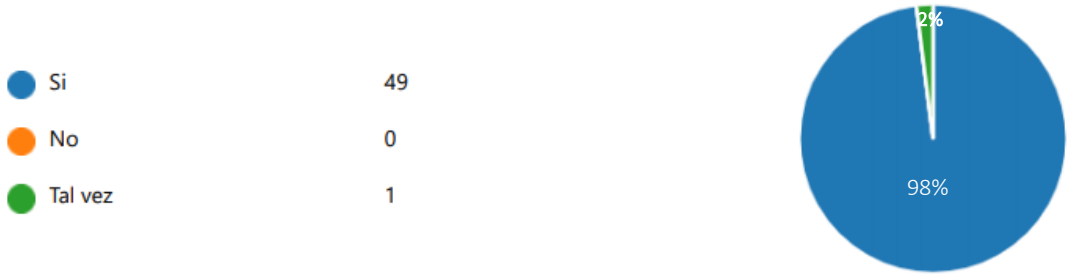


Figura 3.13: ¿Cree usted que es de suma importancia tener en cuenta políticas de seguridad informática que ayuden a una mejor realización del teletrabajo reduciendo las amenazas y riesgos en la empresa?
Elaborado por: Investigador

Análisis e Interpretación: En la Figura 3.13 se puede observar que de 50 empleados que realizan teletrabajo en la empresa que fueron encuestados, 49 empleados (98%) indicaron que es de suma importancia políticas de seguridad informática que ayuden a la realización de teletrabajo, mientras que 1 empleado (2%) indico que tal vez sea importante. De los resultados obtenidos se puede evidenciar que 49 empleados que corresponde al 98%, que son casi en su totalidad de los encuestados están de acuerdo en que es de suma importancia contar con políticas de seguridad informática que ayuden a una mejor seguridad para la empresa mientras se realiza teletrabajo.

Análisis Total

Mediante los datos obtenidos en la encuesta se puede observar un gran déficit de conocimientos de las amenazas informáticas que existen en el teletrabajo, además de que el personal no se encuentra al tanto de procedimientos y mecanismo que realiza la empresa en cuanto a las seguridades informáticas. De igual manera se observa ciertos inconvenientes que pueden afectar a la empresa como es el caso de no encontrarse cifradas las unidades de almacenamiento empleadas en el trabajo,

así como cierto porcentaje del personal que no emplea contraseñas robustas en los dispositivos y sistemas de la empresa, de igual manera el envío de archivos mediante herramientas que no se consideran totalmente seguras, además de que al emplear estas herramientas la información puede verse comprometida. Por ende, es necesario tener en cuenta ciertos aspectos de seguridad informática que deben ser contenidos en la realización de las políticas de seguridad, para con ello lograr que el personal tenga una guía y pueda realizar sus actividades de manera adecuada.

3.1.1. Desarrollo de la propuesta

Antes de establecer las políticas es necesario aclarar ciertos aspectos en cuanto a la teoría que servirán para la mejor comprensión y para la adecuada realización de las políticas de seguridad informática que estén acorde a las necesidades de la empresa.

3.1.1.1. Seguridad de la Información

Todo tipo de entidades, empresas, organismos, etc., en su realización de actividades generan información que puede ser muy valiosa o no dependiendo del rol que desempeñe en la empresa, dicho de ese modo se puede generar diferente información como: clientes, datos de contacto, pedidos, proveedores, facturas, proyectos, listados de ventas, desarrollo y actualización de productos, etc. Por ende, la información es crucial ya que una perdida supondría graves problemas para la continuidad de la empresa.

La seguridad de la información comprende la protección en cuanto a la integridad, disponibilidad y confidencialidad según los objetivos planteados de la empresa en cuanto al nivel requerido para la empresa [20].

3.1.1.2. Amenaza

Una amenaza comprende cualquier evento que puede comprometer los activos de información de una empresa, organización, etc., que pueden afectar gravemente la integridad, disponibilidad y confidencialidad [20].

Se clasifican en:

- **Intencionadas:** Intento organizado o no para producir daños.
- **No Intencionadas:** Incidente que no estaba planificado que suceda y puede generar daños
    - **Humanos:** Error cometido en un tarea u operación, descuidos, etc.
    - **Técnicos:** Fallos a nivel de Hardware o Software, sobrecarga del sistema, etc.
- **Desastres**
    - **Naturales:** Terremotos, tsunami, huracán, etc.
    - **Intencionales:** Robos, incendios, etc.
    - **Accidentales:** Incendios no intencionados, etc.

3.1.1.3. Vulnerabilidad

Una vulnerabilidad se considera cualquier debilidad como puede ser un activo o sistema informático que puede producir daños y con ello producir perdidas en la empresa u organización [21].

Algunas vulnerabilidades pueden ser:

- Equipos sin la presencia de un antivirus.
- Entradas de las instalaciones sin ningún tipo de protección.
- Lugares no adecuados de los servidores.
- Falta de suministro eléctrico.

Es importante tener en cuenta que una vulnerabilidad por sí sola no produce daños, si no es una condicionante para que una amenaza afecte a los activos.

3.1.1.4. Riesgo

Un riesgo comprende la probabilidad de que se materialice una amenaza sobre una vulnerabilidad para con ello causar un determinado impacto dentro de una empresa u organización [21].

3.1.1.5. Sistema de Gestión de la Seguridad de la Información (SGSI)

Un SGSI permite a las empresas u organizaciones implementar estratégicamente políticas, procedimientos, así como controles de seguridad informática que se encuentren alineados con los objetivos de cada empresa, con el fin de evaluar los riesgos e implementar acciones para mitigarlos, con ello aumentar la calidad del servicio y competitividad de la empresa.

SGSI es una estructura organizativa, técnica y procedimental en la cual se busca la seguridad de la información mediante:

- Análisis de situación actual y planificación.
- Aplicación de diversos controles
- Revisión de su funcionamiento
- Aplicaciones de correcciones y mejoras.

Comprende un ciclo sin fin (PHVA) o (PDCA) por sus siglas en ingles Plan, Do, Act, Check, que se muestra en la Figura 3.14, con cada iteración nueva se perfecciona el sistema y por ende se obtiene una mejor gestión de la seguridad.

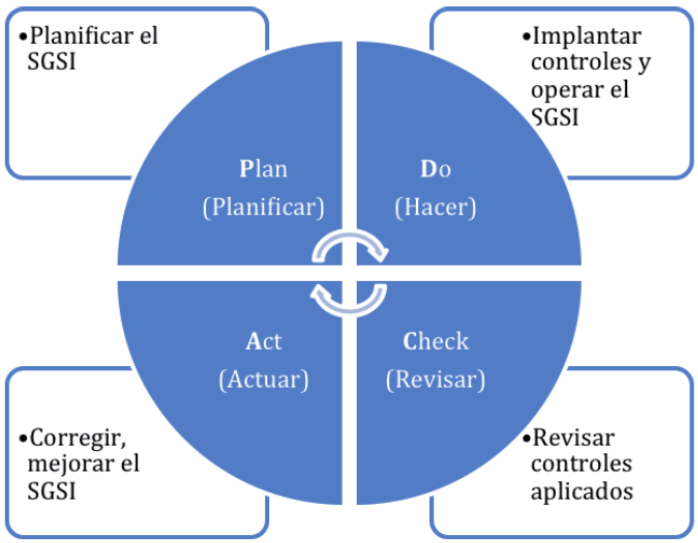


Figura 3.14: Modelo de ciclo (PDAC).

Fuente: Protección de datos y seguridad de la información [21].

3.1.1.5.1. Planificación del SGSI

En un SGSI la planificación es la parte más importante donde se recogen las siguientes tareas [22]:

1. Definición de los Objetivos, Propósito y el Alcance.
2. Valoración de los Riesgos.
   2.1.Valoración de los Activos
   2.2.Identificación de Amenazas
      - Intencionadas
      - No Intencionadas
         - Humanos
         - Técnicos
      - Desastres
         - Naturales
         - Intencionados
         - Accidentales
   2.3.Valoración de las Vulnerabilidades
   2.4.Valoración de Riesgos
      - Riesgos Asumibles
      - Riesgos no Aceptables
      - Riesgo Critico
3. Tratamiento de los Riesgos
   3.1.Asumir el Riesgo
   3.2.Evitar el Riesgo
   3.3.Transferir el Riesgo
   3.4.Reducir el Riesgo
4. Identificación y Selección de Controles
   4.1.Disminuir la Probabilidad
   4.2.Reducir el Impacto

3.1.1.5.2. Implantar los Controles del SGSI (Hacer)

La parte de la implantación llega una vez se ha identificado y se tiene claro los riesgos, así como el análisis de impacto en el negocio y los diferentes controles que se deben implantar [22].

3.1.1.5.3. Revisar los Controles del SGSI

La siguiente etapa en un SGSI es revisar la eficiencia de los controles implantados y revisar si cumple con los objetivos marcados por el SGSI; para le revisión es necesario realizar periódicamente auditorías internas que permitan dictaminar sobre la adecuación de las medidas y controles en cuanto a la seguridad, así como la identificación de deficiencias que permitan tomar medidas correctoras o complementarias [23].

3.1.1.5.4. Mejorar el SGSI (Actuar)

En la etapa de actuación, una vez detectadas las deficiencias en los controles y en la operatividad del SGSI, es necesario la identificación e implantación de acciones correctivas y preventivas para la mejora en el rendimiento de un SGSI [23].

El proceso comprende:

- Identificación de nuevos controles.
- Modificación de controles actuales para mejorar la eficiencia.
- Modificación de los objetivos de seguridad y los controles asociados.
- Eliminación de controles obsoletos.
- Comunicación de los cambios efectuados.
- Modificación en el diseño del SGSI

3.1.1.6. Política de Seguridad

Las políticas de seguridad delinean lo que la organización espera que sea cumplido por sus colaboradores y las consecuencias que derivan al no ser cumplidas.

Las políticas de seguridad constituyen la piedra angular para una correcta implantación de seguridad. Pueden comprender todos los recursos de la organización como: software, hardware, personal, comunicaciones, redes, accesos, contratación de personal, etc.; debiendo así contemplar las áreas más importantes de la organización [24].

Una política de seguridad debería cumplir con [25]:

- Definir la información como un activo de la empresa.
- Subrayar la importancia de la información como activo.
- Establecer las reglas de comportamiento en el manejo del activo de información.
- Describir cómo denunciar una presunta infracción de las políticas;
- Articular las consecuencias de las violaciones de políticas;
- Autorizar la investigación de violaciones de políticas.

3.1.1.7. Política Organizacional

La política organizacional o institucional detalla el propósito, propiedad, roles y responsabilidades y documentación o políticas relacionadas. La política de la organización es a menudo la declaración de políticas de más alto nivel de la que todas las demás políticas, estándares, directrices o procedimientos obtienen su legitimidad. Debe ser obligatoria y reflejar los requisitos de la administración para el comportamiento organizacional. Se recomienda que no esté ligado a un lenguaje sobre una tecnología especifica o un producto de un proveedor, sino ser independiente de cómo se cumple el objetivo de la política [25].

3.1.1.8. Estándares

Un estándar describe la implementación y gestión de controles de seguridad de la información. Un estándar proporciona un control de seguridad de la información para poder llegar a cumplir con las especificaciones requeridas, incluidas aquellas que son para cumplir con industrias especificas u objetivos de cumplimiento normativo [26].
Existen varios estándares muy utilizados como:

- Los Objetivos de Control para la Tecnología de la Información y Afines (COBIT). COBIT es un marco desarrollado por la Asociación de Control y Auditoría de Sistemas de Información (ISACA), una organización independiente de profesionales de gobierno de TI. COBIT se centraba originalmente en reducir los riesgos técnicos en las organizaciones, pero con

la evolución de cada versión sucesiva ha incorporado la alineación de TI con los objetivos estratégicos del negocio. Es el marco más utilizado para lograr el cumplimiento de las reglas SOX.

- Organización Internacional de Normalización (ISO) 27000 Gestión de la seguridad de la información. La serie ISO 27000: 2013 proporciona un marco de seguridad de la información muy sólido para cualquier industria. Enraizado en el estándar 17799 del British Standards Institution (BSI) anterior, a menudo se lo conoce como la versión de seguridad de la información del estándar de calidad ISO 9000. ISO 27000 se descompone además en varios subestándares basados en el contenido. Por ejemplo, ISO 27000 proporciona una descripción de la norma, ISO 27001 define los requisitos del programa e ISO 27002 define los requisitos del programa de seguridad de la información operativa.
- La publicación especial 800 del Instituto Nacional de Estándares y Tecnología (NIST). La serie NIST SP 800 proporciona orientación general y específica sobre casi todos los aspectos de la seguridad de la información. NIST SP 800-53 es un marco modelo que las agencias gubernamentales y los proveedores de los EE. UU. Utilizan para cumplir con los requisitos federales. Aunque es específico para agencias gubernamentales, el marco NIST podría aplicarse en cualquier otra industria y las empresas que buscan crear un programa de seguridad de la información no deben pasarlo por alto.

3.1.1.9. Procedimientos

Los procedimientos comprenden la implementación real del estándar. Brindan orientación sobre cómo, específicamente, los estándares se logran a un nivel muy granular. Esto se puede lograr con instrucciones paso a paso sobre lo que se debe hacer. Puede comprender varios procedimientos para cada estándar, ya que puede haber varias organizaciones involucradas en la implementación del estándar. Con una orientación de alto nivel como es en una política, es probable que no sea necesario realizar cambios con mucha frecuencia. Las políticas se revisan con regularidad, pero la escala de tiempo para cuando las políticas cambian se mide en años, si las políticas están bien consideradas y redactadas. Sin embargo, es posible que sea necesario actualizar los estándares con mayor regularidad. Los cambios en los activos de

información dan lugar a la actualización de los estándares. Cualquier cambio en la tecnología dentro de la organización puede resultar en una actualización de los estándares. Es probable que los procedimientos cambien con más regularidad. A medida que las organizaciones de la empresa cambian o cambian las responsabilidades, los procedimientos cambian para adaptarse a ellas [27].

3.1.1.10. Directrices

Las directrices consisten en recomendaciones que pueden respaldar una política o estándar. Las directrices están relacionadas con las mejores prácticas de seguridad de la información que respaldan una política o estándar. Las directrices de apoyo pueden ser una lista de información importante que respaldaría el informe (es decir, cuándo ocurrió, quién estuvo involucrado, computadoras afectadas). Un ejemplo, el estándar puede dictar el uso de encriptación para información sensible. La guía complementaria puede ser qué tipo de información se debe cifrar [28].

3.1.1.11. Listas de Verificación

La lista de verificación es empleada para validar o confirmar ciertas condiciones o configuraciones asociadas con la política o estándar de seguridad. La lista de verificación es utilizada, a menudo por el personal de seguridad o de TI, para validar que una condición o configuración se haya implementado correctamente. Un segundo ejemplo es el uso de listas de verificación durante las inspecciones o evaluaciones. El auditor usará la lista de verificación para anotar la conformidad o no conformidad con una política o lista de verificación específica [25].

3.1.1.12. Proceso de Desarrollo de Políticas

Existen dos formas para el desarrollo de políticas. En ciertas organizaciones, el desarrollo de políticas se inicia por la parte superior de la organización. El enfoque conocido como desarrollo de políticas de arriba hacia abajo, significa que las políticas pasan de la alta dirección a los niveles inferiores de la organización. Existe una ventaja en el desarrollo de políticas de arriba hacia abajo en la cual se garantiza que las políticas están alineadas con la estrategia y la visión de la alta dirección. Una desventaja es el proceso en la gran cantidad considerable de tiempo para la

implementación y posiblemente no aborde por completo las preocupaciones operativas de los empleados promedio.

Un enfoque diferente comprendería el desarrollo de políticas de abajo hacia arriba. El enfoque de abajo hacia arriba en el desarrollo de políticas aborda las preocupaciones de los empleados promedio. El proceso de abajo hacia arriba inicia con los comentarios y preocupaciones de los empleados promedio y se basa en los riesgos conocidos que los empleados y gerentes de grupos organizaciones han identificado; sin embargo, existe una gran desventaja en el proceso que no siempre se adapta bien a la estrategia de la alta dirección.

Independientemente de cómo se desarrolle una política de seguridad debe contener algunos componentes específicos, como se muestra en la Figura 3.15 [29].

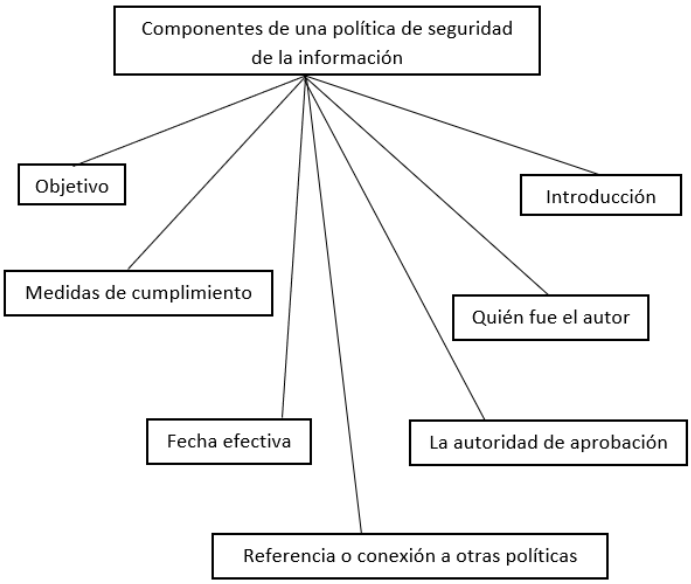


Figura 3.15: Componentes de una buena política de seguridad de la información.
Fuente: CASP CompTIA Advanced Security Practitioner [29].

Algunos tipos específicos de políticas son [29]:

Regulatoria: Garantizan que los estándares de la organización estén de acuerdo con las leyes locales, estatales y federales. Las industrias que hacen uso frecuente de estos documentos incluyen la atención médica, servicios públicos, refinamiento, educación y las agencias federales.

Informativa: Como su nombre lo indica son informativas, se crean para enseñar o ayudar a los empleados y otras personas a comprender reglas específicas. El objetivo es informar a los empleados o clientes.

Asesoramiento: Esta diseñada para garantizar que todos los empleados conozcan las consecuencias de determinados comportamientos y acciones. Un ejemplo puede ser una política de asesoramiento la cual es una política de uso aceptable (AUP). Esta política puede indicar como los empleados pueden utilizar Internet y pude impedir que los empleados visiten redes sociales o sitios pornográficos. La política podría indicar que los empleados que violen la política podrían enfrentar medidas disciplinarias o incluso el despido.

En la Figura 3.16 así como en la Figura 3.17 se puede observar la estructura de las políticas y los subdocumentos que posee, así como la jerarquía de los documentos y el orden en la cual se recomienda su realización.

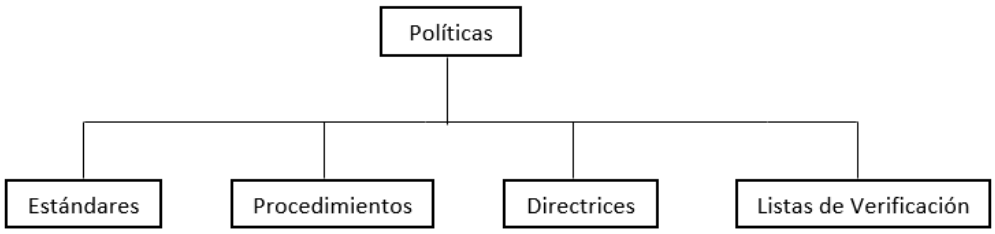


Figura 3.16: Estructura de políticas y subdocumentos.
Elaborado por: Investigador

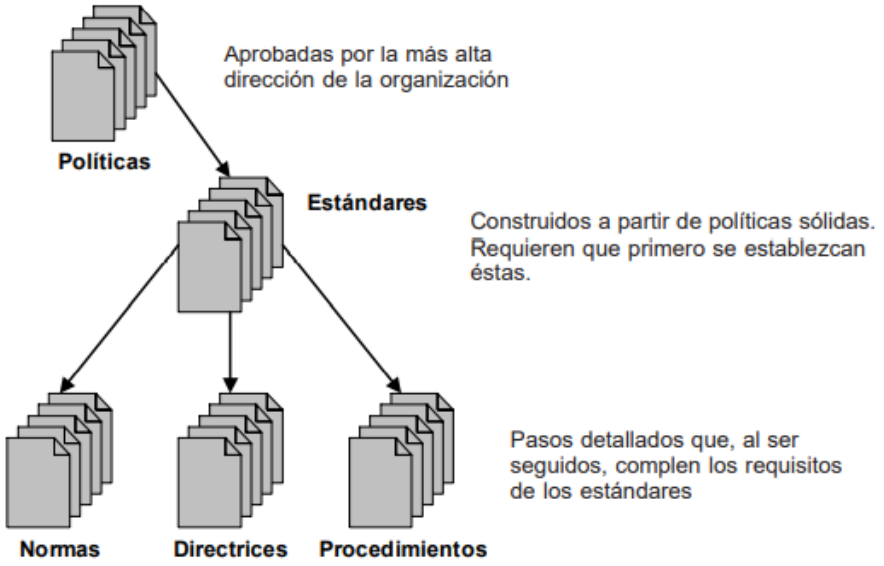


Figura 3.17: Estructura jerárquica de documentación de seguridad.

Fuente: Seguridad Informática Para Empresas Y Particulares [24].

El equipo de desarrollo de políticas varía según el alcance, la escala y la complejidad del tema o materia de la política. Un caso puede ser una política de alcance limitado y dirigido a un proceso, tecnología o población en particular, el equipo de desarrollo puede estar conformado por un grupo pequeño o un solo individuo, otro caso puede ser para aquellas políticas de largo alcance, en este caso un equipo de desarrollo de políticas multifuncional puede ser el más apropiado [25].

Pueden participar los siguientes roles:

Líder de Seguridad de la Información o Punto Focal

Una política de seguridad al ser una iniciativa de seguridad de la información se necesita designar un líder o punto focal para gestionar la fase de desarrollo hasta la promulgación final de la política. La responsabilidad general puede asignarse a una persona clave con el consentimiento de los otros miembros del equipo de desarrollo en un rol de apoyo. Este punto focal guiará cada política a través del desarrollo y las revisiones posteriores. Al administrar la fase de desarrollo como un proyecto, es responsabilidad del punto focal establecer las tareas, el cronograma y los recursos necesarios para entregar con éxito el documento de política [28].

Expertos en la Materia

El equipo de desarrollo de políticas probablemente estará integrado por expertos en la materia en el tema o materia de la política. Es probable que los expertos en la materia provengan del equipo de seguridad. Además del equipo de seguridad el equipo de desarrollo de políticas puede necesitar la experiencia de otro miembro del personal en el área de TI que tenga conocimientos técnicos específicos en el dominio de la materia. Los expertos deben estar familiarizados con la tecnología o el proceso asociado con las políticas. Pueden ayudar a proporcionar una buena perspectiva si las políticas son realmente razonables, factibles y ejecutables [30].

Consejero Legal

De igual manera es de suma importancia que la Oficina del Asesor Jurídico, o una función similar, revise las políticas en un punto lógico del proceso de desarrollo, muy a menudo cuando se acerca a un borrador final. El asesor legal puede brindar su opinión sobre la aplicabilidad de la política o el conflicto que puede suceder con cualquier estatuto o regla legal o reglamentaria. La función de privacidad a menudo reside en el departamento legal y el oficial de privacidad deberá revisar cualquier conflicto que pueda existir con preocupaciones de privacidad. El abogado general puede aportar información sobre la viabilidad de la aplicación si se produce alguna infracción de la política [30].

Controles Internos y Auditoría

Los departamentos de Auditoría Interna y Controles Internos deben revisar la política para verificar que exista coherencia con el marco general de control y auditoría (por ejemplo, SOX) de la empresa. Se debe consultar al departamento de controles internos sobre la coherencia de las políticas con otros controles como una mejor práctica. La auditoría interna debe proporcionar una buena retroalimentación sobre la capacidad de monitorear y auditar las políticas en términos de sus procedimientos de auditoría [25].

Recursos Humanos

Muchas políticas de seguridad se centran en los empleados sobre lo que está permitido o es aceptable. El departamento de Recursos Humanos puede necesitar revisar las políticas de seguridad para verificar su coherencia y consistencia con otras políticas relacionadas con la seguridad. También deberán examinar las políticas para determinar la capacidad para hacer cumplir y cuáles serían las consecuencias del incumplimiento o de las violaciones de las políticas. El punto focal o equipo de seguridad de la información debe poder comunicar la gravedad o el impacto de no cumplir con las políticas para determinar si la violación puede ser considerada motivo de despido o de un sanción [28].

Redactor Técnico

Un redactor técnico puede resultar de mucha ayuda para determinar la estructura, el estilo y el formato adecuados para las políticas. Aunque algunos departamentos de seguridad pueden tener un redactor técnico en su grupo, la mayoría de las veces es mejor idea obtener un grupo de soporte técnico como recurso compartido. En el caso en que este recurso no esté disponible y se deje al equipo de seguridad para que sea el autor y editor del borrador de las políticas. El redactor técnico puede ayudar a organizar las políticas, editar los distintos borradores y corregir de ser necesario las políticas iniciales en busca de errores ortográficos o gramaticales que puedan surgir en el desarrollo. Un beneficio es que, si el redactor técnico tiene experiencia en la redacción de políticas de la empresa, puede impulsar la creación de políticas a través de su familiaridad con el estilo, así como el proceso para obtener unas políticas al nivel de aceptabilidad que la gerencia está acostumbrada. De igual manera es de suma importancia adoptar la guía de estilo corporativa para que sean publicables. Si existe, debe utilizarse para garantizar que las políticas tengan la misma apariencia que otras políticas corporativas, y evitar reescrituras y ayudar a que se acepten lo más rápidamente como documentos corporativos [30].

Representantes de Socios Comerciales

En un punto dado de la creación de las políticas, es muy útil probar las políticas para su aceptabilidad y receptividad con un representante comercial. Un socio comercial puede proporcionar retroalimentación al equipo de desarrollo de políticas sobre temas como: el lenguaje, la prosa y el estilo de la escritura. El personal técnico tiende a hablar en términos muy complejos; el representante comercial puede ser de mucha ayuda al equipo a adaptar la intención y el contenido en términos que sean más comerciales. Si los empleados no pueden comprender las políticas, es menos probable que las cumplan. Además, para las empresas globales, es posible que se requiera de un representante comercial para que cada región revise la política en el idioma nativo en el que se implementara. El equipo no debe depender exclusivamente de los servicios de traducción, sino utilizar un representante comercial para examinar e incluso corregir las traducciones inexactas. Cuando se revisa o actualiza las políticas de seguridad actuales, las pruebas con un representante comercial ayudan a determinar el éxito de la intención de las políticas. Esto ayudará a indicar si se requiere una actualización o revisión. Esto es particularmente significativo cuando las políticas se han implementado durante varios años y están en peligro de volverse irrelevantes y que no sea necesario continuar con algunas.

Existen tres consideraciones clave en la redacción de las políticas: mantener el propósito y el alcance de la política, identificar a la audiencia y garantizar la aplicabilidad, redactar la política en el nivel correcto o los detalles necesarios e identificar cualquier condición de excepción y proceso para lograr una excepción.

El grado de detalle y extensión suele depender del tipo de política y de la audiencia objetivo. Las políticas organizativas deben estar redactadas a un nivel suficientemente alto que sean duraderas y no requieran cambios frecuentes. Las políticas deben ser lo suficientemente universales para adaptarse a cambios organizativos como fusiones, adquisiciones y desinversiones con poca necesidad de actualizar o modificar las políticas fuera de las revisiones programadas. Las políticas de la organización deben tener solo dos o tres páginas (quién es responsable de qué) y un funcionario corporativo u otro gerente superior apropiado debe aprobar la política para otorgarle la autoridad

adecuada. Las políticas también pueden referirse a los estándares, procedimientos o pautas subordinados asociados con la política de alto nivel.

Las normas, como formas más detalladas de política, son a menudo requisitos operativos o técnicos, como controles u objetivos de control. Las políticas que combinan declaraciones de intenciones de alto nivel con estándares detallados dan como resultado un documento complejo el cual puede crear problemas con la receptividad y comprensión de los empleados, así de igual forma problemas cuando terceros, como los clientes, requieren que la empresa divulgue las políticas. Estas solicitudes dan como resultado que la empresa tenga que generar más información de la que se siente cómoda con la divulgación. Es una buena práctica limitar el detalle en las políticas de alto nivel y dejar que los tipos de políticas subordinadas, como estándares o procedimientos, contengan el detalle adicional sobre cómo se encuentra la implementación de la política [25].

