República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

Trabajo de Titulación para la

obtención del título de:

Ingeniera en Telecomunicaciones

Tema:

Propuesta de una guía para auditar la ciberseguridad en entidades del sector agroalimentario de Daule.

Autor/a:

Naomi Jomar Terán Méndez

Director de trabajo de titulación:

Ing. Diego Aguirre González, MSC.

2024

Guayaquil - Ecuador

AGRADECIMIENTO

Agradezco a Dios por guiarme en cada uno de mis aciertos y desaciertos en los pasos que he dado en mi vida, por darme la fortaleza y paciencia para concluir este hito académico.

Agradezco a mis padres, por ser mi ejemplo para seguir en el camino profesional, además de brindarme su apoyo emocional y amor incondicional en esta carrera, con cada consejo me motivan a culminar cada etapa u objetivo que me he propuesto.

Agradezco Rick, por ser mi compañerito de amanecidas.

Agradezco a todos aquellos que fueron un granito de arena para construir este trayecto, mis abuelos y amigos.

DECLARACION EXPRESA

Yo, Naomi Jomar Teran Méndez, hago constar bajo juramento que el presente trabajo de titulación titulado "Propuesta de una guía para auditar la ciberseguridad en entidades del sector agroalimentario de Daule" cumplió con los estándares éticos y académicos establecidos por la Universidad Tecnológica Empresarial de Guayaquil. Declaro que este trabajo fue realizado de forma independiente y original, sin la contribución de terceros, excepto las referencias y créditos debidamente citados en el trabajo. Asimismo, afirmo que el contenido de este trabajo de titulación no ha sido previamente presentado para obtener un grado o título en otra institución, y que no infringe los derechos de propiedad intelectual de terceros. La Universidad Tecnológica Empresarial de Guayaquil tiene derecho a hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Naomi Jomar Teran Méndez

PROPUESTA DE UNA GUÍA PARA AUDITAR LA CIBERSEGURIDAD EN ENTIDADES DEL SECTOR AGROALIMENTARIO DE DAULE.

Naomi Jomar Teran Méndez

naomiteran09@gmail.com

RESUMEN

El objetivo de esta propuesta es definir una guía de auditoría para la ciberseguridad en entidades del sector agroalimentario en Daule, se busca dar las pautas necesarias para brindar un proceso de tecnología a vanguardia y que con este se ayude a la mitigación, prevención y contingencia ante ciberataques. Por esta razón es de relevancia realizar un entendimiento del ambiente tecnológico para la correcta evaluación de la susceptibilidad a posibles ataques o vulneraciones que pueden ser críticos dentro de las empresas financieras.

En este trabajo se procura establecer la relevancia que tiene la ciberseguridad dentro de cada empresa y sus usuarios, concientizando y definiendo todos los equipos críticos que manejan datos o información sensible y que pueden ser el blanco directo para la vulneración.

Al culminar el presente trabajo, se podrá dar las claves para fortalecer el ambiente tecnológico y la seguridad de la información para la creación de una estrategia que permita la continuidad del negocio basado en observaciones generales según lo sugerido por las buenas prácticas y la ISO27000.

Palabras claves: Ciberataque, auditoria de ciberseguridad, usuario, seguridad de la información, ISO27000.

INTRODUCCIÓN

Actualmente en la vida cotidiana de los seres humanos y en diversos aspectos de su entorno laboral, académico o de entretenimiento se utilizan medios digitales que generan información y datos los cuales son expuestos notablemente y deben ser protegidos evitando su vulnerabilidad, para no ser el blanco de la sustracción, eliminación o alteración de datos confidenciales.

A pesar de la existencia de especialistas dentro de la seguridad de información y soluciones tecnológicas no siempre se crean mecanismos efectivos dentro de sus activos de tecnología o no existe este rol para proteger y velar por la seguridad tecnológica del eslabón más débil de cada entidad, el usuario. Esto se puede comprobar con el estudio del sector agroalimentario que aplica la tecnología en Reino Unido, donde indican su preocupación por la alta vulnerabilidad que tiene el sector y que afecta mayormente a la cadena de suministros, detallan que estas empresas son solo 50% autosuficientes y se recomienda un 80% de automatización dentro de sus procesos.