3.1.1.13. Proceso Publicación de Políticas

Finalizada la fase de desarrollo de las políticas están listas para la revisión, seguirá el proceso de gobierno establecido y se distribuirá a los departamentos de TI complementarios para la revisión y aprobación de las políticas. Si el departamento de TI está satisfecho con las políticas en la versión finalizada, se envía al grupo de administración de políticas centralizada. Posterior, el grupo de administradores de políticas asigna personal a las políticas con las funciones corporativas relevantes y los representantes de liderazgo empresarial. Las funciones corporativas (como pueden ser, Recursos Humanos, Legal, Auditoría) pueden preguntar quién estuvo involucrado en la redacción de la política y luego consultar con un miembro del equipo de desarrollo para poder observar si hay algún problema o crítica. Algunas funciones corporativas pueden asignar un revisor independiente que no se encontraba en el equipo de desarrollo original para comprobar el cumplimiento. La revisión del liderazgo empresarial implica una revisión más detallada para obtener su aprobación. El liderazgo empresarial tiene una razón válida para realizar una revisión tan detallada: una política que generalmente no es aceptable para la empresa o que carece de apoyo empresarial es una política que no se adoptará ni se hará cumplir fácilmente. Una vez

que el equipo de gestión de políticas ha completado la socialización y la dotación de personal de la política propuesta, se puede considerar que el documento está listo para la publicación.

Una vez aceptadas y promulgadas formalmente, como documentos, las políticas deben publicarse electrónicamente para que sean de fácil acceso para todos los empleados. Las grandes empresas deben contar con un repositorio de políticas organizado en la intranet de su empresa, disponible para descargar, imprimir y guardar. Para esas organizaciones o empresas más pequeñas, la función de seguridad de la información puede alojar sus políticas en su propio sitio interno.

El siguiente paso en la publicación es dar a conocer la política. Una estrategia de comunicación de políticas eficaz garantizará que todas las audiencias objetivo conozcan las políticas de seguridad nuevas o actualizadas, conozcan en qué lugar encontrarlas y que comprendan cómo cumplirlas y las consecuencias que se pueden generar el incumplimiento. La decisión se toma si la política se comunica a toda la población de empleados o un subconjunto de los empleados más afectados por la política. Algunas empresas grandes luchan en la manera de cómo comunicar las políticas, pero para las políticas de seguridad, el enfoque de comunicación debe ser un enfoque de estrategia de comunicación personalizado, de modo que la población o grupo de empleados objetivo reciba directamente solo las políticas necesarias [31].

Una manera eficaz de comunicar las políticas de seguridad es mediante el establecimiento anual de educación sobre seguridad y capacitación en concientización. La mayoría de las organizaciones utilizan la plataforma de aprendizaje común para organizar una formación anual obligatoria sobre seguridad de la información en la que las políticas se comunican a todos los empleados [25].

3.1.1.14. Revisión y Actualización de Políticas

Es necesario revisarlas y actualizarlas periódicamente todas las políticas de seguridad. Una revisión anual garantiza que la política se mantenga actualizada, relevante y actualizada. Las actualizaciones AD HOC pueden ser necesarias cuando un cambio fundamental significativo en la tecnología, el proceso o la realineación organizacional afecta la relevancia o aplicabilidad de la política existente, o partes de ella. El proceso de revisión debe seguir el proceso de desarrollo inicial con una cuestión de integridad del proceso. La revisión puede ser más corta si la política no requiere cambios o actualizaciones importantes [32].

El tiempo de revisión varía según la empresa y el sector empresarial en el que se opera; lo recomendable es una vez al año, pero los tiempos pueden varias de seis meses a una vez cada cinco años. Durante la revisión es necesario tener presente las siguientes preguntas [27]:

- ¿Han cambiado los procedimientos o procesos?
- ¿Es la política relevante?
- ¿Han cambiado las leyes?
- ¿El proceso de gestión de cambios incorpora cambios en la documentación?
- ¿Han cambiado las mejores prácticas de la industria?
- ¿Los hallazgos de las auditorías periódicas han indicado un problema con la documentación, como políticas y procedimientos?

Una vez completado el proceso de revisión, los resultados deben documentarse en las mismas políticas, generalmente una sección de revisión y cambio del documento de cada política. Las decisiones agregadas de actualizar, retirar o mantener la misma política en su lugar también deben estar contempladas en la documentación de alguna forma, generalmente en las actas de la reunión del equipo de revisión. De igual manera se deben seguir los mismos pasos seguidos en la publicación y comunicación de la política inicial para mantener la coherencia. Sin embargo, puede simplificarse mucho más mediante un correo electrónico para las audiencias objetivo; si no hubo cambios, el equipo de gestión de políticas puede decidir que una notificación formal es innecesaria [32].

3.1.1.15. Métodos para el Desarrollo de Políticas de Seguridad

Para el desarrollo de políticas de seguridad se sigue las siguientes cinco fases interrelacionadas:

1. Análisis y valoración de riesgos.
2. Construcción de la política
3. Implantación de la política
4. Mantenimiento de la política.
5. Implicación de todo el componente humano.

3.1.1.16. Objetivos de la Política

En la construcción de una política es muy importante especificar todos los detalles como de quien, cuando y donde se aplicará la política de seguridad, así como explicar los resultados esperados por el documento de la política de seguridad, como se muestra en la Figura 3.18 [33].

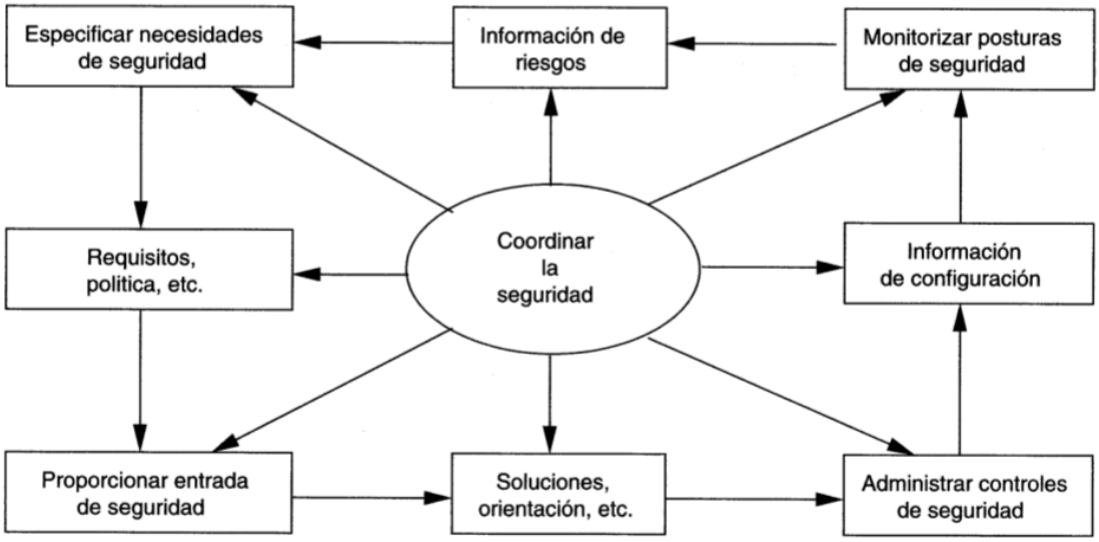


Figura 3.18: Ciclo de vida del proceso de seguridad.

Fuente: Seguridad de la Información [33].

3.1.1.17. SGSI y ISO 27001

La ISO 27001 mediante un enfoque por procesos, presenta un modelo para la creación, implementación, funcionamiento, supervisión, revisión y mantenimiento de un SGSI. El éxito que posee se debe a que posee los modelos de gestión en las UNE-EN ISO 9001 y 14001 que permite la integración de los sistemas. Los objetivos de control y controles que se desarrollan con más profundidad en la ISO 27002, [21]. En la Figura 3.19 se muestra el modelo PDCA para un sistema SGSI implementada por la ISO 27001.

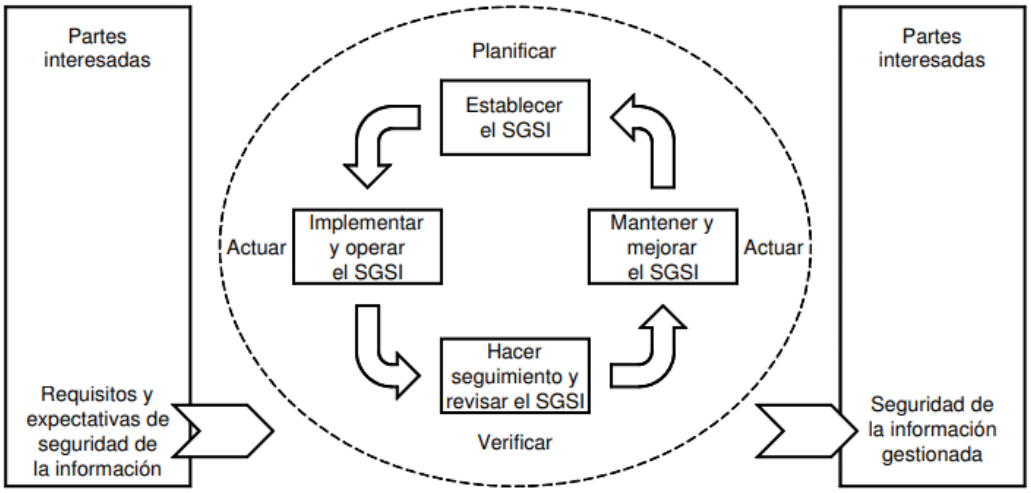


Figura 3.19: Modelo PDCA para un SGSI.

Fuente: ISO 27001 [34].

3.1.1.18. ISO 27002

La ISO 27002 es un código de buenas prácticas la cual comprende un catálogo de los controles de seguridad y una guía para la implantación de SGSI; se compone de 11 dominios, 39 objetivos de seguridad y 133 controles de seguridad; y cada dominio conforma un capítulo de la norma que se centra en un aspecto de seguridad de la información, como se puede observar en la Figura 3.20 [21].

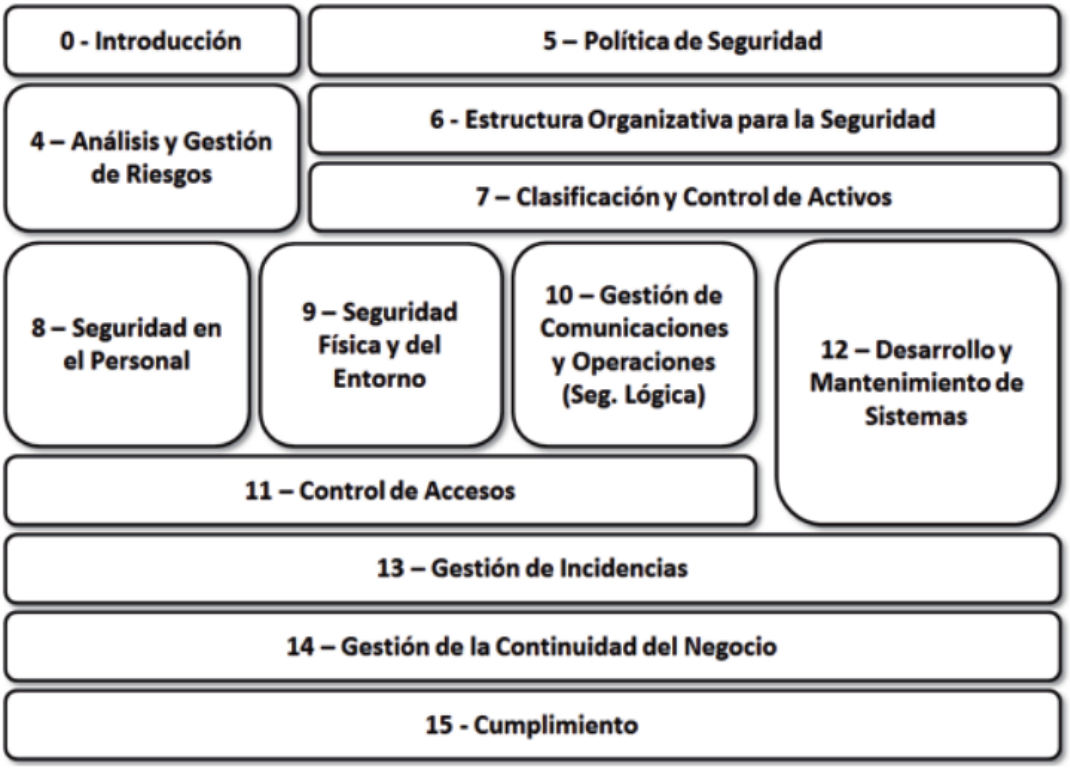


Figura 3.20: ISO 27002.

Fuente: ISO 27002 [35].

3.1.2. Análisis y Valoración de Riegos en la Empresa

En base a estudios e investigaciones realizadas en el ámbito de la seguridad informática y el teletrabajo, se observan varios aspectos en cuanto a la seguridad informática que se deben tomar en cuenta para poder reducir o mitigar ciertas amenazas que puede surgir con la realización de teletrabajo y que podían afectar gravemente a los activos de la empresa y representaría grandes pérdidas económicas para la misma.

Con la realización de la encuesta y entrevista; se obtuvo información en cuanto a las amenazas que podrían afectar a la empresa y el impacto que tendría; para ello se emplea un indicador de 1 a 10, los datos obtenidos se muestran en la Tabla 3.1.

Tabla 3.1 Priorización de Amenazas.

Elaborado por: Investigador

Amenaza	Impacto
Robo de información secreta	10
Acceso ilegitimo a información	8
Infección de equipos con malware	9
Indisponibilidad de servidores web	10
Robo y perdida de equipos informáticos	9
Phishing, Web Spoofing, etc.	8
Correo Malicioso	8
Fallos de hardware en equipos de la empresa	9
Fallos de software de la empresa	9
Configuración inadecuada de routers	8
Aplicaciones y equipos desactualizados	8
Configuración y políticas en equipos inadecuadas o inexistentes	7
Gestión inadecuada de contraseñas	7
Contraseñas que no cumple con estándares de seguridad	8
Desconocimientos de los empleados de nuevas técnicas que aplican los atacantes	8
Uso personal y empresarial de equipos empresariales	7
Ingreso a sistemas empresariales mediante una red publica	9
Unidades de almacenamiento sin protección	9

3.1.3. Análisis de Vulnerabilidades Mediante Herramientas

Para obtener más información de posibles vulnerabilidades presentes en la empresa se empleó varias herramientas que son muy conocidas en el ámbito del análisis forense como son: Maltego, The Harvester, Anubis, Sublist3r; que proporcionan información sobre dominios o personas, despendiendo de la herramienta; la información que se obtiene comprende desde correos electrónicos, host, usuarios, cuentas de Facebook, Twitter, documentos, etc.

La herramienta por excelencia para obtener información es Maltego, una aplicación de inteligencia y análisis forense de código abierto la cual permite extraer y recopilar información y representar la información de una manera significativa. El término fuente abierta en Maltego posee un significado que recopila información de fuente abierta. Una vez que Maltego recopila la información permite identificar las relaciones clave entre la información recopilada [36].

Mediante Maltego se obtuvo:

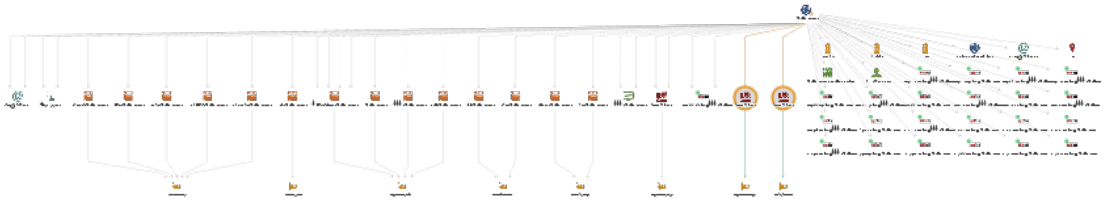


Figura 3.21: Datos obtenidos por Maltego.

Elaborado por: Investigador.

En la Figura 3.21 se observa la información obtenida con Maltego en el análisis del dominio de Bioalimentar, en la cual se puede apreciar: NS Record, DNS from Domain, MX Record, Número de Teléfono, Correo Electrónico, Dirección, Entidad Persona, Snapshots del dominio, etc.

Toda la información obtenida mediante Maltego se puede observar en la Tabla 3.2, la información obtenida será empleada posteriormente para análisis con otras herramientas.

Tabla 3.2 Servidores Relacionados al Dominio.

Elaborado por: Investigador.

Nombre	Servicio	Dirección IP
bioalimentar.com	DNS Name	3.
. bioalimentar.com	DNS Name	3.
bioalimentar.com	DNS Name	3.
.bioalimentar.com	DNS Name	3.
bioalimentar.com	DNS Name	3.
bioalimentar.com	DNS Name	144.
www.bioalimentar.com	Website	144.
www.bioalimentar.com	DNS Name	144.
bioalimentar.com	DNS Name	144.
bioalimentar.com	DNS Name	144.
bioalimentar.com	DNS Name	52.
.bioalimentar.com	DNS Name	181.
bioalimentar.com	DNS Name	181.
.outlook.com	MX Record	104. 104.
bioalimentar.com	DNS Name	181.
bioalimentar.com	DNS Name	181.
dns1.nodovip.com	NS Record	144.
dns2.nodovip.com	NS Record	144.
dns3.nodovip.com	NS Record	179.

Otra herramienta muy conocida es Anubis, una herramienta de recolección de información y enumerador de subdominios, obtiene información de fuentes públicas, resultados de búsquedas indexados y de AnubisDB, además es capaz de identificar todos los servidores clave detrás de los dominios y generar cualquier IP [37].

En la Figura 3.22 se muestra una captura de la información obtenida en el análisis realizado con Anubis.

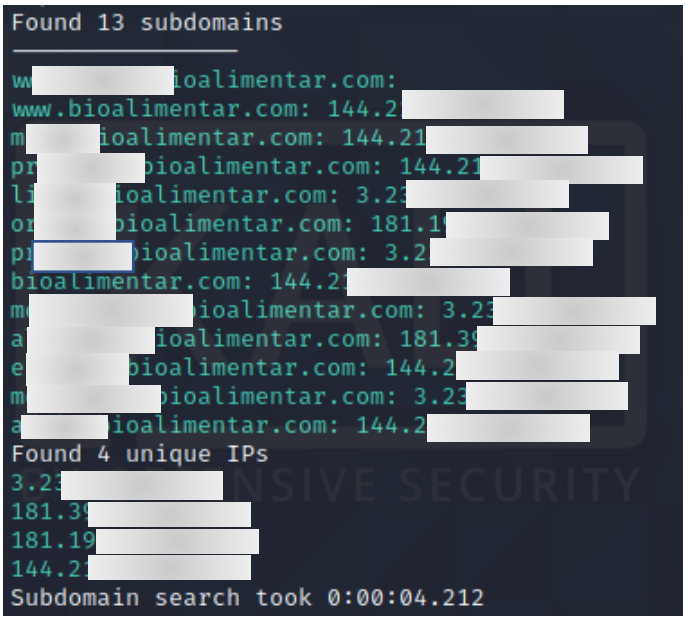


Figura 3.22: Subdominios y IPs obtenidas por Anubis.

Elaborado por: Investigador.

Tabla 3.3 Subdominios y IPs (Anubis).

Elaborado por: Investigador.

Subdominio	Dirección IP
[redacted].bioalimentar.com	--
www.bioalimentar.com	144.[redacted]
[redacted]bioalimentar.com	144.[redacted]
[redacted]bioalimentar.com	144.[redacted]
[redacted]bioalimentar.com	3.[redacted]
[redacted].bioalimentar.com	181.[redacted]
[redacted]bioalimentar.com	3.[redacted]
bioalimentar.com	144.[redacted]
[redacted].bioalimentar.com	3.[redacted]
[redacted]bioalimentar.com	181.[redacted]
[redacted]bioalimentar.com	144.[redacted]
[redacted]bioalimentar.com	3.[redacted]
[redacted].bioalimentar.com	144.[redacted]

En la Tabla 3.3 se encuentra la información obtenida mediante Anubis organizada por dominio y dirección IP a la que pertenece.

Existe otra manera de obtener información y es mediante la herramienta the Harvester; un script que busca a través de diferentes fuentes para localizar información de contacto según el dominio proporcionado, además cuenta con diferente fuentes de búsqueda como son: Google, DuckDuckGo, Bing, Linkedin, entre otras; de igual manera puede buscar usuarios y por ende direcciones de correo electrónico [27].

En la Figura 3.23 y en la Figura 3.24 se muestra una captura que muestra la información obtenida por la herramienta theHarvester que muestra los diferentes usuarios con los cargos que desempeñan o desempeñaron en la empresa.

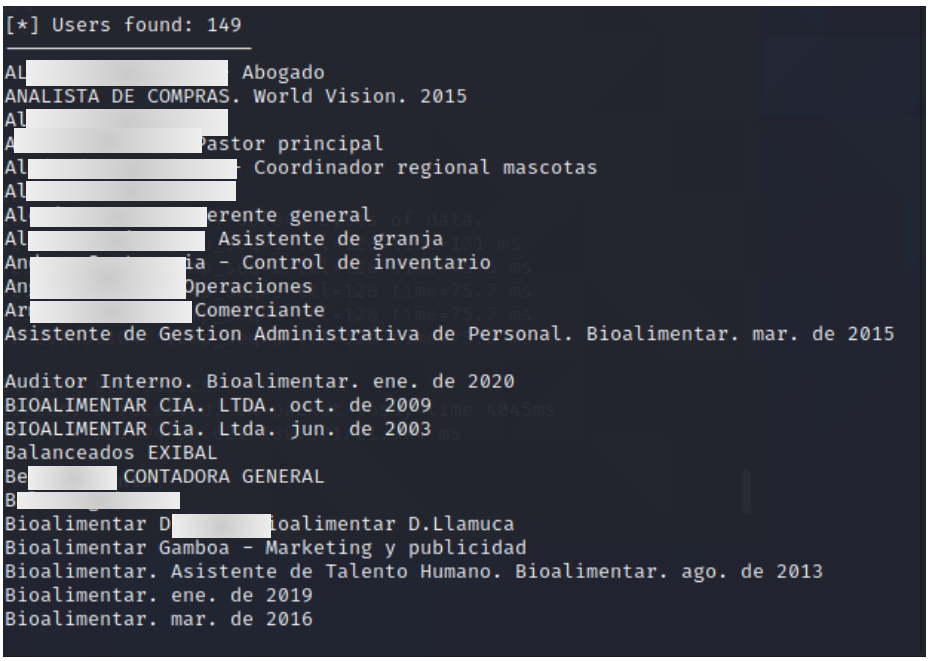


Figura 3.23: Usuarios Parte 1 (theHarvester).

Elaborado por: Investigador.

Figura 3.24: Usuarios Parte 2 (theHarvester).

Elaborado por: Investigador.

En la Figura 3.25 se muestran los correos electrónicos y los hosts encontrados mediante la herramienta theHarvester en su análisis.

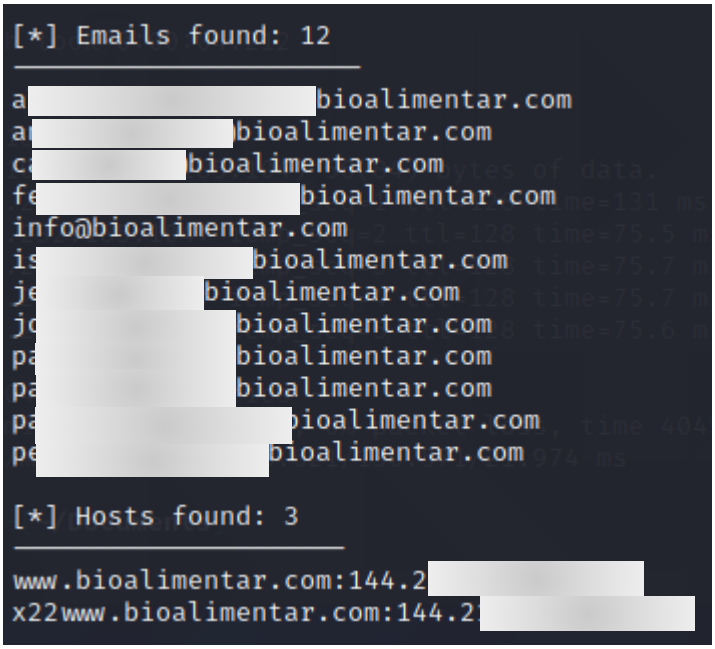


Figura 3.25: Correos Electrónicos y Subdominios (theHarvester).

Elaborado por: Investigador.

En la Tabla 3.4 se muestra la información obtenida mediante el análisis realizado con la herramienta theHarvester, la cual se encuentra organizada por subdominios y direcciones IPs a la que pertenece.

Tabla 3.4 Subdominios y IPs de la empresa (theHarvester).

Elaborado por: Investigador.

Subdominio	Dirección IP
www.bioalimentar.com	--
www.bioalimentar.com	144.
bioalimentar.com	144.
bioalimentar.com	144.
bioalimentar.com	3.
bioalimentar.com	181.
bioalimentar.com	3.
bioalimentar.com	144.
bioalimentar.com	3.
.bioalimentar.com	181.
bioalimentar.com	144.
bioalimentar.com	3.
.bioalimentar.com	144.

Sublist3r es una herramienta desarrollada en Python la cual permite enumerar subdominios de sitios web, para ello emplea un sin número de motores de búsqueda como Google, Yahoo, Bing, Baidu y Ask; de igual manera Sublist3r enumera los subdominios que utilizan Netcraft, Virustotal, ThreatCrowd, DNSdumpster y ReverseDNS [38]. Se empleo Sublist3r para obtener información de la empresa, la cual se muestra en la Figura 3.26.

Figura 3.26: Subdominios (Sublist3r).

Elaborado por: Investigador.

En la Tabla 3.5 se muestra los subdominios que se obtuvieron mediante la herramienta Sublist3r; solo se logró obtener los dominios de la empresa, los cuales concuerdan con los obtenidos por las demás herramientas con lo cual se corrobora que la información obtenida es correcta.

Tabla 3.5 Subdominios (Sublist3r).

Elaborado por: Investigador.

Subdominios
www.bioalimentar.com
bioalimentar.com
.bioalimentar.com
bioalimentar.com
.bioalimentar.com
bioalimentar.com
.bioalimentar.com
bioalimentar.com
www.libra.bioalimentar.com
bioalimentar.com
bioalimentar.com
.bioalimentar.com

Mediante los datos obtenidos con las 4 herramientas empleadas que son: Maltego, Anubis, theHarvester y Sublist3r se puede llegar a observar que dominios y subdominios posee la empresa , además de cuales no deben estar expuesto en Internet, de igual manera se observa correos de la empresa que pueden ser víctimas de spam, así como el patrón que se sigue para la creación de correos electrónicos. Un aspecto muy importante a tener en cuenta son los usuarios encontrados que en cierto caso constan en los correos electrónicos de la empresa, así como la información sobre los empleados y los cargos en los que se encontraban o se encuentran actualmente.

En la Tabla 3.6 se puede observar un cuadro comparativo con la información que se obtuvo de cada herramienta empleada.

Tabla 3.6 Cuadro comparativo de información obtenida de fuentes abiertas.

Elaborado por: Investigador.

	Maltego	Anubis	theHarvester	Sublist3r
Dominios y direcciones IPs	X	X	X	X
Números de teléfono	X	-	X	-
Correos electrónicos	X	-	X	-
Información personal y cargos desempeñados	-	-	X	-

Sondeo de Puertos

Una vez obtenidos los subdominios y las IPs se procede a realizar un sondeo de los puertos que se encuentran abiertos; para ello se lo realiza mediante la herramienta zenmap. Zenmap es la versión GUI de nmap, es una aplicación multiplataforma que es gratuita y de código abierto, la cual fue diseñada para que sea más fácil de usar para los principiantes, además de al mismo tiempo proporcionar funciones avanzadas para usuarios expertos con nmap [39]. En la Figura 3.27 se puede observar el funcionamiento de Zenmap.

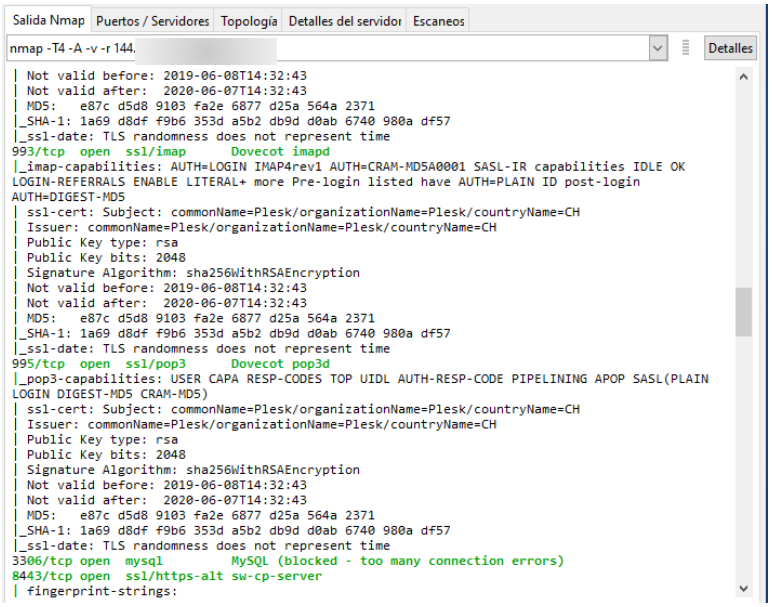


Figura 3.27: Sondeo de Puertos con Zenmap.

Elaborado por: Investigador.

IP 144.*.***.***

Mediante el análisis realizado con la herramienta zenmap a la primera dirección IP se observa una gran variedad de puertos que se encuentran abiertos con su respectivo servicio y versión del mismo, los cuales se encuentran organizados en la Tabla 3.7.

Tabla 3.7 Puertos Abiertos IP 1.

Elaborado por: Investigador.

Puerto	Servicio	Versión
21	ftp	ProFTPD
22	ssh	OpenSSH 7.4 (protocol 2.0)
80	http	Nginx
106	tcpwrapped	--
110	pop3	Dovecot pop3d
143	imap	Dovecot imapd
443	ssl/http	Nginx
465	ssl/smtp	Postfix smtpd
587	smtp	Postfix smtpd
993	ssl/imap	Dovecot imapd
995	ssl/pop3	Dovecot pop3d
3306	mysql	MySQL
8443	ssl/https-alt	sw-cp-server

IP 3.*.***.***

En el análisis realizado a la segunda IP muestra de igual manera puertos que se encuentran abiertos, pero en este caso son menores, los datos obtenidos de la segunda IP se muestran en la Tabla 3.8.

Tabla 3.8 Puertos Abiertos IP 2.

Elaborado por: Investigador.

Puerto	Servicio	Versión
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd
443	ssl/http	Apache httpd

IP 181.*.***.***

De igual manera en la siguiente dirección IP escaneada se obtiene muy buenos resultados al presentar un solo puerto abierto, el cual se muestra en la Tabla 3.9.

Tabla 3.9 Puertos Abiertos IP 3.

Elaborado por: Investigador.

Puerto	Servicio	Versión
443	ssl/http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 mod_perl/2.0.11 Perl/v5.16.3)

IP 181.*.***.***

En la Tabla 3.10 se muestra los puertos que se encuentran abiertos en la siguiente dirección IP, en este caso son el puerto 22 con OpenSHH y el puerto 80 y 443 de nginx que es un servidor web/proxy inverso ligero de alto rendimiento, que se encuentra en la versión 1.16.1.

Tabla 3.10 Puertos Abiertos IP 4.

Elaborado por: Investigador.

Puerto	Servicio	Versión
22	ssh	OpenSSH 7.4 (protocol 2.0)
80	http	nginx 1.16.1
443	ssl/http	nginx 1.16.1

IP 52.*.***.***

En análisis realizado a la IP 52.***.***.***, se observa un único puerto abierto que comprende el puerto 443 con RTC que comprende los servicios de comunicación en tiempo real, que se puede observar en la Tabla 3.11.

Tabla 3.11 Puertos Abiertos IP 5.

Elaborado por: Investigador.

Puerto	Servicio	Versión
443	ssl/sip	RTC/7.0

IP 144.*.***.***

En el análisis realizado a la dirección IP 144.***.***.***, arrojo los datos que se muestran en la Tabla 3.12, en donde se puede observar una mayor cantidad de puertos que se encuentran abiertos como son el puerto 80 y el puerto 433 de Apache, así como el puerto 3306 que es la base de datos MariaDB.

Tabla 3.12 Puertos Abiertos IP 6.

Elaborado por: Investigador.

Puerto	Servicio	Versión
22	ssh	OpenSSH 7.4 (protocol 2.0)
25	smtp	--
53	domain	(unknown banner: Windows 3.11 for Workgroups unexistant DNS ver: 6.666.66)
80	http	Apache httpd
443	ssl/http	Apache httpd
3306	mysql	MariaDB
8080	ssl/http	Apache httpd (PHP 5.4.16)
8081	http	Apache httpd

IP 144.*.***.***

En el análisis realizado a la dirección 144.***.***.***, que se muestra en Tabla 3.13, se puede observar que se encuentran abiertos 3 puertos que son: 22, 25 y 53 que corresponden a OpenSHH, servicio smtp y NLnet Labs NSD que corresponde a un servidor de nombres DNS autorizado.

Tabla 3.13 Puertos Abiertos IP 7.

Elaborado por: Investigador.

Puerto	Servicio	Versión
22	ssh	OpenSSH 7.4 (protocol 2.0)
25	smtp	--
53	domain	NLnet Labs NSD

IP 179.*.***.***

En la última dirección analizada con zenmap, se obtiene de igual manera que los puertos 22 y 53 se encuentra abiertos, como se puede observar en la Tabla 3.14.

Tabla 3.14 Puertos Abiertos IP 8.

Elaborado por: Investigador.

Puerto	Servicio	Versión
22	ssh	OpenSSH 7.4 (protocol 2.0)
53	domain	NLnet Labs NSD

Se determino que en ciertos casos algunos servidores poseen demasiados puertos abiertos y que en ciertos casos no son necesarios y que los atacantes informáticos pueden aprovecharse de estas vulnerabilidades y explotarlas. De igual manera se determinó que la empresa no posee un IDS (Sistema de Detección de Intrusos) o IPS (Sistema de Prevención de Intrusos) que sea de ayuda en la detección de este tipo de ataques como es un sondeo de puertos, en este caso con Zenmap.

En la Figura 3.28 se puede observar la topología de la red de la empresa con todos los servidores que posee y que función cumple cada servidor.

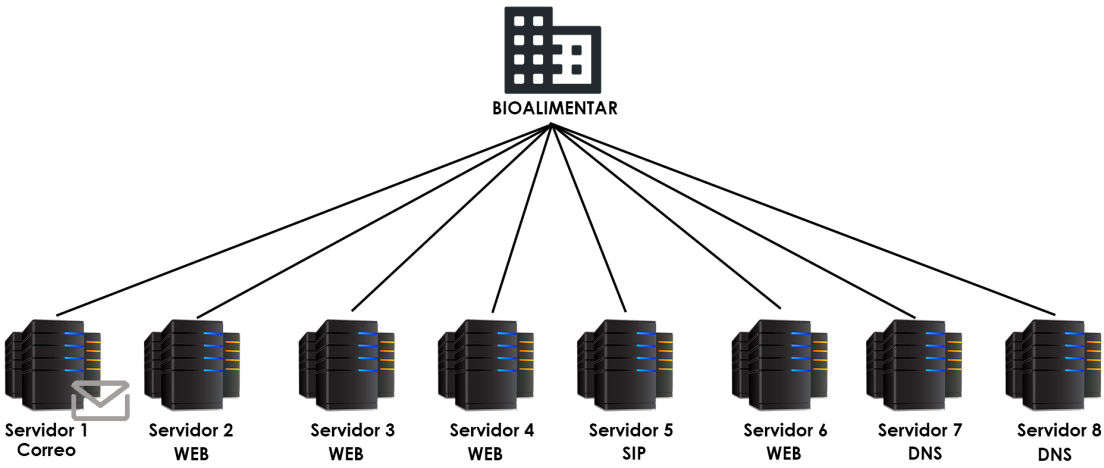


Figura 3.28: Topología de la Red de la Empresa.

Elaborado por: Investigador.

Análisis de Vulnerabilidades mediante la herramienta InsightVM

Para tener una visión más amplia de las vulnerabilidades presentes en la empresa es necesario emplear software especializado en la detección de vulnerabilidades; un software muy conocido es InsightVM de Rapid7 que es la evolución de Nexpose, la cual reúne las bibliotecas de investigación de vulnerabilidades de Nexpose, el conocimiento de Metasploit, el comportamiento de los atacantes, los datos de escaneo del Internet, el análisis de exposición y los informes en tiempo real denominados Liveboards [40].

Mediante el análisis realizado con la herramienta InsightVM en la empresa se obtiene la siguiente información en cada servidor.

Servidor 1

Mediante el análisis realizado con InsightVM al servidor 1, se obtiene la información acerca del servidor y de las vulnerabilidades que posee, como se puede observar en la Figura 3.29; en donde se observa un resumen del último análisis realizado y las características del servidor, mientras que en la Tabla 3.15 se pueden observar las vulnerabilidades detectadas en el análisis.

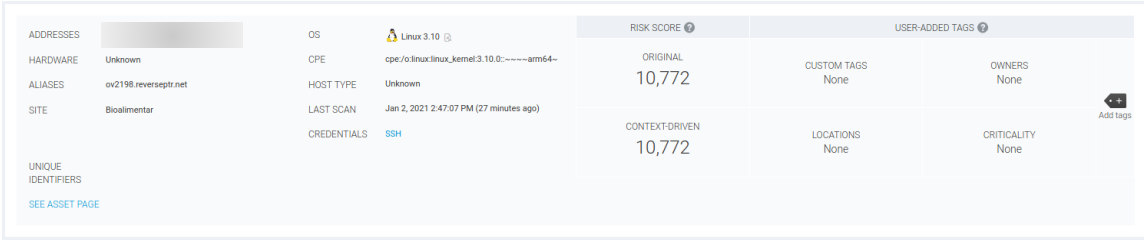


Figura 3.29: Análisis de Vulnerabilidades Servidor 1 (InsightVM).

Elaborado por: Investigador.

Tabla 3.15 Vulnerabilidades Detectadas Servidor 1 (InsightVM).

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Credenciales IMAP transmitidas sin cifrar	Severo	1
Credenciales FTP transmitidas sin cifrar	Severo	1
Credenciales POP transmitidas sin cifrar	Severo	1
El CN sujeto del certificado X.509 no coincide con el nombre de la entidad	Severo	7
El certificado del servidor X.509 no es válido / ha caducado	Severo	7
Certificado X.509 de servidor TLS / SSL que no es de confianza	Severo	7
Acceso abierto a la base de datos	Severo	1
Ataques SSH Birthday en cifrados de bloque de 64 bits (SWEET32)	Severo	1
El servidor SSH admite algoritmos de intercambio de claves débiles	Severo	1
El servidor SSH admite diffie-hellman-group1-sha1	Severo	1
El servidor TLS / SSL está habilitando el ataque BEAST	Severo	5
Certificado TLS / SSL autofirmado	Severo	7
TLS Server admite TLS versión 1.0	Severo	9
Vulnerabilidad SSH CBC	Moderado	1
Método HTTP OPTIONS habilitado	Moderado	2
Grupo Diffie-Hellman menor de 2048 bits	Moderado	2
El servidor TLS / SSL admite el uso de cifrados de clave estática	Moderado	5
TLS Server admite TLS versión 1.1	Moderado	9
El servidor SSH admite el conjunto de cifrado 3DES	Moderado	1

Servidor 2

Al igual que en el análisis realizado al servidor 1 en el análisis realizado al servidor 2 se puede observar el tipo de sistema operativo, el sitio, el último escaneo, los riesgos, entre otra información que se muestran en la Figura 3.30.

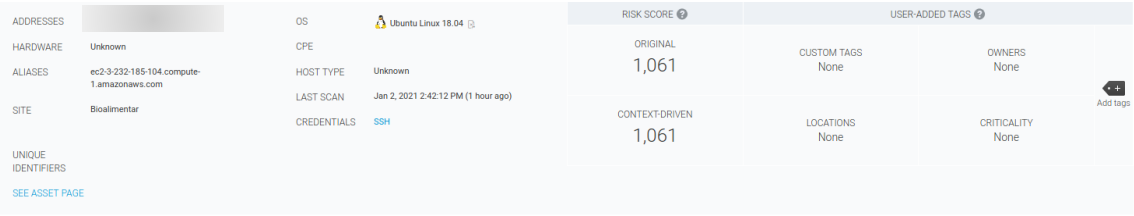


Figura 3.30: Análisis de Vulnerabilidades Servidor 2 (InsightVM).

Elaborado por: Investigador.

En el análisis realizado al servidor 2 se muestra vulnerabilidades moderadas en lo que es la transferencia de paquetes en la capa de transporte, que se muestran en la Tabla 3.16.

Tabla 3.16 Vulnerabilidades Detectadas Servidor 2 (InsightVM).

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
TLS Server admite TLS versión 1.1	Moderado	1
El servidor TLS / SSL admite el uso de cifrados de clave estática	Moderado	1
El servidor TLS / SSL utiliza números primos de uso común	Moderado	1
Respuesta de marca de tiempo TCP	Moderado	1

Servidor 3

En el análisis al servidor 3 se puede observar en la Figura 3.31 que la cantidad de riesgos es mucho mayor que la de los anteriores dos servidores; en la Tabla 3.17 se muestran las vulnerabilidades que son críticos lo que significa que hay que tenerlos en cuenta para solucionar lo más antes posible.

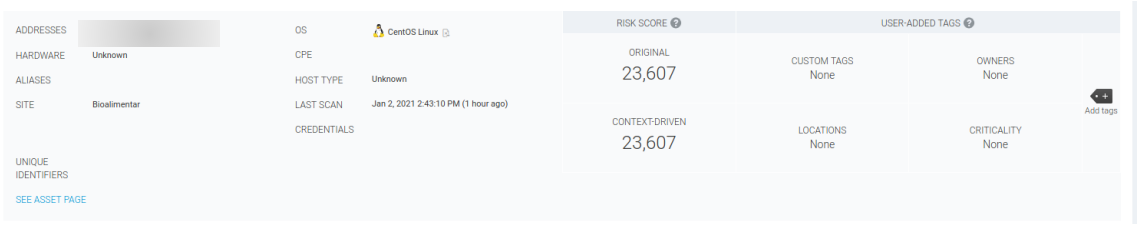


Figura 3.31: Análisis de Vulnerabilidades Servidor 3 (InsightVM).

Elaborado por: Investigador.

Tabla 3.17 Vulnerabilidades Detectadas Servidor 3 (InsightVM).

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Versión obsoleta de PHP	Crítico	1
MS15-034: Una vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553)	Crítico	1
Apache HTTPD: ap_get_basic_auth_pw () Omisión de autenticación (CVE-2017-3167)	Crítico	1
Apache HTTPD: mod_mime Buffer Overread (CVE-2017-7679)	Crítico	1
Apache HTTPD: mod_ssl Desreferencia del puntero nulo (CVE-2017-3169)	Crítico	1
El CN sujeto del certificado X.509 no coincide con el nombre de la entidad	Severo	1
Apache HTTPD: desbordamiento del búfer mod_status (CVE-2014-0226)	Severo	1
Apache HTTPD: generación de autenticación de resumen débil en mod_auth_digest (CVE-2018-1312)	Severo	1
Apache HTTPD: <FilesMatch> omite con una nueva línea al final del nombre del archivo (CVE-2017-15715)	Severo	1
Certificado X.509 de servidor TLS / SSL que no es de confianza	Severo	1
Método HTTP TRACE habilitado	Severo	1
Apache HTTPD: reflejo de la memoria no inicializada en mod_auth_digest (CVE-2017-9788)	Severo	1
Apache HTTPD: mod_rewrite potencial redireccionamiento abierto (CVE-2019-10098)	Severo	1

En la Tabla 3.17 se muestra la cantidad de 13 vulnerabilidades, pero el total de vulnerabilidades obtenidas mediante InsightVM es de 69, debido a que son demasiadas no se incluyen todas en el documento.

Servidor 4

En la Figura 3.32 se observa las características del servidor 4 además de no presentar un alto índice de riesgos como se puede comprobar en la Tabla 3.18 en donde se muestran 2 riesgos severos en relación con el SSH, y de igual manera vulnerabilidades y problemas en cifrado del SHH.

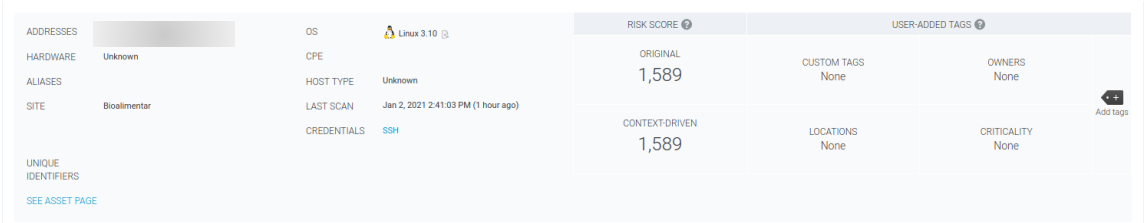


Figura 3.32: Análisis de Vulnerabilidades Servidor 4 (InsightVM).

Elaborado por: Investigador.

Tabla 3.18 Vulnerabilidades Detectadas Servidor 4 (InsightVM).

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Ataques SSH Birthday en cifrados de bloque de 64 bits (SWEET32)	Severo	1
El servidor SSH admite algoritmos de intercambio de claves débiles	Severo	1
El servidor SSH admite diffie-hellman-group1-sha1	Severo	1
Vulnerabilidad SSH CBC	Moderado	1
Respuesta de marca de tiempo TCP	Moderado	1
El servidor SSH admite el conjunto de cifrado 3DES	Moderado	1

Servidor 5

En el análisis realizado al servidor 5 no se obtuvo las características del mismo, como se muestra en la Figura 3.33; además presenta una única vulnerabilidad en lo que es el certificado, la cual es severa y se presenta en la Tabla 3.19.

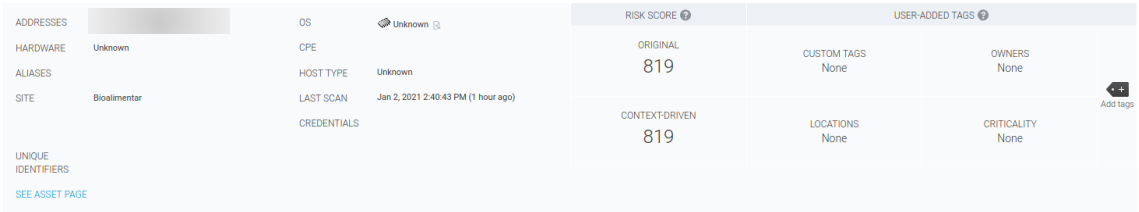


Figura 3.33: Análisis de Vulnerabilidades Servidor 5 (InsightVM).

Elaborado por: Investigador.

Tabla 3.19 Vulnerabilidades Detectadas Servidor 5 (InsightVM).

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
El CN sujeto del certificado X.509 no coincide con el nombre de la entidad	Severo	1

Servidor 6

En el análisis del servidor 6, obtuvo el mayor índice de riesgos en los servidores que hasta el momento han sido analizados, como se puede observar en la Figura 3.34.

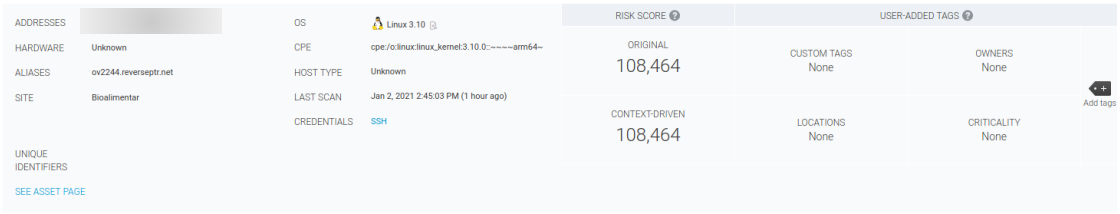


Figura 3.34: Análisis de Vulnerabilidades Servidor 6 (InsightVM).

Elaborado por: Investigador.

La cantidad de vulnerabilidades es muy extensa en el servidor 6, que comprenden desde la versión obsoleta de PHP, que es crítica, problemas en el SHH, que son severos, y otros que se muestran en la Tabla 3.19 que solo comprende una parte de las vulnerabilidades.

Tabla 3.20 Vulnerabilidades Detectadas Servidor 6 (InsightVM).

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Versión obsoleta de PHP	Critico	1
Vulnerabilidad de PHP: CVE-2015-4599	Critico	1
Instalación obsoleta de ISC BIND	Critico	2
Certificado X.509 de servidor TLS / SSL que no es de confianza	Severo	1
Método HTTP TRACE habilitado	Severo	4
Instalación predeterminada de Apache / página de bienvenida instalada	Severo	1
Ataques SSH Birthday en cifrados de bloque de 64 bits (SWEET32)	Severo	1
Ataques de cumpleaños TLS / SSL en cifrados de bloque de 64 bits (SWEET32)	Severo	1
El servidor TLS / SSL está habilitando el ataque BEAST	Severo	1
El servidor TLS / SSL admite algoritmos de cifrado RC4 (CVE-2013-2566)	Severo	1
TLS Server admite TLS versión 1.0	Severo	1

El servidor SSH admite algoritmos de intercambio de claves débiles	Severo	1

En la Tabla 3.20 se muestra la cantidad de 13 vulnerabilidades, pero el total de vulnerabilidades obtenidas con InsightVM es de 228, debido a que son demasiadas no se incluyen todas en el documento.

Servidor 7

En el análisis realizado al servidor 7 se puede observar que posee una cantidad mínima de vulnerabilidades, además de las características del servidor que se muestran en la Figura 3.35.

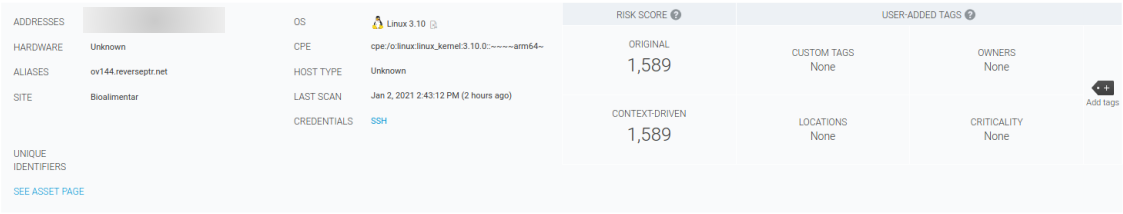


Figura 3.35: Análisis de Vulnerabilidades Servidor 7 (InsightVM).

Elaborado por: Investigador.

En cuanto a las vulnerabilidades obtenidas en el análisis están relacionadas al SHH y al DNS, la cuales comprenden un riesgo severo y moderado como se muestran en la Tabla 3.21.

Tabla 3.21 Vulnerabilidades Detectadas Servidor 7 (InsightVM).

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Ataques SSH Birthday en cifrados de bloque de 64 bits (SWEET32)	Severo	1
El servidor SSH admite algoritmos de intercambio de claves débiles	Severo	1
El servidor SSH admite diffie-hellman-group1-sha1	Severo	1
Vulnerabilidad SSH CBC	Moderado	1
El servidor SSH admite el conjunto de cifrado 3DES	Moderado	1
Amplificación del tráfico DNS	Moderado	1

Servidor 8

En el análisis al servidor 8 que es el último se obtuvo de igual manera una cantidad mínima de vulnerabilidades, además de las características del mismo que se muestran en la Figura 3.36.

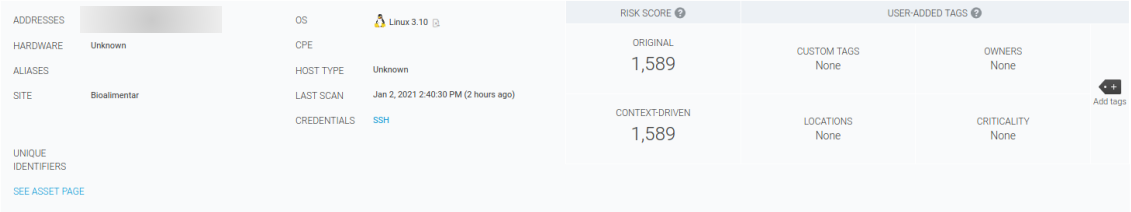


Figura 3.36: Análisis de Vulnerabilidades Servidor 8 (InsightVM).

Elaborado por: Investigador.

Las vulnerabilidades presentes en el servidor 8 comprenden algunas presentes en los servidores previamente analizados como son, problemas en el SHH, la respuesta de tiempo TCP, el cifrado en el SHH y otras más que muestran en la Tabla 3.22.

Tabla 3.22 Vulnerabilidades Detectadas Servidor 8 (InsightVM).

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Ataques SSH Birthday en cifrados de bloque de 64 bits (SWEET32)	Severo	1
El servidor SSH admite algoritmos de intercambio de claves débiles	Severo	1
El servidor SSH admite diffie-hellman-group1-sha1	Severo	1
Vulnerabilidad SSH CBC	Moderado	1
Respuesta de marca de tiempo TCP	Moderado	1
El servidor SSH admite el conjunto de cifrado 3DES	Moderado	1

En la Figura 3.37 se puede observar un resumen de los servidores analizados con el nombre del servidor, el sistema operativo, el número de vulnerabilidades y el escaneo realizado.

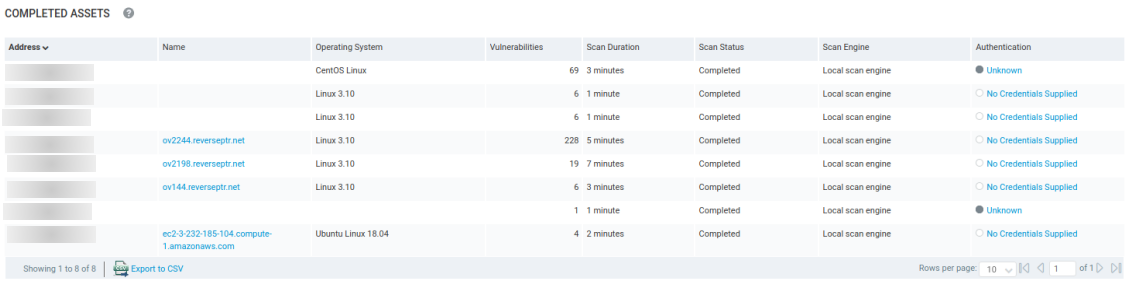


Figura 3.37: Resumen de Vulnerabilidades (InsightVM).

Elaborado por: Investigador.

Mediante el análisis realizado con la herramienta InsightVM se puede tener una primera visión del estado actual de la empresa, pero de igual manera es necesario corroborar que la información obtenida es la correcta, por ende es de suma importancia realizar otro análisis mediante otras herramientas y no confiar ciegamente solo en una, para ello también se realiza un análisis de vulnerabilidades con la herramienta OWASP ZAP que es una herramienta muy potente diseñada para monitorizar la seguridad de las aplicaciones web de las compañías [41].

Mediante el análisis realizado con OWASP ZAP se obtiene los siguientes resultados:

Servidor 1

- **www.bioalimentar.com**

El análisis al servidor 1 comprende la página principal de la empresa, en la cual se realiza el escaneo mediante la herramienta OWASP ZAP, en la Figura 3.38 se puede observar el análisis realizado en tiempo real.

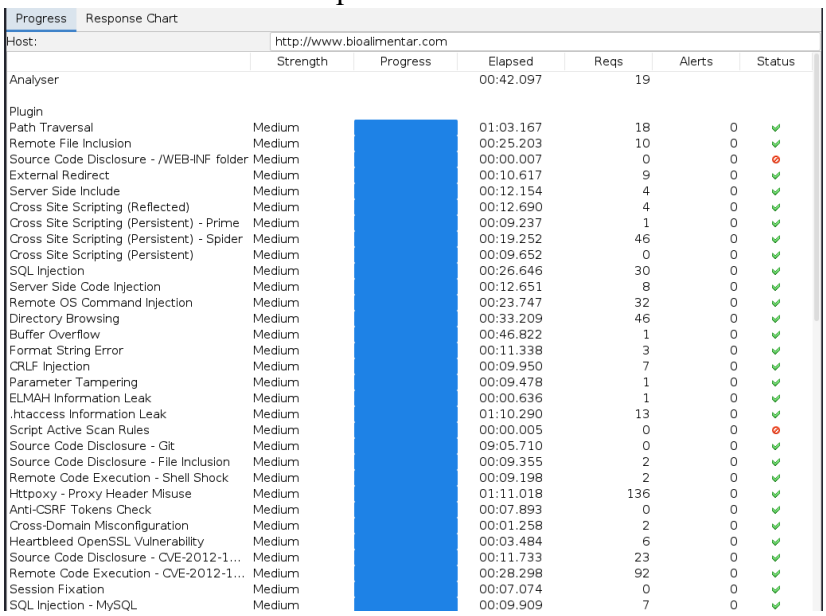


Figura 3.38: Proceso de Análisis de Vulnerabilidades (OWASP ZAP).

Elaborado por: Investigador.

Mediante el análisis realizado con OWASP ZAP se obtiene la información presente en la Tabla 3.23, en donde se puede observar las vulnerabilidades relacionadas con PHP, bibliotecas JS obsoletas, además de otras vulnerabilidades las cuales comprende un riesgo alto, medio y bajo.

Tabla 3.23 Vulnerabilidades Detectadas Dominio 1 (OWASP ZAP)

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Divulgación de PII	Alto	2
Encabezado de política de seguridad de contenido (CSP) no establecido	Medio	733
Tabnabbing Inverso	Medio	609
Divulgación del código fuente - PHP	Medio	53
Divulgación del código fuente - Perl	Medio	17
Falta el atributo de integridad del recurso secundario	Medio	7730
Biblioteca JS vulnerable	Medio	6
Encabezado X-Frame-Options no establecido	Medio	626
Ausencia de tokens anti-CSRF	Baja	120
Cross-Domain JavaScript Source File Inclusion	Baja	1834

En la Tabla 3.23 se muestra la cantidad de 10 vulnerabilidades, pero en el análisis realizado con OWASP ZAP muestra un total de 30, debido a que son demasiadas no se incluyen todas en el documento.

- *****.bioalimentar.com**
- **pr*****.bioalimentar.com**
- **e****.bioalimentar.com**
- **a*****.bioalimentar.com**
- **w********.bioalimentar.com**

De igual manera mediante el análisis realizado a los subdominios, se obtiene las mismas vulnerabilidades pertenecientes a la misma dirección IP, por ende, se muestran una sola tabla, como se puede observar en la Tabla 2.24.

Tabla 3.24 Vulnerabilidades Detectadas Dominio 2-6 (OWASP ZAP)

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Encabezado de política de seguridad de contenido (CSP) no establecido	Medio	3
Tabnabbing Inverso	Medio	1
Falta el atributo de integridad del recurso secundario	Medio	1
Encabezado X-Frame-Options no establecido	Medio	1
Inclusión de archivos de origen JavaScript entre dominios	Bajo	1
Cabecera de política de funciones no establecida	Bajo	3
Aislamiento insuficiente del sitio frente a la vulnerabilidad de Spectre	Bajo	6
Falta el encabezado X-Content-Type-Options	Bajo	4
Contenido almacenable en caché	Informativo	6
Fuzzer de agente de usuario	Informativo	14

Servidor 2

- **o****-p***.bioalimentar.com

En el análisis realizado al primer subdominio del servidor 2 se observa que posee riesgos de nivel medio, bajo e informativo, los cuales algunos se encontraban presentes en el primer servidor como son: bibliotecas JS obsoletas, ausencia de tokens anti-CSRF, entre otros que se muestran en la Tabla 3.25.

Tabla 3.25 Vulnerabilidades Detectadas Dominio 7 (OWASP ZAP)

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Encabezado de política de seguridad de contenido (CSP) no establecido	Medio	3
Confusión de ruta relativa	Medio	2
Tabnabbing Inverso	Medio	11
Biblioteca JS vulnerable	Medio	1
Encabezado X-Frame-Options no establecido	Medio	11
Ausencia de tokens anti-CSRF	Bajo	5
Cookie No HttpOnly Flag	Bajo	11
Cookie sin atributo SameSite	Bajo	11
Cookie sin bandera segura	Bajo	10
Funciones JS peligrosas	Bajo	6
Cabecera de política de funciones no establecida	Bajo	40
Conjunto de encabezado HTTP Pragma incompleto o sin control de caché	Bajo	19
Aislamiento insuficiente del sitio frente a la vulnerabilidad de Spectre	Bajo	84
Cabecera de seguridad de transporte estricta no establecida	Bajo	61
Falta el encabezado X-Content-Type-Options	Bajo	62
Divulgación Base64	Informativo	15
Falta el encabezado del tipo de contenido	Informativo	2
Envenenamiento por Cookie	Informativo	2
Divulgación de información: comentarios sospechosos	Informativo	13
Aplicación web moderna	Informativo	6
Contenido no almacenable	Informativo	12
Contenido almacenable en caché	Informativo	53
Divulgación de marca de tiempo - Unix	Informativo	11
Fuzzer de agente de usuario	Informativo	7
Atributo de elemento HTML controlable por el usuario (XSS potencial)	Informativo	5

- **l****.bioalimentar.com**

En el análisis al segundo subdominio del servidor 2, no se observan vulnerabilidades de alto riesgo si no de riesgo medio, bajo e informativo que están relacionadas con el encabezado X-Frame-Options, contenido almacenable en cache y otros más que se encuentran en la Tabla 3.26.

Tabla 3.26 Vulnerabilidades Detectadas Dominio 8 (OWASP ZAP)

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Encabezado de política de seguridad de contenido (CSP) no establecido	Medio	4
Encabezado X-Frame-Options no establecido	Medio	2
Cabecera de política de funciones no establecida	Bajo	4
Conjunto de encabezado HTTP Pragma incompleto o sin control de caché	Bajo	1
Aislamiento insuficiente del sitio frente a la vulnerabilidad de Spectre	Bajo	6
Cabecera de seguridad de transporte estricta no establecida	Bajo	3
Falta el encabezado X-Content-Type-Options	Bajo	2
Divulgación Base64	Informativo	2
Contenido no almacenable	Informativo	3
Contenido almacenable en caché	Informativo	4
Fuzzer de agente de usuario	Informativo	14

- **p****.bioalimentar.com**
- **m*******.bioalimentar.com**

En el análisis realizado a los siguientes subdominios del servidor 2 se puede observar que la presencia de vulnerabilidades es menor, siendo solo 2 vulnerabilidades de riesgo medio, 3 de nivel bajo y 4 informativos. Como se muestra en la Tabla 3.27 las vulnerabilidades presentes son de igual manera algunas vulnerabilidades que se encontraban presentes en el subdominio anterior.

Tabla 3.27 Vulnerabilidades Detectadas Dominio 9-10 (OWASP ZAP)

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Encabezado de política de seguridad de contenido (CSP) no establecido	Medio	1
Encabezado X-Frame-Options no establecido	Medio	1
Cabecera de política de funciones no establecida	Bajo	1
Aislamiento insuficiente del sitio frente a la vulnerabilidad de Spectre	Bajo	3
Falta el encabezado X-Content-Type-Options	Bajo	1
Divulgación Base64	Informativo	1
Contenido no almacenable	Informativo	3
Contenido almacenable en caché	Informativo	1
Fuzzer de agente de usuario	Informativo	14

- **m******.bioalimentar.com**

En el análisis del ultimo subdominio del servidor 2 se observan cierto tipo de vulnerabilidades que se muestran en la Tabla 3.28, que comprende la divulgación de marca de tiempo Unix, problemas en los comentarios con divulgación de información, entre otras, las cuales tienen que ser revisadas y tomadas en cuenta mediante el análisis previo que se realizó mediante el uso de diferentes herramientas.

Tabla 3.28 Vulnerabilidades Detectadas Dominio 11 (OWASP ZAP)

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Encabezado de política de seguridad de contenido (CSP) no establecido	Medio	14
Configuración incorrecta entre dominios	Medio	26
Confusión de ruta relativa	Medio	2
Tabnabbing inverso	Medio	12
Encabezado X-Frame-Options no establecido	Medio	12
Ausencia de tokens anti-CSRF	Bajo	48
Cookie No HttpOnly Flag	Bajo	13
Cookie sin atributo SameSite	Bajo	13
Cookie sin bandera segura	Bajo	12
Funciones JS peligrosas	Bajo	2
Cabecera de política de funciones no establecida	Bajo	22
Conjunto de encabezado HTTP Pragma incompleto o sin control de caché	Bajo	1
Aislamiento insuficiente del sitio frente a la vulnerabilidad de Spectre	Bajo	24
Cabecera de seguridad de transporte estricta no establecida	Bajo	23
Falta el encabezado X-Content-Type-Options	Bajo	24
Divulgación Base64	Informativo	21
Detector de holgura de cookies	Informativo	1

Divulgación de información: información confidencial en URL	Informativo	12
Divulgación de información: comentarios sospechosos	Informativo	7
Aplicación web moderna	Informativo	13
Contenido no almacenable	Informativo	16
Contenido almacenable en caché	Informativo	5
Contenido almacenable pero no almacenable en caché	Informativo	9
Divulgación de marca de tiempo - Unix	Informativo	15
Fuzzer de agente de usuario	Informativo	14

Servidor 3

- **g***.bioalimentar.com**
- **o***.bioalimentar.com**

En el análisis de vulnerabilidades realizado a los dominios g***.bioalimentar.com y o***.bioalimentar.com, la IP desde la cual se estaba analizando las vulnerabilidades fue bloqueada y por ende no se puedo continuar con el análisis de los dominios previamente mencionados, tampoco mediante el uso de una VPN, ya que el ingreso solo se encontraba permitido para el Ecuador.

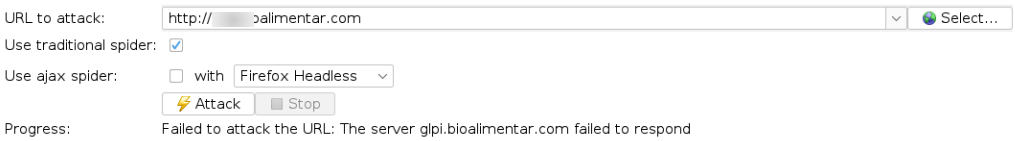


Figura 3.39: Proceso de Análisis de Vulnerabilidades Dominio 12 (OWASP ZAP).

Elaborado por: Investigador.

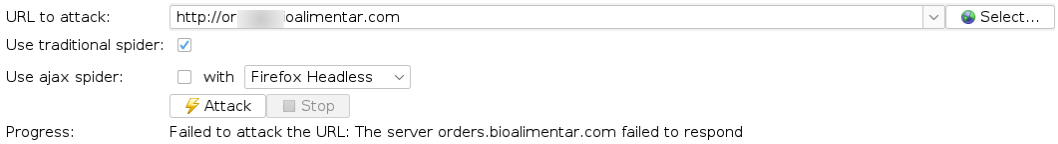


Figura 3.40: Proceso de Análisis de Vulnerabilidades Dominio 13 (OWASP ZAP).

Elaborado por: Investigador.

Como se puede observar en la Figura 3.39 así como en la Figura 3.40 falla el ataque a los dominios tanto con el uso de una VPN como sin él uso de una, por lo que en este punto se puede mencionar que mediante algún mecanismo o software como un IPS y IDS se bloqueó el acceso.

Servidor 4

- **d****.bioalimentar.com**

En la Tabla 3.29 se puede observar las vulnerabilidades del servidor 4 en el primer subdominio, en el cual se observa algunas vulnerabilidades presentes en los anteriores servidores y subdominios previamente analizados.

Tabla 3.29 Vulnerabilidades Detectadas Dominio 14 (OWASP ZAP)

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Encabezado de política de seguridad de contenido (CSP) no establecido	Medio	1
Encabezado X-Frame-Options no establecido	Medio	1
Cookie sin atributo SameSite	Bajo	1
Cabecera de política de funciones no establecida	Bajo	1
Aislamiento insuficiente del sitio frente a la vulnerabilidad de Spectre	Bajo	3
Información de versión de fugas de servidor a través del campo de encabezado de respuesta HTTP "Servidor"	Bajo	3
Falta el encabezado X-Content-Type-Options	Bajo	1
Divulgación Base64	Informativo	1
Contenido almacenable en caché	Informativo	3
Fuzzer de agente de usuario	Informativo	21

- **a*******.bioalimentar.com**

En la Tabla 3.30 se puede observar como a diferencia de las vulnerabilidades del anterior subdominio, presenta otras vulnerabilidades como es la divulgación de información en comentarios sospechosos, así como los diferentes contenidos almacenables y no almacenables en cache que son de tipo informativo pero que comprende un número elevado de instancias en dichas vulnerabilidades.

Tabla 3.30 Vulnerabilidades Detectadas Dominio 15 (OWASP ZAP)

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Encabezado de política de seguridad de contenido (CSP) no establecido	Medio	18
Encabezado X-Frame-Options no establecido	Medio	12
Cookie sin atributo SameSite	Bajo	5
Cabecera de política de funciones no establecida	Bajo	18
Conjunto de encabezado HTTP Pragma incompleto o sin control de caché	Bajo	19

Aislamiento insuficiente del sitio frente a la vulnerabilidad de Spectre	Bajo	47
Información de versión de fugas de servidor a través del campo de encabezado de respuesta HTTP "Servidor"	Bajo	40
Cabecera de seguridad de transporte estricta no establecida	Bajo	34
Falta el encabezado X-Content-Type-Options	Bajo	23
Divulgación Base64	Informativo	7
Divulgación de información: comentarios sospechosos	Informativo	2
Contenido no almacenable	Informativo	6
Contenido almacenable en caché	Informativo	27
Contenido almacenable pero no almacenable en caché	Informativo	7
Divulgación de marca de tiempo - Unix	Informativo	7
Fuzzer de agente de usuario	Informativo	21

Servidor 5 (52.112.64.140)

- **s***.bioalimentar.com**

En el análisis realizado al último servidor que se muestra en la Tabla 3.31, se puede observar que es el servidor que menos vulnerabilidades posee, además de que los niveles de riesgo son bajo e informativo.

Tabla 3.31 Vulnerabilidades Detectadas Dominio 16 (OWASP ZAP)

Elaborado por: Investigador.

Vulnerabilidad	Nivel de Riesgo	Instancias
Aislamiento insuficiente del sitio frente a la vulnerabilidad de Spectre	Bajo	18
Información de versión de fugas de servidor a través del campo de encabezado de respuesta HTTP "Servidor"	Bajo	17
Cabecera de seguridad de transporte estricta no establecida	Bajo	18
Falta el encabezado X-Content-Type-Options	Bajo	18
Divulgación Base64	Informativo	17
Contenido no almacenable	Informativo	1
Obtenido de caché	Informativo	17
Contenido almacenable en caché	Informativo	18
Divulgación de marca de tiempo - Unix	Informativo	23

Mediante los análisis realizados para conocer el estado actual de la empresa y las vulnerabilidades presentes en la misma, mediante el uso de diferentes herramientas como son: Maltego, Anubis, TheHarvester, Sublister, Zenmap, InsightVM y OWASP

ZAP. Se obtuvo bastante información que ayudo a corroborar que aspectos son necesarios tener en cuenta, cuáles son los riesgo críticos presentes en la empresa en cuanto a la seguridad informática, entre otros; con toda la información obtenida se puede tener una visión más clara de que aspectos son necesarios tener en cuenta al momento de desarrollar las políticas de seguridad informática que ayuden a reducir los riesgo y amenazas en la empresa, además que contribuyan al desarrollo adecuado del teletrabajo sin comprometer la integridad de la empresa.

Mediante el análisis realizado con las diferentes herramientas se puede resumir las vulnerabilidades críticas y de suma importancia que son necesarias tener en cuenta al momento de la realización de las políticas de seguridad informática, las cuales se muestran en la Tabla 3.32.

Tabla 3.32 Resumen de Vulnerabilidades Críticas.

Elaborado por: Investigador.

Vulnerabilidad
Credenciales IMAP transmitidas sin cifrar.
Credenciales FTP transmitidas sin cifrar.
Credenciales POP transmitidas sin cifrar.
Acceso abierto a la base de datos.
Ataques SSH Birthday en cifrados de bloque de 64 bits (SWEET32).
Vulnerabilidad de PHP: CVE-2015-4599.
Instalación predeterminada de Apache / página de bienvenida instalada.

Un aspecto a tener en cuenta muy importante en el ámbito de la seguridad informática es el eslabón más débil de todo sistema informático, que son las personas, esto se debe en cierta medida a cómo se comportan las personas y la psicología de las mismas, debido a esto muchos atacantes se aprovechan de esto para obtener información confidencial como: tarjetas de crédito, cuentas de redes sociales, datos sensibles de una empresa, entre otras; todas con un fin, verse beneficiados de algún modo con dicha información y llegar a cumplir sus objetivos; una estrategia muy utilizada para aprovecharse de las personas es la Ingeniería Social en la cual el atacante usa comúnmente un teléfono o Internet para engañar a la víctima, fingiendo ser un empleado de un banco, un empleado de otra empresa, un compañero de trabajo, personal de servicio técnico, entre otras. En Internet a menudo se emplea un envió de solicitudes falsas de renovación de permisos de acceso a la página web, actualización de sistemas, antivirus, programas, además de aprovechar tendencias naturales de la gente a reaccionar de manera predecible en ciertas situaciones [42, 43].

Los procesos para llevar acabo un ataque de Ingeniería Social se basa básicamente en los siguientes pasos [43]:

1. **Identificación de la víctima.**

   En este paso se identifica la psicología de la víctima, y de ser necesario se convierte en una persona muy distinta a fin de agradar y de tener confianza con la victima para con ello poder obtener la información deseada por el atacante.

2. **Fase de reconocimiento.**

   Se obtiene toda la información posible de la víctima, ya sea mediante sitios web, base de datos, redes sociales, grupos de noticias, socios de negocios, telefónicamente o mediante el uso de herramientas informáticas.

3. **Creación del escenario.**

   Una vez estudiado cuidadosamente el objetivo, es necesario la creación de un posible escenario en el cual el principal participante será la víctima y el atacante. Esta es la fase más importante ya que en esta, se llevará el ataque en sí, y en la cual todos los principios antes expuestos serán cuidadosamente elaborados para engañar a la víctima.

4. **Ejecución del ataque.**

   En esta parte el atacante lleva acabo el ataque con calma y confianza, con el fin de obtener la información que busca. Para ello es necesario conocer de antemano toda la información necesaria para llevar acabo el ataque sin dejar rastros.

5. **Salida.**

   Finalmente se debe salir eliminando todo tipo de huellas, de modo que no quede evidencias de quien estuvo.

Conociendo que el eslabón más débil son las personas, se emplea Ingeniería Social para observar cómo es la reacción del personal de la empresa ante un ataque de phishing en el cual mediante el análisis previo realizado con las herramientas, se obtuvo información que será empleada para convencer al personal que la información es legítima y que accedan a un enlace adjunto, el cual redirecciona a una página que aparenta ser de Office 365, pero en realidad no lo es, si no que, lo que realiza la página al momento de ingresar es obtener la dirección IP de las personas que ingresaron y la fecha y posterior a ello las almacena en una base de datos.

Figura 3.41: Página Creada para Ataque de Phishing.

Elaborado por: Investigador.

En la Figura 3.41 se observa la página creada para el ataque, la cual contiene contenido de la página oficial de Office 365 Enterprise para hacerla más creíble, de igual amanera contiene las imágenes de la página oficial de Microsoft y Office.

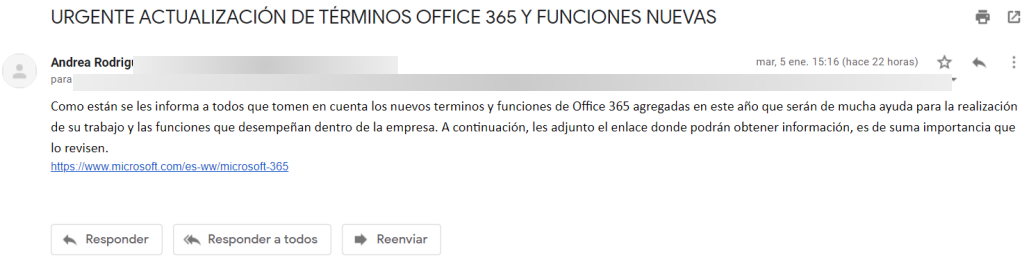
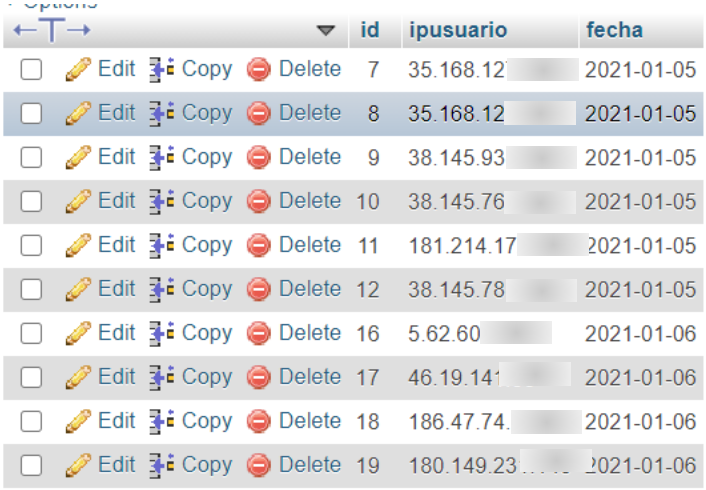


Figura 3.42: Correo Enviado al Personal de la Empresa.

Elaborado por: Investigador.

En la Figura 3.42 se observa el correo enviado al personal de la empresa en donde se especifica que es de suma importancia que ingresen y revisen la información ya que Office 365 actualizó sus términos y además contiene nuevas funciones por lo que se les solicita que accedan al enlace para obtener información.



	id	ipusuario	fecha
Edit Copy Delete	7	35.168.12	2021-01-05
Edit Copy Delete	8	35.168.12	2021-01-05
Edit Copy Delete	9	38.145.93	2021-01-05
Edit Copy Delete	10	38.145.76	2021-01-05
Edit Copy Delete	11	181.214.17	2021-01-05
Edit Copy Delete	12	38.145.78	2021-01-05
Edit Copy Delete	16	5.62.60	2021-01-06
Edit Copy Delete	17	46.19.141	2021-01-06
Edit Copy Delete	18	186.47.74.	2021-01-06
Edit Copy Delete	19	180.149.23	2021-01-06

Figura 3.43: Direcciones IPs y Fecha de Ingreso.

Elaborado por: Investigador.

En la Figura 3.43 se observa las direcciones IPs de los empleados que accedieron al enlace y la fecha.

Resultados de Ataque

En la Figura 3.44 se puede observar que de un total de 50 empleados a los que se les envió el correo electrónico para la realización del ataque de ingeniería social, 10 empleados (20%) fueron víctimas del ataque, mientras que 40 empleados (80%) no fueron víctimas del ataque al no ingresar al enlace en el correo adjunto. Lo que muestra un gran déficit en conocimientos de seguridad informática y en este tipo de ataques, con lo cual es de suma importancia educar al personal de la empresa ante posibles ataques; como el realizado, y otros, para que no sean víctimas de este tipo de engaños que pueden repercutir seriamente en la empresa, teniendo en cuenta que si hubiera sido un ataque real en el cual un ciber atacante instale algún tipo de malware o que obtenga acceso a cierto tipo de información Bancaria o Empresarial la empresa hubiera tenido serias repercusiones.

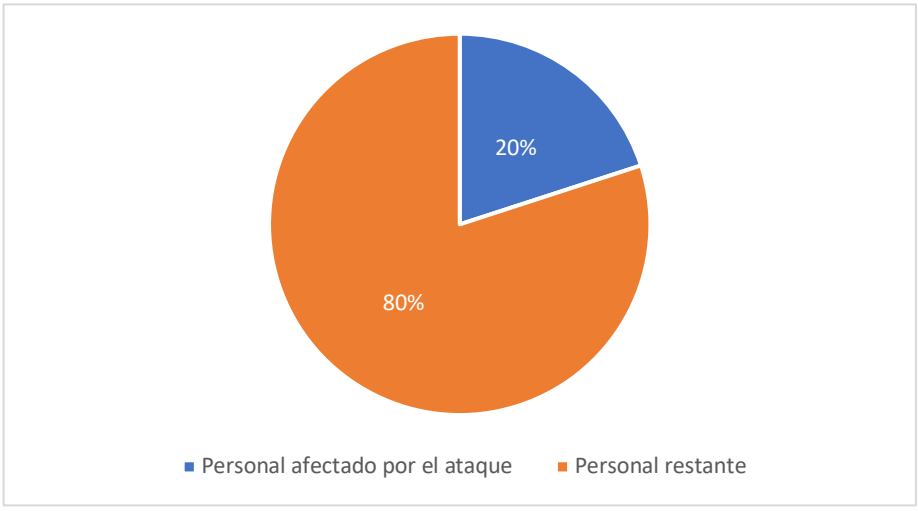


Figura 3.44: Resultados de Ataque de Phishing

Elaborado por: Investigador

3.1.4. Desarrollo de Políticas de Seguridad Informática

Una vez realizado un análisis de la situación actual de la empresa mediante la entrevista y encuestas realizadas al personal de la empresa, así como la información obtenida mediante el uso de las diferentes herramientas y técnicas; es necesario analizar la parte legal en el ecuador; para ello se analizó el proyecto presentado por el gobierno ecuatoriano, la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal) del cual se tomaron ciertas partes muy importantes para la realización del presente proyecto.

Una vez analizada la parte legal como es el Cogido Penal, el Código de Trabajo, los Delitos Informáticos contemplado en la parte legal y la LOPD, se tomaron como base los siguientes artículos:

Artículo 66, numeral 19: Establece el derecho a la protección de datos de carácter personal y la autorización requerida del titular o el mandato de la ley.

Artículo 92: Toda persona tiene derecho a conocer de la existencia de los datos además de poder acceder a los documentos y conocer el uso que se haga de ellos.

Artículo 9. Juridicidad, lealtad y transparencia: Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones. No deben ser tratados para fines ilícitos o desleales.

Artículo 18. Seguridad de datos personales: Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias frente a cualquier riesgo, amenaza, vulnerabilidad, acceso no autorizado, perdidas, etc.

Artículo 50. Seguridad de datos personales: Se deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la efectividad, eficiencia, eficacia de las medidas implementadas con el objetivo de garantizar y mejorar la seguridad.

Entre otras medidas se puede incluir las medidas de anonimización, encriptación, cifrado o codificación de los datos personales; de igual manera medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanente de los sistemas y servicios, entre otros.

Artículo 51. Medidas de seguridad en el ámbito del sector público: La seguridad de la información incluirá las medidas que deban implementarse para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, acceso no autorizado, entre otros.

Artículo 55. Notificación de vulneración de seguridad: EL responsable del tratamiento debe notificar la vulneración a la Autoridad de Protección de Datos Personales dentro del término de tres días a partir del conocimiento de la vulneración. El encargado del tratamiento deberá notificar la vulneración en un término no mayor a dos días después de tener conocimiento de ella.

En caso de retraso del responsable o del encargado del tratamiento en la notificación de la vulneración de seguridad se le aplicaran las sanciones correspondientes conforme a lo establecido en la ley.

Artículo 71. Obligaciones del responsable del tratamiento de datos personales: Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular. Adherirse a mecanismos de certificación, códigos de protección o sellos de protección de datos personales aprobados por la Autoridad de Protección de Datos Personales. Realizar evaluaciones de adecuaciones a nivel de seguridad previas al tratamiento de datos personales.

Para más información sobre las leyes empleadas para la realización de las políticas, ver el detalle en el Anexo B.

Teniendo en cuenta todo lo analizado previamente se procede al desarrollo de políticas de seguridad informáticas acordes a las necesidades de la empresa con el fin de garantizar la protección de los activos de la empresa, así como a la integridad de la misma, además de mitigar o minimizar el impacto de los riesgos identificados en la empresa.

Las políticas estarán dirigidas a todo el personal de la empresa, y en las cuales cada departamento tendrá un papel muy importante dentro del desarrollo de las políticas ya sea desde los altos funcionarios para su aprobación, el departamento de comunicación para divulgación, así como el departamento de TI para brindar apoyo en el área tecnológica.

La estructura de las políticas consta de la siguiente manera:

1. **Información General**
2. **Propósito**
3. **Alcance**
4. **Políticas**
5. **Excepciones**
6. **Incumplimiento**
7. **Información Relacionada (Estándares, Políticas, Procesos, Otros)**
8. **Revisión Histórica**

Las políticas desarrolladas que fueron aprobadas y entregadas a la empresa Bioalimentar son:

1. Configuraciones Básicas de Seguridad Informática

Está diseñada para ayudar a los empleados, socios y a la compañía en general a tener una mejor seguridad al momento de la realización de sus actividades diarias, garantizando la seguridad y la integridad tanto del personal de la empresa como de los activos de la empresa. La realización de teletrabajo puede suponer una vulnerabilidad para la empresa si no se tienen en cuenta ciertas configuraciones básicas antes de la realización del teletrabajo como puede ser: la configuración adecuada del Router, el proveedor de Internet, antivirus y sistemas operativos desactualizados, inexistencia de

copias de seguridad de activos críticos, etcétera. Ver Anexo C, Configuraciones Básicas de Seguridad Informática.

2. Estándar de Comunicación Inalámbrica

En la política de comunicación inalámbrica se especifica los diferentes requisitos que deben cumplir las comunicaciones inalámbricas para garantizar la seguridad y que no exista ningún tipo de filtrado de información o que se llegue a comprometer la seguridad de la empresa. Ver Anexo C, Estándar de comunicación inalámbrica.

3. Directrices para la Creación de Contraseñas Robustas

El propósito es proporcionar las mejores prácticas para la creación de contraseñas robustas que cumplan con ciertos estándares. Ver Anexo C, Directrices para la Creación de Contraseñas Robustas.

4. Política de Uso Aceptable

La política de uso aceptable está diseñada con el fin de describir el uso aceptable de equipos informáticos mediante reglas que están en vigor para proteger al empleado y a la empresa ya que el uso inadecuado podría exponer a la empresa a riesgos que incluyen ataques de virus, compromiso de los sistemas y servicios de red así como problemas legales. Ver Anexo C, Política de Uso Aceptable.

5. Directrices para Antivirus

Se plantea una serie de directrices con el fin de presentar al personal de la empresa como se puede reducir la infección de dispositivos informáticos de algún tipo de malware, y la concienciación de cuán importante es la presencia de un antivirus en los dispositivos informáticos, además de que se encuentren actualizados y en correcto funcionamiento. Ver Anexo C, Directrices para Antivirus.

6. Política de Escritorio Limpio

La política de escritorio limpio establece los requisitos mínimos para mantener un "escritorio limpio", donde la información sensible y crítica de la empresa esté segura en áreas bloqueadas y fuera del sitio. Una política de escritorio limpio no solo cumple con la norma ISO 27001/17799, sino que también forma parte de los controles de privacidad básicos de ciertos estándares. Ver Anexo C, Política de Escritorio Limpio.

7. Política de Filtrado y Supervisión del Uso de Internet

Se definen estándares para los sistemas que monitorean y limitan el uso de la web desde cualquier host dentro de la red de la empresa. Estos estándares están diseñados para garantizar que los empleados usen Internet de manera segura y responsable, y garantizar que el uso de la web por parte de los empleados se pueda monitorear o investigar en caso de que suceda un incidente. Ver Anexo C, Política de Filtrado y Supervisión del Uso de Internet.

8. Política de Protección de Claves

Mediante la política de protección de claves se busca describir los requisitos para proteger las claves que están bajo el control de los usuarios. Estos requisitos están diseñados para evitar la divulgación no autorizada y el posterior uso fraudulento. Los métodos de protección descritos incluyen controles operativos y técnicos, como procedimientos de copia de seguridad de claves, cifrado con una clave separada y uso de hardware resistente a la manipulación. Ver Anexo C, Política de Protección de Claves.

9. Política de Cifrado de Dispositivos Móviles

Se describen los requisitos de seguridad de la información para cifrar datos en los dispositivos móviles. Ver Anexo C, Política de Cifrado de Dispositivos Móviles.

10. Política de Acceso Remoto

El propósito de la política es definir reglas y requisitos para conectarse a la red de la empresa desde cualquier host. Estas reglas y requisitos están diseñados para minimizar en lo posible la exposición a la empresa por daños que puedan resultar del uso no autorizado de los recursos de la empresa. Los daños incluyen la pérdida de datos sensibles o confidenciales de la empresa, propiedad intelectual, daños a la imagen pública, daños a los sistemas internos críticos de la empresa y multas u otras responsabilidades financieras incurridas como resultado de esas pérdidas. Ver Anexo C, Política de Acceso Remoto.

11. Política de Herramientas de Acceso Remoto

Se define los requisitos para el uso de herramientas de acceso remoto utilizadas en la empresa. Ver Anexo C, Política de Herramientas de Acceso Remoto.

12. Política de Seguridad del Servidor

Mediante la política de seguridad del servidor se pretende establecer estándares para la configuración básica del equipo de servidor interno que es propiedad de la empresa o es operado por ella. La implementación efectiva de esta política minimizará el acceso no autorizado a la información y tecnología que es propiedad de la empresa. Ver Anexo C, Política de Seguridad del Servidor.

13. Política Sobre Ingeniería Social

Se pretende informar y capacitar a los empleados sobre las diferentes técnicas y ataques que ocurren de ingeniería social y que además existen procedimientos que los empleados pueden usar para detectar las diferentes técnicas y ataques utilizados. Ver Anexo C, Política Sobre Ingeniería Social.

14. Política de Instalación de Software

La política de instalación de software pretende describir los requisitos relacionados con la instalación del software en dispositivos informáticos que son propiedad de la empresa. Para minimizar el riesgo de pérdida de la funcionalidad del programa, la exposición de información confidencial contenida dentro de la red informática de la empresa, el riesgo de introducir malware y la exposición legal de ejecutar software sin licencia. Ver Anexo C, Política de Instalación de Software.

15. Política de Red Privada Virtual (VPN)

El propósito de esta política es proporcionar pautas para las conexiones de red privada virtual (VPN) IPSec o L2TP de acceso remoto a la red corporativa de la empresa. Ver Anexo C, Política de Red Privada Virtual (VPN).

3.1.4. Validación de Políticas Mediante Hacking Ético

Una vez desarrolladas las políticas y revisadas por la empresa se procede a validar las políticas creadas, para ello se emplea técnicas de hacking ético para corroborar la eficiencia de las políticas, cabe recalcar que al ser políticas de teletrabajo y al encontrarse el personal laborando en sus domicilios las técnicas más eficientes corresponden a la ingeniería social.

Para ello se realiza una clonación del sitio web de Bioalimentar de ingreso de cierto personal de la empresa y se monta en un servidor gratuito como se puede observar en la Figura 3.45 y Figura 3.46. Se realiza un ataque mediante correo electrónico y otro mediante WhatsApp para que ingresen a un enlace en donde podrán actualizar sus credenciales del sistema. Una vez que ingresen sus credenciales estas serán almacenadas en una Base de Datos y posterior a ello se redireccionara al sitio web verdadero.

Figura 3.45: Web Verdadera.

Elaborado por: Investigador.

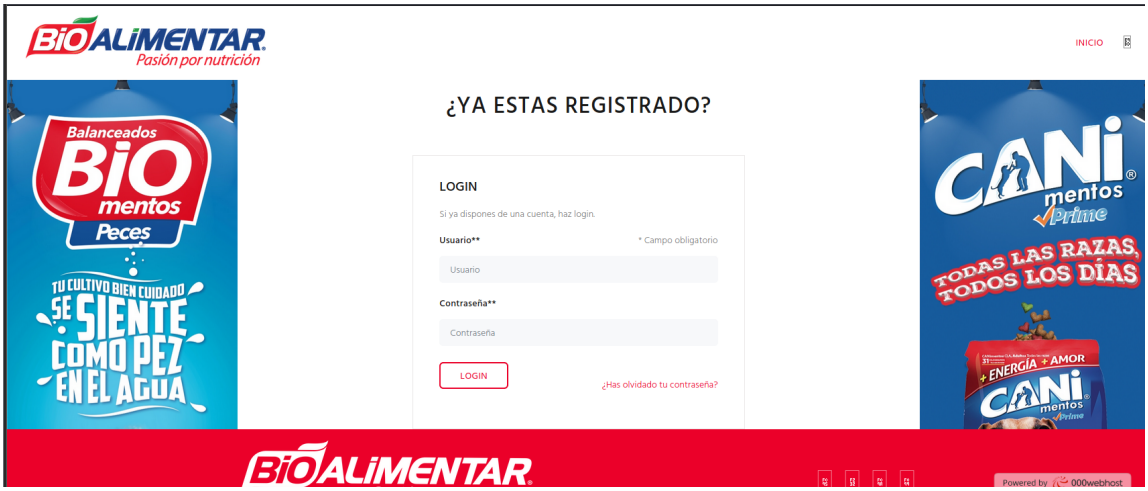


Figura 3.46: Web Falsa.

Elaborado por: Investigador.

En la Figura 3.47 se puede observar el email enviado al personal de Bioalimentar para el ataque, mientras que en la Figura 3.48 se observa los datos obtenidos en el ataque; en este caso solo existe un único dato que es el de prueba; en el ataque se observa que nadie ingresa al enlace por ende no existe ninguna credencial almacenada. Esto sucede debido a la socialización realizada sobre las políticas de seguridad informática en el teletrabajo donde se pudieron analizar diferentes casos de ataques realizados en los 2 últimos años y como prevenir dichos ataques.

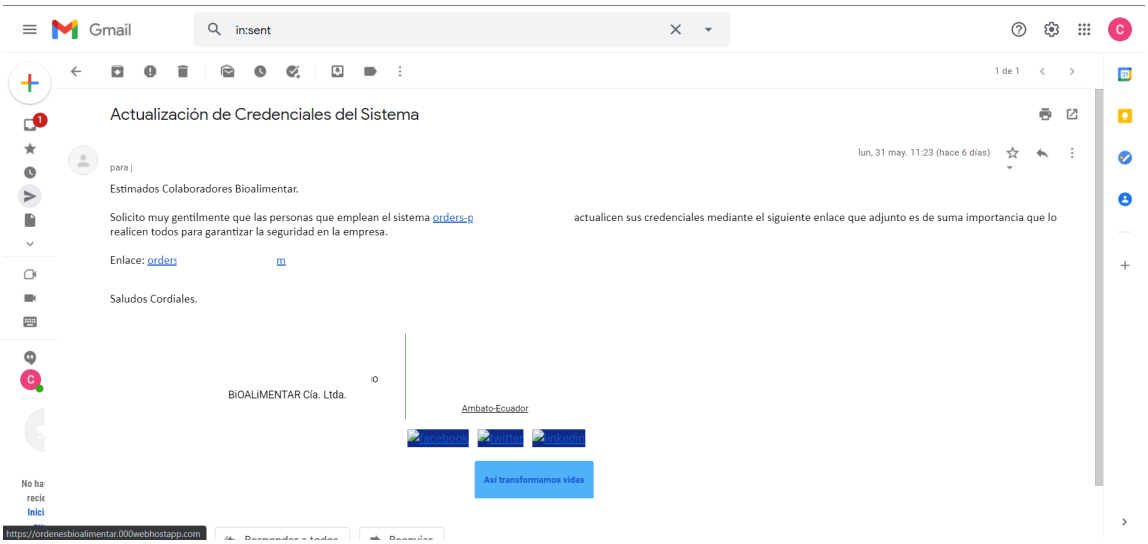


Figura 3.47: Correo Enviado.

Elaborado por: Investigador.

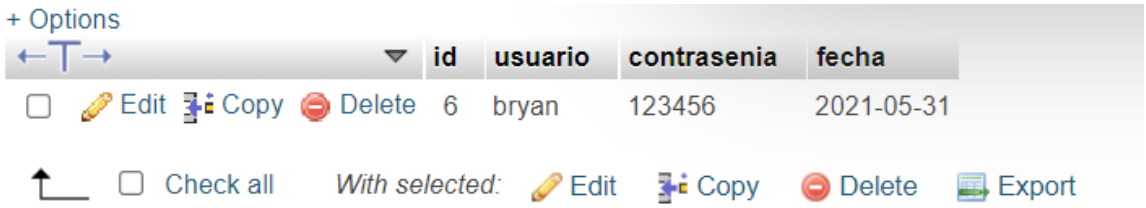


Figura 3.48: Base de Datos de Página Clonada de Bioalimentar.

Elaborado por: Investigador.

En el ataque realizado mediante WhatsApp se suplanto la identidad de un colaborador de la empresa el cual posee un cargo en el departamento de TI, el mensaje fue enviado a 5 colaboradores de la empresa; cómo se puede observar en la Figura 3.49, Figura 3.50 y Figura3.51.

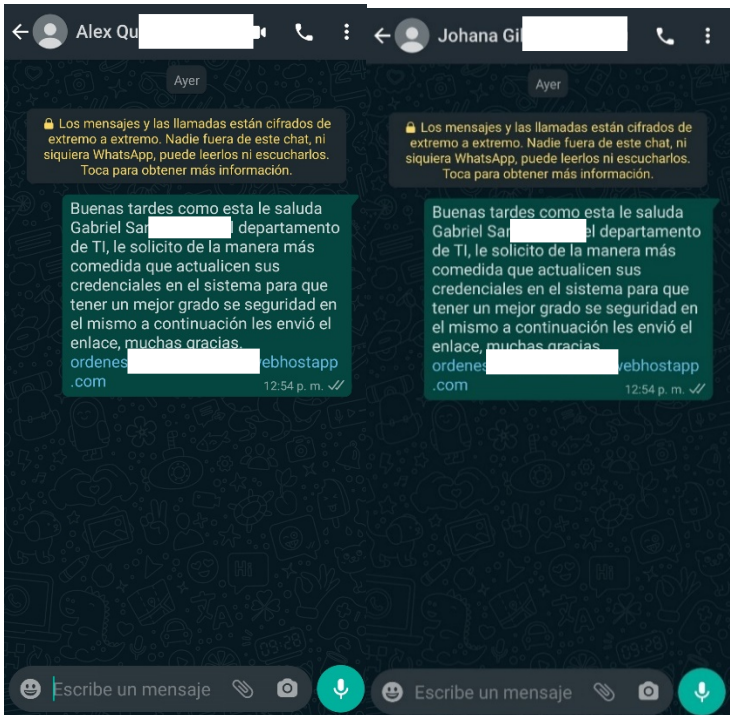


Figura 3.49: Colaborador de Biolimentar 1 y 2.

Elaborado por: Investigador.

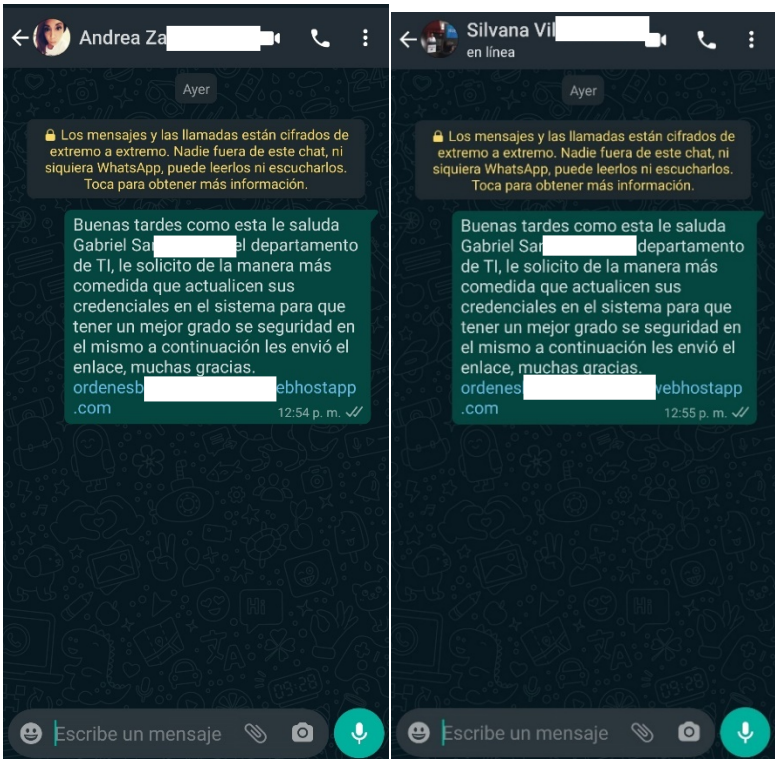


Figura 3.50: Colaborador de Biolimentar 3 y 4.

Elaborado por: Investigador.

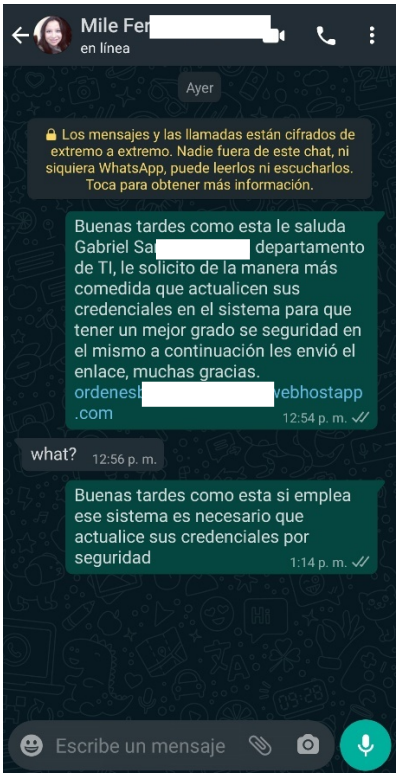


Figura 3.51: Colaborador de Biolimentar 5.

Elaborado por: Investigador.

Resultados de Ataque

Correo Electrónico

En la Figura 3.52 se puede observar que de un total de 50 empleados a los que se les envió el correo electrónico para la realización del ataque de ingeniería social, 50 empleados (100%) no fueron víctimas del ataque realizado.

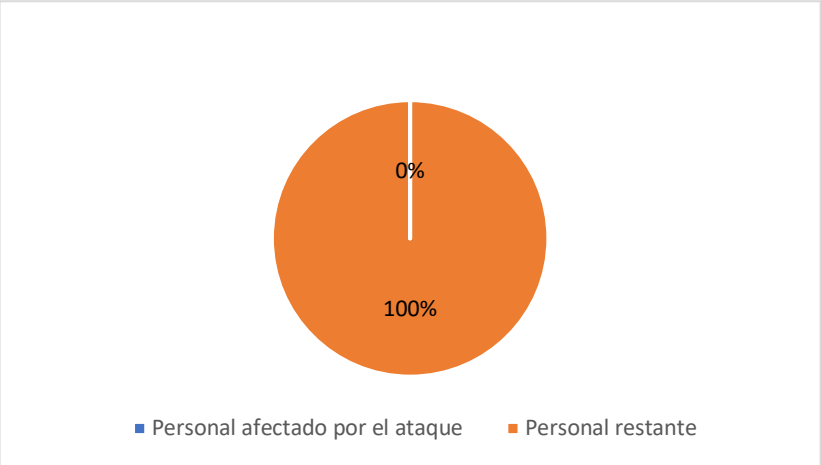


Figura 3.52: Resultados Ataque Correo Electrónico.

Elaborado por: Investigador.

WhatsApp

En la Figura 3.53 se puede observar que de un total de 5 empleados a los que se les envió el correo electrónico para la realización del ataque de ingeniería social, 5 empleados (100%) no fueron víctimas del ataque realizado.

Figura 3.53: Resultados Ataque WhatsApp.

Elaborado por: Investigador.

De los resultados obtenidos se puede evidenciar que una vez difundidas las políticas que se encuentran en el Anexo C en la empresa Bioalimentar el personal que labora en la empresa ya no fue víctima de ningún ataque realizado, debido a que se socializo las políticas con los colaboradores de la empresa y se les capacito en el tema de seguridad informática con lo cual se mejoró la seguridad en la empresa y se confirmó la importancia de la seguridad y la capacitación del personal en el ámbito de la seguridad.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- Los activos más valiosos para una empresa es la información que posee por ende es importante la seguridad en el manejo y el uso de la misma, por ello es de suma importancia contar con políticas de seguridad informáticas las cuales sirvan para una mejor seguridad y garantizar la continuidad del negocio.

- En el estudio del estado actual de la empresa se pudo observar que es una empresa muy grande que maneja gran cantidad de información que es de suma importancia por lo que es sumamente necesario contar con un nivel de seguridad alto en el que se garantice la confidencialidad, la disponibilidad e integridad de la información; pero al no tener políticas de seguridad informáticas bien definidas de fácil acceso al personal, se complica garantizar la seguridad dentro de la empresa.

- Mediante el uso de herramientas de pago como de uso libre se puede evidenciar ciertos problemas en cuanto a la seguridad, debido a la presencia de vulnerabilidades en ciertos servidores de la empresa, así como la información del personal que labora en la empresa; basados en la información obtenida, se elaboró una propuesta de políticas de seguridad informática que ayuden a tener un mejor nivel de seguridad.

- La aplicación de ingeniería social permitió comprobar que el ser humano es el eslabón más débil de la cadena y del cual se aprovechan los atacantes para obtener información que les permita llegar a su objetivo. Además, se pudo comprobar que el personal que labora en la empresa no tiene los conocimientos básicos sobre que es la ingeniería social y de igual manera los tipos de ataques que existen; por lo que se tomó en cuenta para el desarrollo de las políticas la capacitación del personal en el tema informático y la seguridad.

- El desarrollo de políticas de seguridad mediante la implementación de diferentes estándares y normas como son la ISO 27001, NIST; permitieron obtener políticas de seguridad acordes a las necesidades de la empresa y acordes al estado en el que se encontraba la empresa, llegando con ello a tener una mejor seguridad en las actividades que realiza el personal que la labora en la empresa tanto dentro de la misma como fuera de ella al momento de realizar teletrabajo.

- El uso de técnicas de Hacking Ético permitió comprobar que las políticas desarrolladas en la parte de la seguridad informática para el teletrabajo fueron las adecuadas ya que se pudo cumplir con todos los objetivos planteados además de que se pudo observar la valía de las mimas mediante los resultados obtenidos en los ataques realizados donde el personal de la empresa mostro un grado de seguridad elevado.

4.2. Recomendaciones

- Se debe concientizar y educar al personal sobre la importancia de la seguridad informática para con ello lograr que se sigan las políticas que se definieron en el presente documento con el fin de garantizar una seguridad óptima en la empresa, así como la seguridad del propio personal.

- Se recomienda el uso de sistemas que ayuden a la detección de intrusos (IDS) así como de sistemas de prevención de intrusos (IPS) con el fin de garantizar la continuidad del negocio y detectar posibles ataques informático.

- Se recomienda que se realice análisis periódicos para poder observar el estado de la empresa mediante el uso de herramientas actualizadas que sirvan para la detección de problemas y vulnerabilidades presentes en la empresa con el fin de poder reducirlos y mitigarlos.

- Se sugiere que al personal que va a realizar teletrabajo o realiza teletrabajo se le imparta una charla sobre las medidas de seguridad informática que debe tener en cuenta al realizar las actividades mediante teletrabajo, así como los peligros que encuentra expuesta la información de la empresa, así como la propia persona que realiza teletrabajo.

Bibliografía

[1] J. Peiró and A. Soler, "El impulso al teletrabajo durante el covid-19 y los retos que plantea," pp. 1–10, 2020.

[2] D. Martín and B. Botero, "Teletrabajo: una oportunidad en tiempos de crisis," *CES Derecho*, vol. 11, no. 1, pp. 1–2, 2020, [Online]. Available: http://revistas.ces.edu.co/index.php/derecho/article/view/5620/3161.

[3] F. Arteaga, "Ciberseguridad en tiempos de pandemia: repaso a la covid 19," *Ciberseguridad*, pp. 1–7, 2020, [Online]. Available: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEX T=/elcano/elcano_es/zonas_es/ciberseguridad/ari67-2020-arteaga-ciberseguridad-en-tiempos- de-pandemia-repaso-a-covid-19.

[4] ESET LLC, "ESET SECURITY REPORT Latinoamerica 2019," 2019, [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf.

[5] M. de trabajo Ecuador, "Plan para el retorno paulatino al trabajo 23/04/2020," 2020.

[6] Á. Gómez Vieites, "Directrices Para La Definición E Implantación De Políticas De Seguridad," [Online]. Available: http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Politicas__planes_y_procedimientos_de_seguridad.pdf.

[7] J. M. Kizza, *Computer Network Security Fundamentals*. 2017.

[8] M. C. Cintia and Q. Reyes, "Mecanismos de seguridad," [Online]. Available: http://profesores.fi-b.unam.mx/cintia/Mecanismos.pdf.

[9] A. L. Lorena, "Seguridad informática y seguridad de la información."

[10] Á. Gómez Vieites, "Enciclopedia de la Seguridad Informatica." p. 696, 2007, [Online]. Available: http://www.casadellibro.com/libro-enciclopedia-de-la-seguridad-informatica/9788478977314/1109334.

[11] W. Qiu, S. Rutherford, A. Mao, and C. Chu, "The Pandemic and its Impacts," *Heal. Cult. Soc.*, vol. 9, pp. 1–11, 2017, doi: 10.5195/hcs.2017.221.

[12] E. Castro Marquez, "La economía : conceptos y problemas fundamentales," vol. 2, p. 24, 2011, [Online]. Available: http://novella.mhhe.com/sites/dl/free/8448160991/610259/8448160991_Cap1.pdf.

[13] M. Patricia, R. Caraballo, and D. Ph, "Significado del trabajo desde la psicología del trabajo. Una revisión histórica, psicológica y social," *Psicol. desde el Caribe*, vol. 34, no. 2, pp. 120–138, 2017, doi: 10.14482/psdc.33.2.72783.

[14] Organización internacional del trabajo, "Manual de buenas practicas en el teletrbajo," p. 400, 2011, [Online]. Available: https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---ilo-

buenos_aires/documents/publication/wcms_bai_pub_143.pdf.

[15] “What is Cyber Security? | Definition, Types, and User Protection | Kaspersky.” https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (accessed Dec. 11, 2020).

[16] “What is Cybersecurity? Defined, Explained, and Explored | Forcepoint.” https://www.forcepoint.com/cyber-edu/cybersecurity (accessed Dec. 11, 2020).

[17] E. D. O. Andrade, J. Viterbo, C. N. Vasconcelos, J. Guérin, and F. C. Bernardini, “A model based on LSTM neural networks to identify five different types of malware,” *Procedia Comput. Sci.*, vol. 159, pp. 182–191, 2019, doi: 10.1016/j.procs.2019.09.173.

[18] Y. Diogenes, *Cybersecurity: Attack and Defense Strategies*. 2018.

[19] F. Maggi, M. Balduzzi, R. Flores, L. Gu, and V. Ciancaglini, “Investigating web defacement campaigns at large,” *ASIACCS 2018 - Proc. 2018 ACM Asia Conf. Comput. Commun. Secur.*, pp. 443–456, 2018, doi: 10.1145/3196494.3196542.

[20] W. C. Easttom, *Computer Security Fundamentals*. 2011.

[21] J. C. Perez, *Proteccion de datos y seguridad de la informacion: guia practica para ciudadanos y empresas (4a. ed.)*. RA-MA Editorial, 2015.

[22] W. STEVE, *An Introduction to Information Security and ISO27001*. .

[23] F. J. Valencia-Duque and M. Orozco-Alzate, “A methodology for implementing an information security management system based on the family of ISO/IEC 27000 standards,” *RISTI - Rev. Ibèrica Sist. e Tecnol. Inf.*, no. 22, pp. 73–88, 2017, doi: 10.17013/risti.22.73-88.

[24] G. Álvarez, *Seguridad informática para empresas y particulares*, vol. 4, no. 1. 2016.

[25] M. L. Jason Andress, *Building a Practical Information Security Program*. 2017.

[26] Bishop Matt, *Computer Security*, vol. 53, no. 9. .

[27] R. Messier, *CEH v10 Study Guide*. 2017.

[28] S. Greene and O. Santos, *Developing Cybersecurity Programs and Policies*. 2018.

[29] M. Greegg and B. Haines, *CASP CompTIA Advanced Security Practitioner Study Guide*, vol. 53, no. 9. 2019.

[30] B. L. Williams, *Information Security Policy Development for Compliance*. .

[31] E. C. Thompson, *Cybersecurity Incident Response, How to Contain, Eradicate, and Recover from Incidents*. 2018.

[32] M. E. Whitman and H. J. Mattord, *Principles of Information Security, Sixth Edition*. 2018.

[33] J. AREITIO, *Seguridad de la información. Redes, informática y sistemas de información*. 2008.

[34] N. Técnica, "Norma Técnica Ntc-Iso/Iec Colombiana 27001," 2006, [Online]. Available: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma. NTC-ISO-IEC 27001.pdf.

[35] ICONTEC, "Norma Técnica NTC-ISO/IEC 27002," no. 571, p. 133, 2007.

[36] G. Johansen, L. Allen, T. Heriyanto, and S. Ali, *Kali Linux 2 – Assuring Security by Penetration Testing*. 2016.

[37] "Anubis: Subdomain enumeration and information gathering tool – Cyber Security." https://www.prodefence.org/anubis-subdomain-enumeration-and-information-gathering-tool/ (accessed Dec. 30, 2020).

[38] "Sublist3r | Herramientas de prueba de penetración." https://tools.kali.org/information-gathering/sublist3r (accessed Dec. 30, 2020).

[39] "Zenmap - GUI oficial del escáner de seguridad Nmap multiplataforma." https://nmap.org/zenmap/ (accessed Dec. 31, 2020).

[40] "Rapid7 InsightVM Vulnerability Management." https://www.rapid7.com/info/introducing-insightvm/ (accessed Jan. 02, 2021).

[41] "OWASP ZAP." https://www.zaproxy.org/ (accessed Jan. 02, 2021).

[42] A. Roger, *Hacking the Hacker*. 2554.

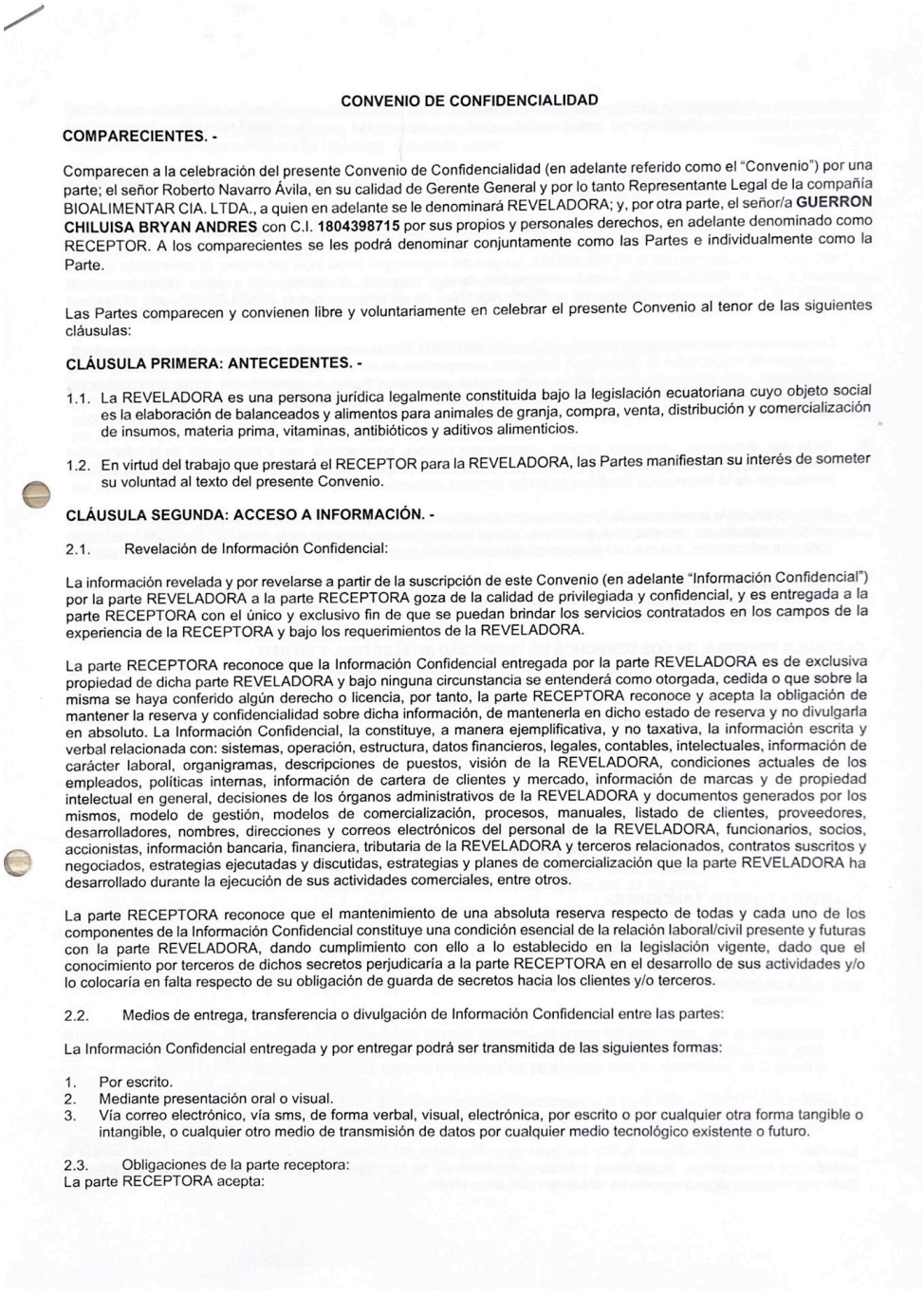
[43] D. Arboledas, *BackTrack 5 Hacking de redes inalambricas*. .

[44] Asamblea Nacional del Ecuador proteccion, "Proyecto de ley organica de protección de datos." p. 52, 2019.

ANEXOS

Anexo A

Convenio de Confidencialidad



CONVENIO DE CONFIDENCIALIDAD

COMPARECIENTES. -

Comparecen a la celebración del presente Convenio de Confidencialidad (en adelante referido como el "Convenio") por una parte; el señor Roberto Navarro Ávila, en su calidad de Gerente General y por lo tanto Representante Legal de la compañía BIOALIMENTAR CIA. LTDA., a quien en adelante se le denominará REVELADORA; y, por otra parte, el señor/a **GUERRON CHILUISA BRYAN ANDRES** con C.I. **1804398715** por sus propios y personales derechos, en adelante denominado como RECEPTOR. A los comparecientes se les podrá denominar conjuntamente como las Partes e individualmente como la Parte.

Las Partes comparecen y convienen libre y voluntariamente en celebrar el presente Convenio al tenor de las siguientes cláusulas:

CLÁUSULA PRIMERA: ANTECEDENTES. -

1.1. La REVELADORA es una persona jurídica legalmente constituida bajo la legislación ecuatoriana cuyo objeto social es la elaboración de balanceados y alimentos para animales de granja, compra, venta, distribución y comercialización de insumos, materia prima, vitaminas, antibióticos y aditivos alimenticios.

1.2. En virtud del trabajo que prestará el RECEPTOR para la REVELADORA, las Partes manifiestan su interés de someter su voluntad al texto del presente Convenio.

CLÁUSULA SEGUNDA: ACCESO A INFORMACIÓN. -

2.1. Revelación de Información Confidencial:

La información revelada y por revelarse a partir de la suscripción de este Convenio (en adelante "Información Confidencial") por la parte REVELADORA a la parte RECEPTORA goza de la calidad de privilegiada y confidencial, y es entregada a la parte RECEPTORA con el único y exclusivo fin de que se puedan brindar los servicios contratados en los campos de la experiencia de la RECEPTORA y bajo los requerimientos de la REVELADORA.

La parte RECEPTORA reconoce que la Información Confidencial entregada por la parte REVELADORA es de exclusiva propiedad de dicha parte REVELADORA y bajo ninguna circunstancia se entenderá como otorgada, cedida o que sobre la misma se haya conferido algún derecho o licencia, por tanto, la parte RECEPTORA reconoce y acepta la obligación de mantener la reserva y confidencialidad sobre dicha información, de mantenerla en dicho estado de reserva y no divulgarla en absoluto. La Información Confidencial, la constituye, a manera ejemplificativa, y no taxativa, la información escrita y verbal relacionada con: sistemas, operación, estructura, datos financieros, legales, contables, intelectuales, información de carácter laboral, organigramas, descripciones de puestos, visión de la REVELADORA, condiciones actuales de los empleados, políticas internas, información de cartera de clientes y mercado, información de marcas y de propiedad intelectual en general, decisiones de los órganos administrativos de la REVELADORA y documentos generados por los mismos, modelo de gestión, modelos de comercialización, procesos, manuales, listado de clientes, proveedores, desarrolladores, nombres, direcciones y correos electrónicos del personal de la REVELADORA, funcionarios, socios, accionistas, información bancaria, financiera, tributaria de la REVELADORA y terceros relacionados, contratos suscritos y negociados, estrategias ejecutadas y discutidas, estrategias y planes de comercialización que la parte REVELADORA ha desarrollado durante la ejecución de sus actividades comerciales, entre otros.

La parte RECEPTORA reconoce que el mantenimiento de una absoluta reserva respecto de todas y cada uno de los componentes de la Información Confidencial constituye una condición esencial de la relación laboral/civil presente y futuras con la parte REVELADORA, dando cumplimiento con ello a lo establecido en la legislación vigente, dado que el conocimiento por terceros de dichos secretos perjudicaría a la parte RECEPTORA en el desarrollo de sus actividades y/o lo colocaría en falta respecto de su obligación de guarda de secretos hacia los clientes y/o terceros.

2.2. Medios de entrega, transferencia o divulgación de Información Confidencial entre las partes:

La Información Confidencial entregada y por entregar podrá ser transmitida de las siguientes formas:

1. Por escrito.
2. Mediante presentación oral o visual.
3. Vía correo electrónico, vía sms, de forma verbal, visual, electrónica, por escrito o por cualquier otra forma tangible o intangible, o cualquier otro medio de transmisión de datos por cualquier medio tecnológico existente o futuro.

2.3. Obligaciones de la parte receptora:
La parte RECEPTORA acepta:

Figura 4.1: Convenio de Confidencialidad Parte 1.

Elaborado por: Investigador.

1. Respecto a la Información Confidencial, tener el mismo cuidado y discreción que como Receptor tiene para con su propia información clasificada en forma similar cuando ha de evitarse que se revele, publique o disemine esa información.

2. Utilizar la Información Confidencial revelada únicamente con el objetivo de desarrollar su trabajo de acuerdo a su cargo y funciones establecidas por parte de la REVELADORA.

3. No podrá divulgar la información y documentación a la cual tenga acceso en virtud de este Convenio, sin autorización previa de la REVELADORA, en especial, no podrá revelar a terceros lo siguiente: i) información de cualquier naturaleza, relacionada con la REVELADORA, su giro del negocio y el Know How del mismo; ii) información o datos usados por la REVELADORA para la conducción de sus negocios; iii) información y datos obtenidos por el RECEPTOR, que sea de propiedad de la REVELADORA o de un tercero y que la REVELADORA esté obligada a tratar como confidencial.

4. En caso de terminación de la relación laboral, la parte RECEPTORA se compromete a devolver, de manera inmediata, a la parte REVELADORA la información entregada acompañada de un inventario de la información recibida, con la declaración bajo juramento de no haber hecho copias adicionales físicas o digitales. Por tanto, toda utilización posterior, desde ya implica la aceptación expresa de la parte "emisora" de haber generado copias, y por tanto faltar a su declaración bajo juramento, causando así la confesión de parte respecto del cometimiento de delito de perjurio.

5. Todo uso, documento, referencia, acceso, contacto con clientes, proveedores, uso y distribución de la Información Confidencial, y que sea comprobable por cualquier medio, será prueba suficiente para constatar el incumplimiento de destrucción de la Información Confidencial en los términos expuestos en el presente instrumento.

   Sin perjuicio de la terminación de la relación contractual, subsistirán el deber de confidencialidad y las restricciones y prohibiciones de uso respecto del know-how y de toda información de propiedad de la parte REVELADORA, así como toda otra información, a la que se hubiere accedido en virtud de la relación contractual, que no revista carácter público.

6. Las obligaciones contenidas en esta cláusula se extienden a compañías relacionadas, proveedores, trabajadores, administradores, directores, accionistas y familiares de los mismos hasta el tercer grado de consanguinidad, dentro y fuera del territorio ecuatoriano.

CLÁUSULA TERCERA: DE LOS DERECHOS DE PROPIEDAD INTELECTUAL Y SU USO.-

3.1. La parte REVELADORA se abstendrá, de forma enunciativa pero no limitativa, a realizar ingeniería inversa, descompilar, desensamblar, modificar, versionar, comercializar, duplicar, transformar ni transmitir parcialmente o en su totalidad, en forma o por medio alguno, ya sea mecánico, magnético, por fotocopia o cualquier otro medio, la Información Confidencial que llegue a manos de la parte RECEPTORA, sin previa y expresa autorización por escrito de la parte "emisora".

3.2. La Parte RECEPTORA no podrá replicar ni versionar el modelo de negocio, know how, manuales de la parte REVELADORA indefinidamente.

3.3. Las obligaciones contenidas en esta cláusula se extienden a compañías relacionadas, proveedores, empleados, administradores, directores, accionistas y familiares de los mismos hasta el tercer grado de consanguinidad, dentro y fuera del territorio ecuatoriano de ambas Partes.

CLÁUSULA CUARTA: SANCIONES.-

4.1. Sin perjuicio de lo estipulado en esta cláusula, las partes de común acuerdo establecen que en caso de que la parte RECEPTORA incumpla las obligaciones del presente instrumento, la parte REVELADORA tendrá el derecho de requerir el pago de una penalidad equivalente a la suma de Treinta Mil de Dólares de los Estados Unidos de América (US $ 30.000,00) en calidad de cláusula penal, a más de los valores que la sentencia o laudo establezcan por daños y perjuicios.

4.2 Cualquiera de las condiciones del presente Convenio que por su naturaleza se extienda más allá de la terminación de éste, sin importar la terminación de la relación comercial de las partes, se mantendrá en efecto hasta su cumplimiento y sobre él se mantendrán la total vigencia de las sanciones en caso de incumplimiento.

La parte RECEPTORA acepta asumir la responsabilidad legal, económica o administrativa en caso de que, por omisión, negligencia o responsabilidad directa o indirecta de uno de sus dependientes o subalternos incumpla con este Convenio.

Las Partes contratantes aceptan aplicar las leyes de la República del Ecuador, para regir, interpretar y hacer cumplir la totalidad de los derechos, obligaciones y responsabilidades de su contraparte, que se derivan del objeto del presente Convenio o que en alguna manera se relacionan con dicho objeto.

Figura 4.2: Convenio de Confidencialidad Parte 2.

Elaborado por: Investigador.

Las Partes contratantes aceptan aplicar las leyes de la República del Ecuador, para regir, interpretar y hacer cumplir la totalidad de los derechos, obligaciones y responsabilidades de su contraparte, que se derivan del objeto del presente Convenio o que en alguna manera se relacionan con dicho objeto.

El presente Convenio constituye completa y exclusivamente el acuerdo establecido entre las partes con respecto a la revelación de Información Confidencial que efectúen las Partes y reemplaza a todas las comunicaciones orales o escritas que las Partes hayan intercambiado anteriormente en relación con las revelaciones mencionadas, y a excepción del contrato de trabajo que se mantiene vigente. Con la firma de este documento las Partes aceptan las condiciones contenidas en este Convenio.

En caso de existir dudas o discrepancias en cuanto si alguna información es un secreto comercial y, por lo tanto, si ésta se encuentra sujeta a los términos del presente Convenio, ésta deberá de ser tratada como confidencial y, por ende, estará sujeta a los términos de este instrumento.

El presente Convenio solamente se puede modificar por escrito y con firma de ambas partes.

CLÁUSULA QUINTA: PLAZO.- El presente Convenio estará vigente por un plazo indefinido, contado desde la suscripción del mismo, o bien hasta que la Información Confidencial divulgada por la parte REVELADORA se vuelva del dominio público, indistintamente de que exista o no relación laboral vigente entre las Partes y la Confidencialidad quede regulada por el Contrato, Acuerdo o símil que rija tal relación laboral, en su caso.

CLÁUSULA SEXTA: CONTROVERSIAS.- Las partes aceptan que este Convenio se regirá por las leyes de la República del Ecuador.

En caso de conflicto, las partes libre y voluntariamente deciden someter su controversia, primeramente, a un proceso de mediación obligatorio de conformidad con lo determinado en la Ley de Arbitraje y Mediación. La Mediación se llevará a cabo en el Centro de Mediación y Arbitraje de la Cámara de Comercio de Ambato.

En caso de no llegar a un acuerdo en Mediación, las partes renuncian a la justicia ordinaria y someterán a un proceso arbitral por medio de un tribunal integrado por tres (3) árbitros del Centro de Arbitraje y Mediación de la Cámara de Comercio de Ambato. Se sujetarán a lo dispuesto en la Ley de Arbitraje y Mediación, al Reglamento del Centro de Arbitraje y Mediación de la Cámara de Comercio de Ambato y a las siguientes normas:

a) Los árbitros serán Abogados seleccionados conforme a lo establecido en la Ley y Reglamento de la Cámara de Comercio de Ambato.
b) El procedimiento arbitral será en derecho.
c) Las partes se obligan a acatar el laudo arbitral y se comprometen a no interponer ningún tipo de recurso en contra de dicho laudo arbitral.
d) Para la ejecución de las medidas cautelares, los árbitros están facultados para solicitar de los funcionarios públicos, judiciales, policiales y administrativos su cumplimiento sin que sea necesario recurrir a Juez ordinario alguno.
e) El lugar de arbitraje será en las instalaciones del Centro de Arbitraje y Mediación de la Cámara de Comercio de Ambato.
f) El valor del arbitraje, costas y los honorarios del abogado defensor serán pagados por la parte que se determine en el laudo arbitral. No obstante, el actor podrá cubrir lo que correspondiere pagar por el arbitraje y podrá repetir el pago en contra del demandado, en caso de así pronunciarse los árbitros.
g) Las partes de mutuo acuerdo, dan la facultad a los árbitros de solicitar auxilio de los funcionarios públicos, judiciales, policiales y administrativos para la ejecución de las medidas cautelares que una de las partes solicite, y que faculta la ley.
h) El proceso arbitral tendrá el carácter de confidencial.
i) Las partes señalan como sus domicilios para todas las citaciones y notificaciones relacionadas con el arbitraje, los que constan en este acuerdo.

Las partes suscriben dos ejemplares de igual contenido y valor, en Ambato a los **01 días del mes de diciembre del 2020.**

BIOALIMENTAR®
Pasión por nutrición

Ing. Roberto Navarro
BIOALIMENTAR CIA. LTDA.

Bryan Andrés Guerrón Chiluisa
1803247012

Figura 4.3: Convenio de Confidencialidad Parte 3.

Elaborado por: Investigador.

Anexo B

LOPD Ecuador

Que, el artículo 66 numeral 19 de la Constitución de la República reconoce y garantiza a las personas: "*19 El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley* ";

Figura 4.4: Articulo 66, numeral 19 de la LOPD.

Fuente: LOPD Ecuador [44].

Que, el artículo 92 de la Norma Suprema prescribe que "*Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez La persona afectada podrá demandar por los perjuicios ocasionados* ",

Figura 4.5: Articulo 92 de la LOPD.

Fuente: LOPD Ecuador [44].

Artículo 9. Juridicidad, lealtad y transparencia: Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la presente Ley, su reglamento y la demás normativa y jurisprudencia aplicable.

En ningún caso los datos personales podrán ser tratados a través de medios o para fines ilícitos o desleales.

Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia.

Figura 4.6: Articulo 9 de la LOPD.

Fuente: LOPD Ecuador [44].

Artículo 18. Seguridad de datos personales: Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, sean éstas técnicas, organizativas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.

Figura 4.7: Articulo 18 de la LOPD.

Fuente: LOPD Ecuador [44].

Artículo 50. Seguridad de datos personales: El responsable o encargado del tratamiento de datos personales, según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos y el nivel de impacto que estos representen a los derechos fundamentales y libertades individuales.

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.

El responsable o encargado del tratamiento de datos personales deberá demostrar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados.

Entre otras medidas, se podrán incluir las siguientes:

1. Medidas de anonimización, encriptación, cifrado o codificación de datos personales;
2. Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y,
3 Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, organizativa, y jurídica.

Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares para medición y gestión de riesgos, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

Figura 4.8: Articulo 50 de la LOPD.

Fuente: LOPD Ecuador [44].

Artículo 51. Medidas de seguridad en el ámbito del sector público: El mecanismo gubernamental de seguridad de la información incluirá las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados,

Figura 4.9: Articulo 51 de la LOPD.

Fuente: LOPD Ecuador [44].

Artículo 55. Notificación de vulneración de seguridad: El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales, dentro del término de tres (3) días a partir del conocimiento de dicha vulneración.

El encargado de tratamiento deberá notificar al responsable la vulneración de la seguridad de datos personales en un término no mayor a dos (2) días después de tener conocimiento de ella.

En caso de retraso del responsable o del encargado del tratamiento de datos personales en la notificación de vulneración de seguridad, sin que intermedie la debida justificación, se aplicarán las sanciones correspondientes, conforme a lo establecido en la presente ley.

La Autoridad de Protección de Datos Personales sólo podrá sancionar al responsable o encargado del tratamiento, cuando la vulneración de seguridad de datos personales ha sido producto de incumplimientos a las medidas de seguridad adecuadas. En tal caso, la notificación oportuna de la violación por parte del responsable de tratamiento, tanto a la autoridad como al titular, así como las medidas de respuesta adoptadas, serán considerados como un atenuante de la infracción

En caso de no cumplimiento del término para la notificación, el responsable del tratamiento deberá justificar la dilación, caso contrario, se procederá conforme al régimen sancionatorio establecido para el efecto.

Figura 4.10: Articulo 51 de la LOPD.

Fuente: LOPD Ecuador [44].

Artículo 71. Obligaciones del responsable del tratamiento de datos personales: El responsable del tratamiento está obligado a.

1. Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
2. Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
3. Aplicar e implementar procesos de verificación, evaluación y valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;
4. Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
5. Adherirse a códigos de protección, mecanismos de certificación o sellos de protección de datos personales aprobados por la Autoridad de Protección de Datos Personales,
6. Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
7. Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;
8. Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas,
9. Notificar a la Autoridad de Protección de Datos Personales y al titular de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;

Figura 4.11: Articulo 51 de la LOPD.

Fuente: LOPD Ecuador [44].

Anexo C

Políticas de Seguridad Informática para el Teletrabajo

Figura 4.12: Políticas de Seguridad Informática para el Teletrabajo Portada.

Elaborado por: Investigador.

BIOALIMENTAR
Pasión por nutrición

Índice

Figura 4.13: Políticas de Seguridad Informática para el Teletrabajo Índice.

Elaborado por: Investigador.

BIOALIMENTAR Pasión por nutrición

Configuraciones Básicas de Seguridad Informática

1. Información General

La intención de la publicación de las políticas de configuraciones básicas de seguridad informática es ayudar al personal de la empresa a tener una mejor seguridad al momento de la realización de sus actividades diarias, garantizando la seguridad y la integridad tanto del personal de la empresa como de los activos de la misma.

La realización de teletrabajo puede suponer una vulnerabilidad para la empresa si no se tienen en cuenta ciertas configuraciones básicas antes de la realización del teletrabajo como puede ser: la configuración adecuada del router, el proveedor de internet, antivirus y sistemas operativos desactualizados, inexistencia de copias de seguridad de activos críticos, etcétera.

La seguridad de la empresa y de todo el personal que la conforma es un esfuerzo de equipo que involucra la participación y el apoyo de todo el personal de la empresa. Es responsabilidad de cada usurario conocer las presentes políticas y realizar sus actividades en consecuencia.

2. Propósito

Evitar la intrusión, robo y divulgación no autorizada de información confidencial de la empresa.

3. Alcance

Estas políticas cubren los aspectos básicos a tener en cuenta para la seguridad informática y para con ello la realización de teletrabajo, y en el caso de incumplir con una de ellas podría significar un grave problema en la seguridad de la empresa viéndose afectada la empresa y el personal que labora en ella, por lo tanto, es de suma importancia que se cumplan por todo el personal de la empresa que realice teletrabajo con el fin de garantizar la seguridad de la empresa, así como la del personal que labora en la misma.

4. Políticas

- Se debe tener en cuenta la velocidad de subida mínima como la velocidad de bajada mínima contratada para la realización de sus actividades; si cumple o no cumple con las necesidades para la realización correcta de sus actividades.
- Es necesario tener en cuenta los problemas y críticas que posee un proveedor de servicio de internet (ISP), contratado o por adquirir; algunos problemas pueden comprender: problemas de seguridad en los equipos que brindan el servicio de internet, quejas de mal funcionamiento del servicio, etcétera.
- Se debe revisar si las configuraciones de los equipos que le brinda el servicio de internet son las adecuadas y cumplen con las seguridades básicas como: actualización de firmware, credenciales los más robustas posibles que cumplan

2

Figura 4.14: Configuraciones Básicas de Seguridad Informática Parte 1.

Elaborado por: Investigador.

con los estándares de seguridad, desactivación de los protocolos WPS y WEB, la utilización de por lo menos el protocolo WPA2 y de ser factible ocultar la red.

- Emplear una conexión por cable antes que Wifi.
- El equipo a emplear para el teletrabajo debe ser configurado por el personal de TI con las configuraciones básicas y necesarias para el desarrollo de las actividades del usuario y con las seguridades necesarias.
- Mantener el sistema operativo, aplicaciones empleadas en el trabajo, así como el antivirus actualizado.
- Comprobar que el dispositivo a utilizar o que se encuentra empleando en el trabajo se encuentre cifrado ya sea mediante el propio sistema operativo o mediante algún software.
- Instalar en los dispositivos a emplear en el trabajo solo los programas y aplicaciones necesarias, siempre de páginas oficiales y no de terceros. Pedir ayuda al personal de TI de ser necesario para mayor seguridad.
- El software instalado debe contar con las licencias para su activación y correcto funcionamiento. Por ende, no se permite el uso de software pirata para la realización de las actividades de la empresa.
- Ningún empleado debe manipular las piezas internas de hardware de los dispositivos entregados por la empresa.

5. Excepciones

En caso de que la empresa no pueda brindar un equipo al usuario y deba emplear un equipo propio, debe ser revisado por el personal de TI de la empresa para corroborar que cumple con las seguridades necesarias para la realización del trabajo.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

Velocidad Recomendada para el Teletrabajo:

- Cuál es la mejor velocidad de internet para realizar teletrabajo en base a las actividades a realizar, https://ultra.pe/blog/la-mejor-velocidad-de-internet-para-teletrabajo/
- Con que tipo de internet se puede teletrabajar y como mejorar la velocidad de internet, https://www.mistercomparador.com/noticias/velocidad-internet-para-teletrabajo/

3

Figura 4.15: Configuraciones Básicas de Seguridad Informática Parte 2.

Elaborado por: Investigador.

Contraseñas Robustas:

- De que está compuesta una contraseña robusta y como se crea una, http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-wstation-pass.html

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

Figura 4.16: Configuraciones Básicas de Seguridad Informática Parte 3.

Elaborado por: Investigador.

Estándar de Comunicación Inalámbrica

Estándar de Comunicación Inalámbrica

1. Información General

La intención de los estándares de comunicación inalámbrica es especificar los diferentes requisitos que deben cumplir las comunicaciones inalámbricas para garantizar la seguridad y que no exista ningún tipo de filtrado de información o que se llegue a comprometer la seguridad de la empresa.

2. Propósito

Este estándar especifica los requisitos técnicos que deben satisfacer los dispositivos de infraestructura inalámbrica para conectarse a una red empresarial. Solo aquellos dispositivos de infraestructura inalámbrica que cumplen con los requisitos especificados en este estándar o que reciben una excepción por parte del equipo TI de la empresa están aprobados para la conectividad a una red de la empresa.

Los dispositivos de red, incluidos, entre otros, concentradores, enrutadores, conmutadores, cortafuegos, dispositivos de acceso remoto, módems o puntos de acceso inalámbricos, deben ser instalados, respaldados y mantenidos por una organización de soporte aprobada en Seguridad de la Información.

3. Alcance

Todos los empleados de la empresa y sus subsidiarias, incluido todo el personal que mantiene un dispositivo de infraestructura inalámbrica en nombre de la empresa, deben cumplir con el estándar. Este estándar se aplica a los dispositivos inalámbricos que hacen una conexión a la red y a todos los dispositivos de infraestructura inalámbrica que brindan conectividad inalámbrica a la red.

4. Estándar

4.1 Requisitos generales

Todos los dispositivos de infraestructura inalámbrica que se conectan a una red de la empresa o proporcionan acceso a la empresa, deben:

- Utilizar el protocolo de autenticación extensible: autenticación rápida a través de túnel seguro (EAP-FAST) o mediante protocolo de autenticación extensible ligero (LEAP), Protocolo de autenticación extensible protegido (PEAP) o Protocolo de autenticación extensible: seguridad de capa de traducción (EAP-TLS) como protocolo de autenticación.
- Utilice el protocolo de integridad de clave temporal (TKIP) o los protocolos del sistema de cifrado avanzado (AES) con una longitud mínima de clave de 128 bits.
- Todos los dispositivos Bluetooth deben utilizar Secure Simple Pairing con el cifrado habilitado.

Figura 4.17: Estándar de Comunicación Inalámbrica Parte 1.

Elaborado por: Investigador.

4.2 Requisitos de los dispositivos inalámbricos domésticos

Todos los dispositivos de infraestructura inalámbrica domésticos que brindan acceso directo a una red empresarial, como los que están detrás de Enterprise Teleworker (ECT) o VPN de hardware, deben cumplir con lo siguiente:

- Habilite la clave pre compartida de acceso protegido WiFi (WPA2-PSK), EAP-FAST, PEAP o EAP-TLS
- Al habilitar WPA2-PSK, configure una clave secreta compartida compleja (al menos 20 caracteres) en el cliente inalámbrico y el punto de acceso inalámbrico
- Deshabilitar la transmisión de SSID
- Cambiar el nombre SSID predeterminado
- Cambiar el nombre de usuario y la contraseña predeterminados

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

Ninguna.

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

Figura 4.18: Estándar de Comunicación Inalámbrica Parte 2.

Elaborado por: Investigador.

Directrices para la Creación de Contraseñas Robustas

Directrices para la Creación de Contraseñas Robustas

1. Información General

Una contraseña es un componente crítico de la seguridad de la información. Sirven para proteger las cuentas de los usuarios, sistemas, informáticos, etcétera; sin embargo, una contraseña que no cumpla con ciertos estándares de seguridad puede llegar a generar problemas que pueden comprometer los sistemas, datos, redes individuales, etcétera.

2. Propósito

El propósito de estas pautas es proporcionar las mejores prácticas para la creación de contraseñas robustas.

3. Alcance

Esta directriz se aplica a empleados, contratistas, consultores, trabajadores temporales y de otro tipo, incluido todo el personal que se encuentre laborando en la empresa. Esta guía se aplica a todas las contraseñas, incluidas, entre otras, las cuentas de nivel de usuario, cuentas de nivel de sistema, cuentas web, cuentas de correo electrónico, protección de protector de pantalla, correo de voz e inicios de sesión del enrutador local, etcétera.

4. Declaración de Directrices

Una contraseña para que se considere robusta debe ser larga, cuantos más caracteres tenga, más segura será la contraseña. Se recomienda un mínimo de 8 a 14 caracteres en la creación de contraseñas. Además, se recomienda que la contraseña se encuentre compuestas por varias palabras y caracteres. Debe contener letras mayúsculas y minúsculas, además de números y caracteres no alfanuméricos.

Las contraseñas deficientes o débiles tienen las siguientes características:

- Contiene menos de ocho caracteres.
- Contienen información personal como fechas de nacimiento, direcciones, números de teléfono o nombres de miembros de la familia, mascotas, amigos y personajes de fantasía.
- Contienen patrones numéricos como aaabbb, qwerty, zyxwvuts o 123321.
- Son alguna versión de "Bienvenido123" "Password123" "Cambiame123"

Además, es muy importante que cada cuenta de trabajo deba tener una contraseña única y diferente. De igual manera gestionar de manera adecuada las contraseñas, no almacenarlas en papeles, en bloc de notas, adhesivos en los dispositivos, entre otras; sino almacenarlas mediante algún tipo de software de cifrado o mediante software de "administrador de contraseñas" autorizado y proporcionado por la organización que además permita a los usuarios mantener varias contraseñas. Siempre que sea posible, se recomienda también el uso de autenticación multifactor.

7

Figura 4.19: Directrices para la Creación de Contraseñas Robustas Parte 1.

Elaborado por: Investigador.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En el caso de la presente política es considerada como recomendación, pero en caso de que pueda verse comprometida la empresa por no tener en cuenta las presentes recomendaciones, se podrá tomar medidas disciplinarias.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

Estándares de contraseñas NIST

- Requisitos y recomendaciones para la creación de una contraseña según el estándar NIST, https://specopssoft.com/blog/nist-password-standards/
- Directrices de identidad digital, https://pages.nist.gov/800-63-3/

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

8

Figura 4.20: Directrices para la Creación de Contraseñas Robustas Parte 2.

Elaborado por: Investigador.

Política de Uso Aceptable

Política de Uso Aceptable

1. Información General

Las intenciones de la publicación de una política de uso aceptable no es imponer restricciones que sean contrarias a la cultura establecida de apertura, confianza e integridad de la empresa. La empresa se compromete a proteger a los empleados, socios y la compañía, de acciones ilegales o dañinas por parte de personas, ya sea a sabiendas o sin saberlo.

Los sistemas relacionados con Internet/Intranet/Extranet, incluidos, entre otros, equipos informáticos, software, sistemas operativos, medios de almacenamiento, cuentas de red que proporcionan correo electrónico, navegación WWW y FTP, son propiedad de la empresa. Estos sistemas deben utilizarse con fines acordes a los intereses de la empresa.

La seguridad efectiva es un esfuerzo de equipo que involucra la participación y el apoyo de todos los empleados y afiliados de la empresa que se ocupan de la información y / o los sistemas de información. Es responsabilidad de cada uno conocer las pautas y realizar sus actividades en consecuencia.

2. Propósito

El propósito de esta política es describir el uso aceptable de equipos informáticos. Estas reglas están en vigor para proteger al empleado y a la empresa. El uso inadecuado expone a la empresa a riesgos que incluyen ataques mediante el uso de malware, compromiso de los sistemas y servicios de red, así como problemas legales.

3. Alcance

Esta política se aplica al uso de información, dispositivos electrónicos y de computación y recursos de red para la realización de las actividades por parte de los empleados. Todos los empleados, contratistas, consultores, trabajadores temporales y otros trabajadores de la empresa y sus subsidiarias son responsables de ejercer su buen juicio con respecto al uso apropiado de la información, los dispositivos electrónicos y los recursos de red de acuerdo con las políticas y estándares establecidos por la empresa, así como de las leyes y regulaciones locales.

Esta política se aplica a los empleados, contratistas, consultores, personal temporal y otros trabajadores que pertenecen a la empresa. Esta política se aplica a todos los equipos que son propiedad o arrendados por la empresa.

Figura 4.21: Política de Uso Aceptable Parte 1.

Elaborado por: Investigador.

4. Políticas

4.1 Uso general y Propiedad

4.1.1. La información de propiedad exclusiva de la empresa que se encuentre almacenada en dispositivos electrónicos e informáticos, ya sean de su propiedad o arrendados por la empresa, el empleado o un tercero, debe asegurarse a través de medios legales o técnicos que garanticen que la información de propiedad está protegida de acuerdo con el Estándar de Protección de Datos.

4.1.2. Tiene la responsabilidad de informar de inmediato el robo, pérdida o divulgación no autorizada de la información de propiedad de la empresa.

4.1.3. Puede acceder, utilizar o compartir información de propiedad de la empresa, solo en la medida en que se esté autorizado y sea necesario para cumplir con las tareas asignadas.

4.1.4. Por motivos de seguridad y mantenimiento de la red, las personas autorizadas dentro de la empresa pueden monitorear el equipo, los sistemas y el tráfico de la red en cualquier momento.

4.1.5. La empresa se reserva el derecho de auditar redes y sistemas periódicamente para garantizar el cumplimiento de esta política.

4.2 Seguridad e Información Patentada

4.2.1. Todos los dispositivos móviles e informáticos que se conectan a la red interna deben cumplir con la Política de Acceso Mínimo.

4.2.2. Las contraseñas de nivel de sistema y de usuario deben cumplir con las Directrices para la Creación de Contraseñas Robustas. Se prohíbe proporcionar acceso a otra persona, ya sea de forma deliberada o sin asegurar su acceso.

4.2.3. Todos los dispositivos informáticos deben estar protegidos con un protector de pantalla protegido por contraseña con la función de activación automática que se encuentre configurado aproximadamente 10 minutos o menos. Se debe bloquear la pantalla o cerrar la sesión cuando el dispositivo no esté en uso.

4.2.4. Los empleados deben tener extrema precaución al abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, que pueden contener algún tipo de malware.

4.3 Uso Inaceptable

Las siguientes actividades se consideran como inaceptables o prohibidas. Los empleados pueden estar exentos de estas restricciones durante el transcurso de sus responsabilidades laborales legítimas (por ejemplo, el personal de administración de

Figura 4.22: Política de Uso Aceptable Parte 2.

Elaborado por: Investigador.

sistemas puede necesitar deshabilitar el acceso a la red de un host si ese host está interrumpiendo los servicios de producción).

Bajo ninguna circunstancia, un empleado de la empresa puede participar en cualquier actividad que sea ilegal según las leyes locales, estatales, federales o internacionales mientras se emplea los recursos de la empresa.

La lista a continuación no es de ninguna manera exhaustiva, pero intenta proporcionar un marco para las actividades que caen en la categoría de uso inaceptable.

4.3.1. Actividades del Sistema y la Red

Las siguientes actividades están estrictamente prohibidas, sin excepciones:

1. Violaciones de los derechos de cualquier persona o empresa protegida por derechos de autor, secretos comerciales, patentes u otra propiedad intelectual, o leyes o reglamentos similares, que incluyen, entre otros, la instalación o distribución de productos de software "pirata" u otros que no tienen la licencia adecuada para su uso por la empresa.

2. Se prohíbe el acceso a datos, servidores o cuentas para cualquier propósito que no esté relacionado con la realización de las actividades laborales, incluso si tiene acceso autorizado.

3. La exportación de software, información técnica, o tecnología de cifrado, en violación de las leyes de control de exportaciones internacionales o regionales, es ilegal. Se debe consultar a la dirección adecuada antes de exportar cualquier material en cuestión.

4. Introducción de programas maliciosos en la red o el servidor (por ejemplo, virus, gusanos, troyanos, correo electrónico malicioso, etc.).

5. Revelar la contraseña de su cuenta a otras personas o permitir el uso de su cuenta por parte de otros. Esto incluye a la familia y otros miembros del hogar cuando el trabajo se realiza en casa.

6. El uso de activos informáticos de la empresa para participar activamente en la obtención o transmisión de material que infrinja las leyes de acoso sexual o del lugar de trabajo hostil en la jurisdicción local del usuario.

7. Efectuar brechas de seguridad o interrupciones de la comunicación de la red. Las infracciones de seguridad incluyen, entre otras, el acceso a datos de los que el empleado no es el destinatario previsto o el inicio de sesión en un servidor o cuenta a los que el empleado no está expresamente autorizado a acceder, a menos que estos deberes estén dentro del alcance de sus deberes regulares. Para los propósitos de esta sección, "interrupción" incluye, pero no se limita a, rastreo de red, inundaciones con ping, suplantación de paquetes, denegación de servicio e información de enrutamiento falsificada con fines maliciosos.

8. El escaneo de puertos o el escaneo de seguridad están expresamente prohibidos a menos que se realice una notificación previa al personal de TI de la empresa.

Figura 4.23: Política de Uso Aceptable Parte 3.

Elaborado por: Investigador.

9. Ejecutar cualquier forma de monitoreo de red que intercepte datos que no estén destinados al host del empleado, a menos que esta actividad sea parte del trabajo o deber normal del empleado.

10. Eludir la autenticación de usuario o la seguridad de cualquier host, red o cuenta.

11. Introducir honeypots, honeynets o tecnología similar en la red de la empresa sin el consentimiento previo del departamento de TI.

12. Interferir o negar el servicio a cualquier usuario que no sea el anfitrión del empleado (por ejemplo, ataque de denegación de servicio).

13. Usar cualquier programa/script/comando, o enviar mensajes de cualquier tipo, con la intención de interferir, o deshabilitar, la sesión de un usuario, por cualquier medio, localmente o vía Internet/ Intranet/ Extranet.

12. Proporcionar información o listas de empleados de la compañía a terceros fuera de la misma.

4.3.2. Actividades de Correo Electrónico y Comunicación

Al emplear los recursos de la empresa para el acceso y utilización de Internet, los usuarios deben tener en cuenta de que representan a la empresa. Siempre que los empleados declaren pertenecer a la empresa, también deben indicar claramente que "las opiniones expresadas son mías y no necesariamente las de la empresa". Las preguntas pueden dirigirse al Departamento de TI

1. Enviar mensajes de correo electrónico no solicitados, incluido el envío de "correo basura" u otro material publicitario a personas que no solicitaron específicamente dicho material (correo no deseado).

2. Cualquier forma de acoso por correo electrónico, teléfono u otros medios, ya sea a través del idioma, frecuencia o tamaño de los mensajes.

3. Uso no autorizado o falsificación de la información del encabezado del correo electrónico.

4. Solicitud de correo electrónico para cualquier otra dirección de correo electrónico, que no sea la de la cuenta del autor, con la intención de acosar o recopilar respuestas.

5. Crear o reenviar "cartas en cadena", u otros esquemas "piramidales" de cualquier tipo.

6. Publicar mensajes iguales o similares no relacionados con la empresa en un gran número de grupos de noticias de Usenet (spam de grupos de noticias).

Figura 4.24: Política de Uso Aceptable Parte 4.

Elaborado por: Investigador.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

- Estándar de Protección de Datos
- Política de Acceso Mínimo
- Política de Contraseñas Robustas

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

Figura 4.25: Política de Uso Aceptable Parte 5.

Elaborado por: Investigador.

BIOALIMENTAR Pasión por nutrición

Directrices para Antivirus

1. Información General

Las directrices que se presentan a continuación comprenden una serie de recomendaciones que se deben tener en cuenta para poder reducir el riesgo de infección de algún tipo de malware que pueda afectar la correcta realización de las actividades en la empresa y con ello comprometer la seguridad de la misma.

2. Propósito

El propósito de estas directrices es mostrar al personal de la empresa como se puede reducir la infección de dispositivos informáticos de algún tipo de malware, y la concienciación de cuán importante es la presencia de un antivirus en los dispositivos informáticos, además de que se encuentren actualizados y en correcto funcionamiento.

3. Alcance

Todos los empleados, contratistas, consultores, trabajadores temporales y otros trabajadores de la empresa y sus subsidiarias deben tener en cuenta las siguientes directrices que servirán de ayuda para no sufrir ningún tipo de infección por malware que pueda afectar a la empresa y a sus activos.

4. Declaración de Directrices

Procesos recomendados para prevenir problemas con malware:

- Ejecute siempre el software antivirus compatible. Descargue y ejecute la versión actual; descargue e instale actualizaciones de software antivirus a medida que estén disponibles.
- NUNCA abra ningún archivo o macros adjunto a un correo electrónico de una fuente desconocida, sospechosa o no confiable. Elimine estos archivos adjuntos inmediatamente, luego "elimínelos dos veces" vaciando la Papelera.
- Elimine el correo no deseado, en cadena y otros correos electrónicos no deseados sin reenviarlos.
- Nunca descargue archivos de fuentes desconocidas o sospechosas.
- Evite el uso compartido directo de discos con acceso de lectura / escritura, a menos que exista un requisito comercial absoluto para hacerlo.
- Escanee siempre los dispositivos de almacenamiento como son: USBs, discos duros, etcétera; de una fuente desconocida en busca de virus antes de usarlo.
- Realice copias de seguridad de los datos críticos y las configuraciones del sistema de forma regular y almacene los datos en un lugar seguro.
- Si existe algún tipo de conflicto con el software antivirus, ejecute la utilidad antivirus para asegurarse de que la máquina esté limpia, desactive el software y luego vuelva a activarlo para comprobar si persiste el conflicto.

14

Figura 4.26: Directrices para Antivirus Parte 1.

Elaborado por: Investigador.

Cuando el software antivirus está desactivado, no ejecute ninguna aplicación que pueda transferir un virus, por ejemplo, correo electrónico o uso compartido de archivos.

- Los equipos infectados con virus deben eliminarse de la red hasta que se verifique que están libres de virus.
- Casi todos los días se descubren nuevos virus. Consulte periódicamente esta lista de procesos recomendados para obtener actualizaciones.

5. Excepciones

Ninguna.

6. Incumplimiento

Ninguna.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

Ninguna.

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

15

Figura 4.27: Directrices para Antivirus Parte 2.

Elaborado por: Investigador.

Política de Escritorio Limpio

Política de Escritorio Limpio

1. Información General

Una política de escritorio limpio garantiza que todos los materiales sensibles/ confidenciales se eliminen del espacio de trabajo del usuario final y se guarden bajo llave cuando los elementos no estén en uso o un empleado abandone su estación de trabajo. Esta política aumenta la conciencia de los empleados sobre la protección de la información confidencial.

2. Propósito

El propósito de esta política es establecer los requisitos mínimos para mantener un "escritorio limpio", donde la información sensible y crítica de la empresa esté segura en áreas bloqueadas y fuera del sitio. Una política de escritorio limpio no solo cumple con la norma ISO 27001/17799, sino que también forma parte de los controles de privacidad básicos de ciertos estándares.

3. Alcance

Esta política se aplica a todos los empleados de la empresa.

4. Políticas

4.1 Se requiere que los empleados se aseguren de que toda la información sensible y confidencial en papel o en formato electrónico esté segura en el área de trabajo y cuando se espera que estén fuera por un período prolongado.

4.2 El lugar de trabajo con computadora deben estar bloqueado cuando no se esté ocupando.

4.3 Las claves utilizadas para acceder a información restringida o confidencial no deben dejarse en un escritorio o en lugares públicos sin vigilancia.

4.4 Las contraseñas no pueden dejarse en notas adhesivas publicadas o debajo de una computadora, ni pueden dejarse escritas en un lugar accesible.

4.5 Guarde bajo llave los dispositivos informáticos portátiles, como computadoras portátiles y tabletas.

4.6 Tratar los dispositivos de almacenamiento masivo como CD-ROM, DVD o unidades USB como sensibles y guardarlos en un lugar seguro.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

Figura 4.28: Política de Escritorio Limpio Parte 1.

Elaborado por: Investigador.

BIOALIMENTAR
Pasión por nutrición

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

- Estándar de Protección de Datos
- ISO 27001/17799

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

Figura 4.29: Política de Escritorio Limpio Parte 2.

Elaborado por: Investigador.

Política de Filtrado y Supervisión del Uso de Internet

Política de Filtrado y Supervisión del Uso de Internet

1. Información General

La política de filtrado y supervisión del uso del internet garantiza que los empleados realicen sus actividades de la mejor manera, garantizando que el uso del internet sea de manera adecuada y segura para todos los empleados.

2. Propósito

El propósito de la política es definir estándares para los sistemas que monitorean y limitan el uso de la web desde cualquier host dentro de la red de la empresa. Estos estándares están diseñados para garantizar que los empleados usen Internet de manera segura y responsable, y garantizar que el uso de la web por parte de los empleados se pueda monitorear o investigar en caso de que suceda un incidente.

3. Alcance

Esta política se aplica a todos los empleados de la empresa con una computadora o estación de trabajo de propiedad personal o de la empresa conectada a la red de la empresa.

Esta política se aplica a todas las comunicaciones iniciadas por el usuario final entre la red de la empresa e Internet, incluida la navegación web, la mensajería instantánea, la transferencia de archivos, el intercambio de archivos y otros protocolos y estándares patentados.

Las comunicaciones de servidor a servidor, como tráfico SMTP, copias de seguridad, transferencias de datos automatizadas o comunicaciones de bases de datos, están excluidas de esta política.

4. Políticas

4.1 Monitoreo del sitio web

El Departamento de Tecnologías de la Información supervisará el uso de Internet desde todas las computadoras y dispositivos conectados a la red corporativa. Para todo el tráfico, el sistema de monitoreo debe registrar la dirección IP de origen, la fecha, la hora, el protocolo y el sitio o servidor de destino. Siempre que sea posible, el sistema debe registrar la identificación de usuario de la persona o cuenta que inicia el tráfico. Se recomienda que los registros de uso de Internet se conserven durante 180 días.

4.2 Acceso a los informes de seguimiento del sitio web

Los informes generales de tendencias y actividades estarán disponibles para cualquier empleado según sea necesario, previa solicitud al Departamento de Tecnologías de la Información. Los miembros del equipo de respuesta a incidentes de seguridad informática pueden acceder a todos los informes y datos si es necesario para responder a un incidente de seguridad. Los informes de uso de Internet que identifican a

18

Figura 4.30: Política de Filtrado y Supervisión del Uso de Internet Parte 1.

Elaborado por: Investigador.

usuarios, sitios, equipos o dispositivos específicos solo se pondrán a disposición de los asociados.

4.3 Sistema de filtrado de uso de Internet

El Departamento de Tecnologías de la Información bloqueará el acceso a los sitios web y protocolos de Internet que se consideren inapropiados para el entorno corporativo de la empresa. Se recomienda bloquear los siguientes protocolos y categorías de sitios web:

- Material para adultos/sexualmente explícito
- Anuncios y ventanas emergentes
- Chat y mensajería instantánea
- Juegos de azar
- Hacking
- Drogas
- Ropa íntima y trajes de baño
- Contactos y citas
- Servicios de redes sociales
- SPAM, phishing y fraude
- Software Espía
- Contenido ofensivo
- Violencia, Intolerancia y Odio

4.4 Cambios en las reglas de filtrado del uso de Internet

El Departamento de Tecnologías de la Información revisará y recomendará periódicamente cambios a las reglas de filtrado de protocolos y web. El departamento de Recursos Humanos deberá revisar estas recomendaciones y decidir si se deben realizar cambios. Los cambios en las reglas de filtrado de protocolos y web se registrarán en la Política de filtrado y supervisión del uso de Internet.

4.5 Excepciones de filtrado de uso de Internet

Si un sitio está mal clasificado, los empleados pueden solicitar que se desbloquee el sitio solicitando al departamento de TI que se realice una revisión del mismo. Un empleado de TI revisará la solicitud y desbloqueará el sitio si está mal categorizado.

Los empleados pueden acceder a sitios bloqueados con permiso si es apropiado y necesario para fines relacionados a los de la empresa. Si un empleado necesita acceder a un sitio que está bloqueado y categorizado adecuadamente, debe enviar una solicitud al departamento de TI. El Departamento de TI analizará la solicitud y permitirá el acceso al sitio o categoría solo para ese asociado de ser el caso. El Departamento de TI rastreará las excepciones aprobadas e informará sobre ellas a pedido.

Figura 4.31: Política de Filtrado y Supervisión del Uso de Internet Parte 2.

Elaborado por: Investigador.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

Ninguna.

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

Figura 4.32: Política de Filtrado y Supervisión del Uso de Internet Parte 3.

Elaborado por: Investigador.

Política de Protección de Claves

Política de Protección de Claves

1. Información General

La gestión de claves de cifrado, si no se realiza correctamente, puede comprometer y divulgar el uso de claves privadas. Si bien los usuarios pueden comprender que es importante encriptar ciertos documentos y comunicaciones electrónicas, es posible que no estén familiarizados con los estándares mínimos para las claves de encriptación de protección.

2. Propósito

Esta política describe los requisitos para proteger las claves que están bajo el control de los usuarios. Estos requisitos están diseñados para evitar la divulgación no autorizada y el posterior uso fraudulento. Los métodos de protección descritos incluyen controles operativos y técnicos, como procedimientos de copia de seguridad de claves, cifrado con una clave separada y uso de hardware resistente a la manipulación.

3. Alcance

Esta política se aplica a las claves que se enumeran a continuación y a la persona responsable de cualquier clave que se enumera a continuación. Las claves son:

- claves de cifrado emitidas por la empresa.
- claves de cifrado utilizadas para la empresa.
- claves de cifrado utilizadas para proteger los datos propiedad de la empresa.

4. Políticas

Todas las claves de cifrado cubiertas por la política deben estar protegidas para evitar su divulgación no autorizada y el posterior uso fraudulento.

4.1 Claves de cifrado de clave secreta

Las claves utilizadas para el cifrado de claves secretas, también llamadas criptografía simétrica, deben protegerse, ya que se distribuyen a todas las partes que las utilizarán. Durante la distribución, las claves de cifrado simétrico deben cifrarse utilizando un algoritmo más fuerte con una clave de longitud de clave más larga. Si las claves son para el algoritmo más fuerte, entonces la clave debe dividirse, cada parte de la clave cifrada con una clave diferente que es la longitud de clave más larga autorizada y cada parte cifrada se transmite utilizando diferentes mecanismos de transmisión. El objetivo es proporcionar una protección más estricta a la clave que los datos cifrados con esa clave de cifrado.

Figura 4.33: Política de Protección de Claves Parte 1.

Elaborado por: Investigador.

Las claves de cifrado simétrico, cuando están en reposo, deben protegerse con medidas de seguridad al menos tan estrictas como las medidas utilizadas para la distribución de esa clave.

4.2 Claves de cifrado de clave pública

La criptografía de clave pública, o criptografía asimétrica, utiliza pares de claves pública-privada. La clave pública se pasa a la autoridad de certificación para que se incluya en el certificado digital emitido al usuario final. El certificado digital está disponible para todos, una vez que se emite. La clave privada solo debe estar disponible para el usuario final al que se emite el certificado digital correspondiente.

4.2.1 Claves de infraestructura de clave pública (PKI) de la empresa.

Los pares de claves públicas-privadas que utiliza la infraestructura de claves públicas (PKI) de la empresa se generan en la tarjeta inteligente a prueba de manipulaciones emitida para un usuario final individual. La clave privada asociada con el certificado de identidad de un usuario final, que solo se utiliza para firmas digitales, nunca abandonará la tarjeta inteligente. La clave privada asociada con los certificados de cifrado, que se utilizan para cifrar el correo electrónico y otros documentos, debe estar en custodia.

El acceso a las claves privadas almacenadas en una tarjeta inteligente estará protegido por un número de identificación personal (PIN) que solo conoce la persona a quien se le expide la tarjeta inteligente. El software de la tarjeta inteligente se configurará para requerir la introducción del PIN antes de acceder a cualquier clave privada contenida en la tarjeta inteligente.

4.2.2 Otras claves de cifrado de clave pública

Se pueden generar otros tipos de claves en software en la computadora del usuario final y se pueden almacenar como archivos en el disco duro o en un token de hardware. Si el par de claves pública-privada se genera en una tarjeta inteligente, los requisitos para proteger las claves privadas son los mismos que para las claves privadas asociadas con la PKI de la empresa. Si las claves se generan en software, el usuario final debe crear al menos una copia de seguridad de estas claves y almacenar las copias de seguridad de forma segura. El usuario también debe crear una copia en custodia de cualquier clave privada utilizada para cifrar datos y entregar la copia en custodia al representante local de seguridad de la información para su almacenamiento seguro.

Todas las copias de seguridad, incluidas las copias en custodia, estarán protegidas con una contraseña o frase de contraseña que cumpla con la Política de contraseña robusta. Los representantes de la empresa almacenarán y protegerán las claves en custodia.

Figura 4.34: Política de Protección de Claves Parte 2.

Elaborado por: Investigador.

4.3 Almacenamiento de tokens de hardware

Los tokens de hardware que almacenan claves de cifrado se tratarán como equipos sensibles de la empresa, cuando se encuentren fuera de las oficinas de la empresa. Además, todos los tokens de hardware, tarjetas inteligentes, tokens USB, etc., no se almacenarán ni se dejarán conectados a la computadora de ningún usuario final cuando no estén en uso. Para los usuarios finales que viajen con tokens de hardware, no se almacenarán ni se transportarán en el mismo contenedor o bolsa que cualquier computadora.

4.4 Números de identificación personal (PIN), contraseñas y frases de contraseña

Todos los PIN, contraseñas o frases de contraseña que se utilizan para proteger las claves de cifrado deben cumplir con los requisitos de complejidad y longitud descritos en la política de contraseña robusta.

4.5 Pérdida y robo

La pérdida, el robo o la posible divulgación no autorizada de cualquier clave de cifrado cubierta por esta política debe informarse de inmediato al departamento de TI. El departamento de TI dirigirá al usuario final en cualquier acción que sea necesaria con respecto a la revocación de certificados o pares de claves público-privadas.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

- Cifrado aceptable
- Política de Contraseñas Robustas

8. Revisión Histórica

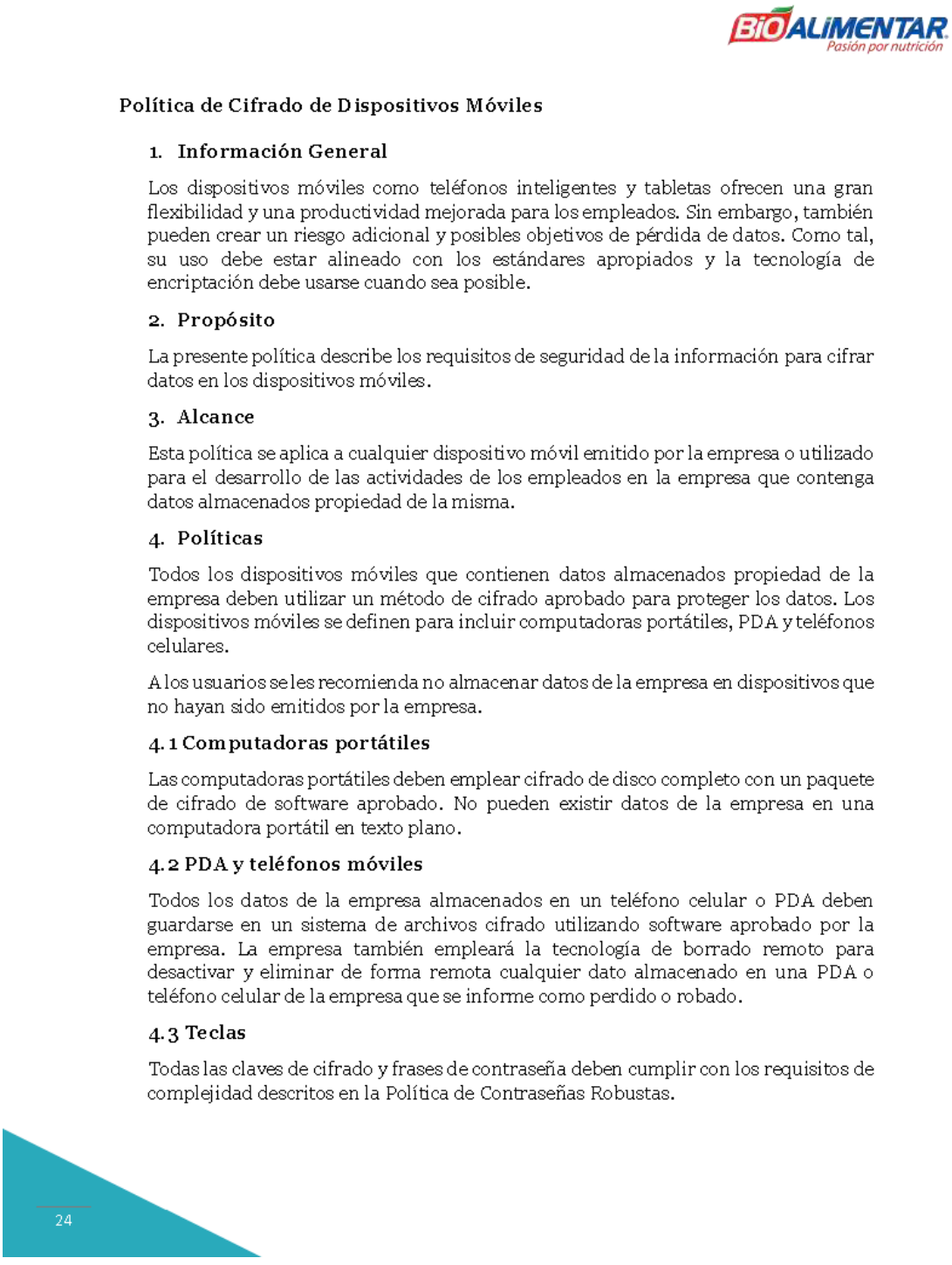
Fecha de Cambio	Responsable	Resumen de Cambio

23

Figura 4.35: Política de Protección de Claves Parte 3.

Elaborado por: Investigador.

Política de Cifrado de Dispositivos Móviles



Política de Cifrado de Dispositivos Móviles

1. Información General

Los dispositivos móviles como teléfonos inteligentes y tabletas ofrecen una gran flexibilidad y una productividad mejorada para los empleados. Sin embargo, también pueden crear un riesgo adicional y posibles objetivos de pérdida de datos. Como tal, su uso debe estar alineado con los estándares apropiados y la tecnología de encriptación debe usarse cuando sea posible.

2. Propósito

La presente política describe los requisitos de seguridad de la información para cifrar datos en los dispositivos móviles.

3. Alcance

Esta política se aplica a cualquier dispositivo móvil emitido por la empresa o utilizado para el desarrollo de las actividades de los empleados en la empresa que contenga datos almacenados propiedad de la misma.

4. Políticas

Todos los dispositivos móviles que contienen datos almacenados propiedad de la empresa deben utilizar un método de cifrado aprobado para proteger los datos. Los dispositivos móviles se definen para incluir computadoras portátiles, PDA y teléfonos celulares.

A los usuarios se les recomienda no almacenar datos de la empresa en dispositivos que no hayan sido emitidos por la empresa.

4.1 Computadoras portátiles

Las computadoras portátiles deben emplear cifrado de disco completo con un paquete de cifrado de software aprobado. No pueden existir datos de la empresa en una computadora portátil en texto plano.

4.2 PDA y teléfonos móviles

Todos los datos de la empresa almacenados en un teléfono celular o PDA deben guardarse en un sistema de archivos cifrado utilizando software aprobado por la empresa. La empresa también empleará la tecnología de borrado remoto para desactivar y eliminar de forma remota cualquier dato almacenado en una PDA o teléfono celular de la empresa que se informe como perdido o robado.

4.3 Teclas

Todas las claves de cifrado y frases de contraseña deben cumplir con los requisitos de complejidad descritos en la Política de Contraseñas Robustas.

Figura 4.36: Política de Cifrado de Dispositivos Móviles Parte 1.

Elaborado por: Investigador.

4.4 Pérdida y robo

La pérdida o robo de cualquier dispositivo móvil que contenga datos de la empresa debe informarse de inmediato.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

- Política de Contraseñas Robustas

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

25

Figura 4.37: Política de Cifrado de Dispositivos Móviles Parte 2.

Elaborado por: Investigador.

Política de Acceso Remoto

Política de Acceso Remoto

1. Información General

El acceso remoto a la red empresarial es esencial para mantener la productividad del equipo de trabajo, pero en muchos casos este acceso remoto se origina en redes que ya pueden estar comprometidas o que se encuentran en una posición de seguridad significativamente más baja que la de la red empresarial. Si bien estas redes remotas están fuera del control, es necesario mitigar estos riesgos externos de la mejor manera.

2. Propósito

El propósito de la política es definir reglas y requisitos para conectarse a la red de la empresa desde cualquier host. Estas reglas y requisitos están diseñados para minimizar en lo posible la exposición a la empresa por daños que puedan resultar del uso no autorizado de los recursos de la empresa. Los daños incluyen la pérdida de datos sensibles o confidenciales de la empresa, propiedad intelectual, daños a la imagen pública, daños a los sistemas internos críticos de la empresa y multas u otras responsabilidades financieras incurridas como resultado de esas pérdidas.

3. Alcance

Esta política se aplica a todos los empleados de la empresa que cuentan con una computadora o estación de trabajo de propiedad personal o de la empresa utilizada para conectarse a la red de la misma. Esta política se aplica a las conexiones de acceso remoto que se utilizan para trabajar en nombre de la empresa, incluida la lectura o el envío de correo electrónico y la visualización de recursos web de la intranet. Esta política cubre todas y cada una de las implementaciones técnicas de acceso remoto que se utilizan para conectarse a las redes de la empresa.

4. Políticas

Es responsabilidad de todos los empleados con privilegios de acceso remoto a la red corporativa de la empresa asegurarse de que su conexión de acceso remoto reciba la misma consideración que la conexión in situ del usuario a la empresa.

El acceso general a Internet para uso recreativo a través de la red de la empresa está estrictamente limitado a los empleados, contratistas, proveedores y agentes de la empresa (en lo sucesivo, "Usuarios autorizados"). Al acceder a la red de la empresa desde una computadora personal, los usuarios autorizados son responsables de evitar el acceso a los datos o recursos informáticos de la empresa por parte de usuarios no autorizados. Se prohíbe la realización de actividades ilegales a través de la red de la empresa por parte de cualquier usuario (autorizado o no). El Usuario Autorizado asume la responsabilidad y las consecuencias del mal uso del acceso del Usuario Autorizado. Para obtener más información y definiciones, consulte la política de uso aceptable.

Figura 4.38: Política de Acceso Remoto Parte 1.

Elaborado por: Investigador.

Los usuarios autorizados no utilizarán las redes de la empresa para acceder a Internet para intereses externos de la empresa.

Para obtener información adicional sobre las opciones de conexión de acceso remoto de la empresa incluido cómo obtener un inicio de sesión de acceso remoto, software antivirus empresarial, solución de problemas, etc., se pueden comunicar con el departamento de TI.

4.1 Requisitos

4.1.1 El acceso remoto seguro debe controlarse estrictamente con cifrado (es decir, redes privadas virtuales (VPN)) y contraseñas seguras.

4.1.2 Los usuarios autorizados deben proteger su nombre de usuario y contraseña, incluso de los miembros de la familia.

4.1.3 Al usar una computadora propiedad de la empresa para conectarse de forma remota a la red corporativa de la misma, los usuarios autorizados deben asegurarse de que el host remoto no esté conectado a ninguna otra red al mismo tiempo, con la excepción de redes que están bajo su control total o bajo el control total de un Usuario Autorizado o Tercero.

4.1.4 Todos los hosts que están conectados a las redes internas de la empresa mediante tecnologías de acceso remoto deben utilizar el software antivirus más actualizado, esto incluye computadoras personales. Las conexiones de terceros deben cumplir con los requisitos establecidos en el Acuerdo de terceros.

4.1.5 El equipo personal utilizado para conectarse a las redes de la empresa debe cumplir con los requisitos del equipo de propiedad de la empresa para el acceso remoto como se indica en los estándares de configuración de hardware y software para el acceso remoto a las redes según la empresa.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

Revise las siguientes políticas para obtener detalles sobre la protección de la información al acceder a la red corporativa a través de métodos de acceso remoto y el uso aceptable de la red de la empresa:

Figura 4.39: Política de Acceso Remoto Parte 2.

Elaborado por: Investigador.

- Política de cifrado de dispositivos móviles
- Política de uso aceptable
- Política de contraseñas robustas
- Estándares de configuración de hardware y software para el acceso remoto a redes planteados por la empresa.

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

Figura 4.40: Política de Acceso Remoto Parte 3.

Elaborado por: Investigador.

Política de Herramientas de Acceso Remoto

Política de Herramientas de Acceso Remoto

1. Información General

El software de escritorio remoto, también conocido como herramientas de acceso remoto, proporciona una forma para que los usuarios de las computadoras y el personal de soporte compartan pantallas, accedan a los sistemas informáticos del trabajo desde casa y viceversa. Algunos ejemplos de este tipo de software son LogMeIn, GoToMyPC, VNC (Computación de red virtual) y Windows Remote Desktop (RDP). Si bien estas herramientas pueden ahorrar mucho tiempo y dinero al eliminar los viajes y permitir la colaboración, también proporcionan una puerta trasera a la red de la empresa que se puede utilizar para el robo, el acceso no autorizado o la destrucción de activos. Como resultado, solo se pueden usar herramientas de acceso remoto aprobadas, monitoreadas y controladas adecuadamente en los sistemas informáticos de la empresa.

2. Propósito

La política define los requisitos para el uso de herramientas de acceso remoto utilizadas en la empresa.

3. Alcance

Esta política se aplica a todos los accesos remotos donde cualquiera de los extremos de la comunicación termina en un activo informático de la empresa.

4. Políticas

Todas las herramientas de acceso remoto utilizadas para comunicarse entre los activos de la empresa y otros sistemas deben cumplir con los siguientes requisitos de política.

4.1 Herramientas de acceso remoto

La empresa proporciona mecanismos para colaborar entre usuarios internos, con socios externos y desde sistemas que no son de la empresa. La lista de software debe ser aprobada por el departamento de TI. Dado que la configuración adecuada es importante para el uso seguro de estas herramientas, se proporcionan procedimientos de configuración obligatorios para cada una de las herramientas aprobadas.

La lista de software aprobado puede cambiar en cualquier momento, pero se debe utilizar los siguientes requisitos para seleccionar productos aprobados:

a) Todas las herramientas o sistemas de acceso remoto que permiten la comunicación con los recursos de la empresa desde Internet o sistemas de socios externos deben requerir autenticación de múltiples factores. Los ejemplos incluyen tokens de autenticación y tarjetas inteligentes que requieren un PIN o contraseña adicional.
b) La fuente de la base de datos de autenticación debe ser Active Directory o LDAP, y el protocolo de autenticación debe incluir un protocolo de desafío-

Figura 4.41: Política de Herramientas de Acceso Remoto Parte 1.

Elaborado por: Investigador.

respuesta que no sea susceptible a ataques de repetición. La herramienta de acceso remoto debe autenticar mutuamente ambos extremos de la sesión.

c) Las herramientas de acceso remoto deben admitir el proxy de la capa de aplicación de la empresa en lugar de las conexiones directas a través de los firewalls perimetrales.
d) Las herramientas de acceso remoto deben admitir un cifrado sólido de extremo a extremo de los canales de comunicación de acceso remoto.
e) Todos los antivirus de la empresa, sistemas de prevención de pérdida de datos y otros sistemas de seguridad no deben desactivarse, interferirse o eludirse de ninguna manera.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

Ninguna.

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

30

Figura 4.42: Política de Herramientas de Acceso Remoto Parte 2.

Elaborado por: Investigador.

Política de Seguridad del Servidor

Política de Seguridad del Servidor

1. Información General

Los servidores vulnerables y no seguros son un importante punto de entrada para los atacantes. Las políticas de instalación del servidor y la administración de la configuración consistentes tienen que ver con hacer bien lo básico.

2. Propósito

El propósito de esta política es establecer estándares para la configuración básica del equipo de servidor interno que es propiedad de la empresa o es operado por ella. La implementación efectiva de esta política minimizará el acceso no autorizado a la información y tecnología que es propiedad de la empresa.

3. Alcance

Todos los empleados deben cumplir con esta política. Esta política se aplica a los equipos de servidor que son propiedad de la empresa, operados o alquilados por la empresa, o registrados en un dominio de red interno propiedad de la empresa.

Esta política especifica los requisitos para los equipos de la red interna de la empresa.

4. Políticas

4.1 Requisitos generales

4.1.1 Todos los servidores internos implementados en la empresa deben ser propiedad de un grupo operativo que sea responsable de la administración del sistema. Cada grupo operativo debe establecer y mantener guías de configuración de servidor aprobadas, según las necesidades comerciales y aprobadas por la empresa. Los grupos operativos deben monitorear el cumplimiento de la configuración e implementar una política de excepción adaptada al entorno. Cada grupo operativo debe establecer un proceso para cambiar las guías de configuración, que incluye revisión y aprobación por parte de la empresa. Deben cumplirse los siguientes elementos:

- Los servidores deben estar registrados dentro del sistema de gestión empresarial corporativa. Como mínimo, se requiere la siguiente información para identificar positivamente el punto de contacto:
    - Contacto (s) del servidor y ubicación, y un contacto de respaldo.
    - Hardware y sistema operativo/versión.
    - Principales funciones y aplicaciones.
- La información en el sistema de gestión empresarial corporativo debe mantenerse actualizada.
- Los cambios de configuración para los servidores deben seguir los procedimientos de gestión de cambios adecuados.

Figura 4.43: Política de Seguridad del Servidor Parte 1.

Elaborado por: Investigador.

4.1.2 Por motivos de seguridad, cumplimiento y mantenimiento, el personal autorizado puede monitorear y auditar equipos, sistemas, procesos y tráfico de red.

4.2 Requisitos de configuración

4.2.1 La configuración del sistema operativo debe estar de acuerdo con las pautas aprobadas por el departamento de TI acordes a las necesidades de la empresa.

4.2.2 Los servicios y aplicaciones que no se utilizarán deben desactivarse lo antes posible.

4.2.3 El acceso a los servicios debe registrarse y / o protegerse mediante métodos de control de acceso, como un firewall de aplicaciones web.

4.2.4 Los servidores deben contemplar los mecanismos de protección contra cualquier tipo de amenaza.

4.2.5 Los parches de seguridad más recientes deben instalarse en el sistema tan pronto como sea posible, siendo la única excepción cuando la aplicación inmediata podría interferir con los requisitos comerciales.

4.2.6 Las relaciones de confianza entre sistemas son un riesgo para la seguridad y se debe evitar su uso. No utilizar una relación de confianza cuando algún otro método de comunicación sea suficiente.

4.2.7 Utilizar siempre los principios de seguridad de acceso mínimo requerido para realizar una función. No usar root cuando una cuenta sin privilegios sea suficiente.

4.2.8 Si está disponible una metodología para la conexión de canal segura (es decir, técnicamente factible), el acceso privilegiado debe realizarse a través de canales seguros (por ejemplo, conexiones de red encriptadas usando SSH o IPSec).

4.2.9 Los servidores deberían estar ubicados físicamente en un entorno de acceso controlado.

4.2.10 Los servidores tienen específicamente prohibido operar desde áreas de cubículo no controladas.

4.3 Seguimiento

4.3.1 Todos los eventos relacionados con la seguridad en sistemas críticos o sensibles deben registrarse y las pistas de auditoría deben guardarse de la siguiente manera:

- Todos los registros relacionados con la seguridad se deben mantener en línea durante un mínimo de 1 semana.
- Las copias de seguridad diarias se deben conservar durante al menos 1 mes.
- Las copias de seguridad de los registros completas semanales se deben conservar durante al menos 1 mes.
- Las copias de seguridad completas mensuales se deben conservar durante un mínimo de 2 años.

32

Figura 4.44: Política de Seguridad del Servidor Parte 2.

Elaborado por: Investigador.

4.3.2 Los eventos relacionados con la seguridad se informarán al departamento de TI. Se prescribirán medidas correctivas según sea necesario. Los eventos relacionados con la seguridad incluyen, pero no se limitan a:

- Ataques de escaneo de puertos
- Evidencia de acceso no autorizado a cuentas privilegiadas
- Incidencias anómalas que no están relacionadas con aplicaciones específicas en el host.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

Ninguna.

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

33

Figura 4.45: Política de Seguridad del Servidor Parte 3.

Elaborado por: Investigador.

Política Sobre Ingeniería Social

Política Sobre Ingeniería Social

1. Información General

Las políticas sobre ingeniería social son políticas y pautas para los empleados de la empresa, con el fin de que puedan reconocer las diferentes técnicas y ataques que existen.

Para proteger los activos de la empresa, todos los empleados deben defender la integridad y confidencialidad de los recursos de la empresa.

2. Propósito

Las siguientes políticas tiene dos propósitos:

2.1 Para informar a los empleados que:

a) Ocurren ataques fraudulentos de ingeniería social
b) Existen procedimientos que los empleados pueden usar para detectar ataques.

2.1.1 Se informa a los empleados sobre las técnicas utilizadas para tales ataques y se les proporciona procedimientos estándar para responder a los ataques.

2.1.2 Los empleados saben a quién contactar en estas circunstancias.

2.1.3 Los empleados reconocen que son una parte importante de la seguridad de la empresa. La integridad de un empleado es la mejor línea de defensa para proteger la información confidencial sobre los recursos de la empresa.

2.2 Crear procedimientos específicos que los empleados deben seguir para ayudarlos a tomar la mejor decisión cuando:

2.2.1 Alguien se está comunicando con el empleado (por teléfono, en persona, por correo electrónico, por fax o en línea) y está tratando de recopilar la información confidencial de la empresa de forma esquiva.

2.2.2 El empleado está siendo "presionado socialmente" o "animado o engañado socialmente" para que comparta datos confidenciales.

3. Alcance

Incluye a todos los empleados de la empresa, incluidos los contratistas temporales o los empleados a tiempo parcial.

4. Políticas

4.1 La información confidencial de la empresa no se compartirá con una persona no autorizada si usa palabras y / o técnicas como las siguientes:

4.1.1 Un "asunto urgente"

4.1.2 Una "contraseña olvidada"

34

Figura 4.46: Política Sobre Ingeniería Social Parte 1.

Elaborado por: Investigador.

4.1.3 Una "emergencia de virus informático"

4.1.4 Cualquier forma de intimidación por parte de la "gerencia de nivel superior"

4.1.5 Cualquier "mención de nombre" por parte del individuo que parezca que proviene de personal legítimo y autorizado.

4.1.6 El solicitante requiere la divulgación de información que revelará contraseñas, modelo, número de serie o marca o cantidad de recursos de la empresa.

4.1.7 Las técnicas son utilizadas por un individuo desconocido (no verificable de inmediato) por teléfono, correo electrónico, en línea, en persona o por otro medio.

4.1.8 Las técnicas son utilizadas por una persona que declara "ser parte de la empresa" o que pertenece a la misma.

4.1.9 Las técnicas son utilizadas por un individuo que dice ser reportero de un conocido editor de prensa o compañía de radio o televisión.

4.1.10 El solicitante está utilizando métodos de seducción del ego y la vanidad, por ejemplo, recompensando al empleado de la recepción con cumplidos sobre su inteligencia, capacidades o saludos inapropiados (provenientes de un extraño).

4.2 Acción

4.2.1 Todas las personas de la empresa DEBEN asistir a la capacitación de concienciación sobre seguridad dentro de los 30 días posteriores a la fecha de contratación y cada 6 meses a partir de entonces.

4.2.2 Si una o más de las circunstancias descritas son detectadas por una persona, entonces DEBE verificarse la identidad del solicitante antes de continuar la conversación o responder al correo electrónico, mensaje, etcétera.

4.2.3 Si la identidad del solicitante NO PUEDE verificarse de inmediato, la persona DEBE comunicarse inmediatamente con su supervisor o gerente directo.

4.2.4 Si el supervisor o gerente no está disponible, esa persona DEBE comunicarse con el personal de seguridad.

4.2.5 Si el personal de seguridad no está disponible, la persona DEBE abandonar inmediatamente la conversación, el correo electrónico, el chat en línea con el solicitante e informar el episodio a su supervisor antes del final del día hábil.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

Figura 4.47: Política Sobre Ingeniería Social Parte 2.

Elaborado por: Investigador.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

Ninguna.

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

Figura 4.48: Política Sobre Ingeniería Social Parte 3.

Elaborado por: Investigador.

Política de Instalación de Software

Política de Instalación de Software

1. Información General

Permitir que los empleados instalen software en los dispositivos informáticos de la empresa abre a la organización a una exposición innecesaria. Versiones de archivos en conflicto o DLL que pueden impedir la ejecución de programas, la introducción de malware a partir de software de instalación infectado, software sin licencia que podría descubrirse durante la auditoría y programas que se pueden utilizar para piratear la red de la organización son ejemplos de los problemas que pueden presentarse cuando los empleados instalan software en los equipos de la empresa.

2. Propósito

El propósito de esta política es describir los requisitos relacionados con la instalación del software en dispositivos informáticos que son propiedad de la empresa. Para minimizar el riesgo de pérdida de la funcionalidad del programa, la exposición de información confidencial contenida dentro de la red informática de la empresa, el riesgo de introducir malware y la exposición legal de ejecutar software sin licencia.

3. Alcance

Esta política se aplica a todos los empleados que cuentan con dispositivos móviles propiedad de la empresa. Esta política cubre todas las computadoras, servidores, teléfonos inteligentes, tabletas y otros dispositivos informáticos que operan dentro de la empresa.

4. Políticas

- Los empleados no pueden instalar software en los dispositivos informáticos de la empresa operados dentro de la red de la empresa.
- Las solicitudes de software primero deben ser aprobadas por el gerente del solicitante y luego enviarse al departamento de TI o al servicio de asistencia por escrito o por correo electrónico.
- El software debe seleccionarse de una lista de software aprobada, mantenida por el departamento de TI, a menos que ninguna selección en la lista satisfaga las necesidades del solicitante.
- El Departamento de TI obtendrá y rastreará las licencias, probará el nuevo software en busca de conflictos y compatibilidad, y realizará la instalación.
- Ningún usuario debe desinstalar, desactivar y/o manipular ninguna pieza de software que no haya sido instalada por soporte técnico; esto podría ocasionar un riesgo alto de seguridad.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en los equipos, a fin de evitar riesgos por mal uso y que podrían generar algún tipo de inconveniente.

37

Figura 4.49: Política de Instalación de Software Parte 1.

Elaborado por: Investigador.

5. **Excepciones**

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. **Incumplimiento**

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. **Información Relacionada (Estándares, Políticas, Procesos, Otros)**

Ninguna.

8. **Revisión Histórica**

Fecha de Cambio	Responsable	Resumen de Cambio

38

Figura 4.50: Política de Instalación de Software Parte 2.

Elaborado por: Investigador.

Política de Red Privada Virtual (VPN)

Política de Red Privada Virtual (VPN)

1. Información General

El acceder remotamente a recursos de la empresa pueden significar un gran problema en la seguridad de la empresa, por ello es muy importante el uso de una Red Privada Virtual (VPN) mediante la cual se pueda cifrar toda la comunicación de extremo a extremo y con ello poder reducir o mitigar los problemas que pueden suceder al emplear el acceso remoto en la empresa.

2. Propósito

El propósito de esta política es proporcionar pautas para las conexiones de red privada virtual (VPN) IPSec o L2TP de acceso remoto a la red corporativa de la empresa.

3. Alcance

Esta política se aplica a todos los empleados de la empresa, incluido todo el personal afiliado a terceros que utilizan VPN para acceder a la red de la empresa.

4. Políticas

Los empleados pueden utilizar los beneficios de las VPN, que son un servicio "administrado por el usuario". Esto significa que el usuario es responsable de seleccionar un proveedor de servicios de Internet (ISP), coordinar la instalación, instalar cualquier software requerido y pagar las tarifas asociadas.

Adicionalmente,

1. Es responsabilidad de los empleados con privilegios de VPN asegurarse de que los usuarios no autorizados no tengan acceso a las redes internas de la empresa.

2. El uso de VPN debe controlarse mediante una autenticación de contraseña de un solo uso, como un dispositivo de token o un sistema de clave pública / privada con una frase de contraseña segura.

3. Cuando se conectan activamente a la red corporativa, las VPN forzarán todo el tráfico hacia y desde la PC a través del túnel VPN: el resto del tráfico se eliminará.

4. NO se permite la tunelización dual (dividida); solo se permite una conexión de red.

5. Las puertas de enlace VPN serán configuradas y administradas por grupos operativos de red de la empresa.

6. Todas las computadoras conectadas a las redes internas de la empresa a través de VPN o cualquier otra tecnología deben utilizar el software antivirus más actualizado; esto incluye computadoras personales.

7. Los usuarios de VPN se desconectarán automáticamente de la red de la empresa después de treinta minutos de inactividad. El usuario debe volver a iniciar sesión para

Figura 4.51: Política de Red Privada Virtual (VPN) Parte 1.

Elaborado por: Investigador.

volver a conectarse a la red. No se deben usar ping u otros procesos de red artificial para mantener la conexión abierta.

8. El concentrador de VPN está limitado a un tiempo de conexión absoluto de 24 horas.

9. Los usuarios de computadoras que no son equipos de la empresa deben configurar el equipo para cumplir con las políticas de red y VPN de la empresa.

10. Solo se pueden utilizar clientes VPN aprobados por el departamento de TI de la empresa.

11. Al usar la tecnología VPN con equipos personales, los usuarios deben comprender que sus máquinas son una extensión de la red de la empresa y, como tales, están sujetas a las mismas reglas y regulaciones que se aplican a los equipos de la empresa, es decir, sus máquinas deben estar configuradas para cumplir con las Políticas de seguridad de la empresa.

5. Excepciones

Cualquier excepción a la política debe ser aprobada por el departamento de TI con anticipación.

6. Incumplimiento

En caso del incumplimiento de las políticas y por ende que se genere un incidente en el que se vea involucrado la seguridad e integridad de la empresa el usuario puede estar sujeto a medidas disciplinarias e incluso se podrá contemplar el despido sujetándose al Código del Trabajo y las Leyes del Ecuador.

7. Información Relacionada (Estándares, Políticas, Procesos, Otros)

- Política de Acceso Remoto

8. Revisión Histórica

Fecha de Cambio	Responsable	Resumen de Cambio

40

Figura 4.52: Política de Red Privada Virtual (VPN) Parte 2.

Elaborado por: Investigador.

Anexo D

Socialización de Políticas de Seguridad Informática para el Teletrabajo

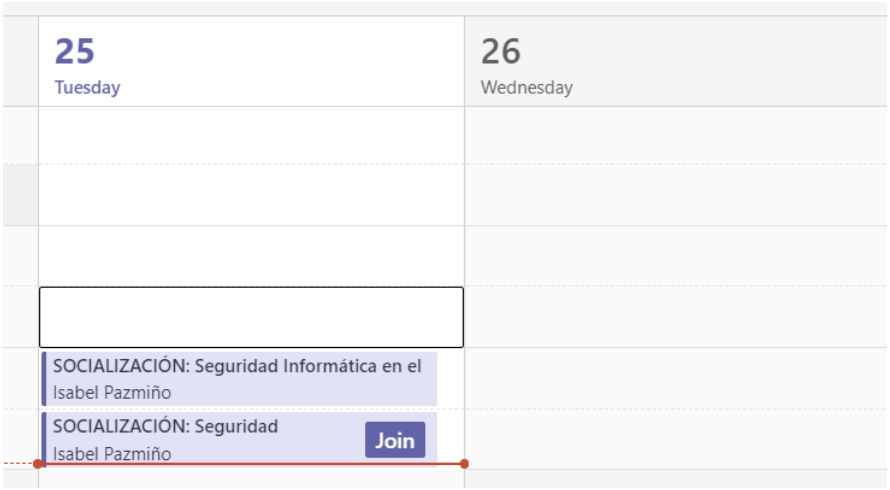


Figura 4.53: Calendario de Fechas de Socialización en la Empresa.

Elaborado por: Investigador.

Figura 4.54: Tema de Socialización en la Empresa.

Elaborado por: Investigador.