Por esta razón, se resalta la urgencia de mecanismos de control de ciberseguridad en las empresas agroalimentarias que manejan un entorno basado solo en tecnología o hibrido, el poder contar con una guía de emergencia que permita tener un plan de mitigación contra los ataques mencionados con anterioridad y que pueden repercutir no solo en los activos de la información sino también en las economías de clientes o proveedores ya que a futuro este sector está encaminado al crecimiento y adaptación tecnológica.

De acuerdo con la afirmación de Patricio Ramon, Socio de Risk Assurance de PwC Ecuador en 2022 hace hincapié en que "Los avances en materia de ciberseguridad empujan a organizar nuevas formas de trabajo en el comercio electrónico. No se trata únicamente de adquirir un software o equipos, sino también de elaborar estrategias de defensa" **(Ramon, 2022)**.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad existen diferentes sistemas que se mantienen conectados de manera electrónica con la finalidad de brindar información que es considerada de disponibilidad alta, entre estos sistemas tenemos los repositorios digitales, los sistemas financieros, la facturación, nómina, entre otros. La afluencia de usuarios, la manera en cómo la información es almacenada o las migraciones de información a la nube son hoy en día uno de los blancos primordiales, de acuerdo a la **(Revista IT AHORA, 2023)** de Ecuador, la oferta de cómputo y almacenamiento que las empresas ecuatorianas están considerando adquirir o migrar, se estimó que durante el 2022 solo el 31% de las empresas contaban con nube privada, 25% usan la nube pública, 11% mantiene una gestión de data centers propios y este porcentaje está proyectado en aumento los próximos años con la transformación digital, por lo cual es relevante vela por la función de ciberseguridad.

Ilustración 1: Oferta de Cómputo y Mantenimiento en Ecuador - (Revista IT AHORA, 2023)

La empresa de Seguridad Cibernética Kaspersky detalló que durante agosto del 2022 hasta agosto del 2023 se detectaron alrededor de dos millones de ataques en toda Latinoamérica, según

este informe Ecuador ocupa el cuarto lugar dentro de los países más vulnerados y a nivel mundial durante el 2023 con un 19.02% se tiene a Ecuador dentro de los 20 de países donde los usuarios enfrentan el mayor riesgo de ataques online.

TOP 10 countries and territories where users faced the greatest risk of online infection

	Countries and territories*	%**
1	Taiwan	24.41
2	Greece	24.12
3	Belarus	22.65
4	Algeria	22.64
5	Turkey	22.54
6	Serbia	22.09
7	Tunisia	21.17
8	Moldova	21.10
9	Nepal	20.99
10	Bangladesh	20.81
11	Sri Lanka	20.47
12	Bosnia and Herzegovina	20.20
13	Portugal	19.87
14	Qatar	19.62
15	Morocco	19.50
16	Ecuador	19.02
17	Philippines	18.55
18	Mongolia	18.51
19	Peru	18.36
20	Russian Federation	18.22

Ilustración 2: TOP 20 de Países que enfrentan mayor riesgo online - (Kaspersky, 2022)

En 2023, se ha estimado critico al Sector Agroalimentario pues según declara la "Revista IT AHORA" mediante datos estadísticos que más del 60% de las PYMES de industria o productos de consumo en el país han sido víctimas de ataques cibernéticos en el último año. **(Revista IT AHORA, 2023)**

OBJETIVOS DE LA INVESTIGACIÓN

OBJETIVO GENERAL

Analizar la necesidad de la función de ciberseguridad que ayude a cumplir con los componentes robustos de seguridad de un área de tecnológica en empresas pymes del sector Agroalimenticio de Daule.

OBJETIVOS ESPECÍFICOS:

- Examinar los diferentes tipos de ataques que se presentan actualmente en las empresas agroalimenticias de Daule.
- Identificar los que ataques que mayormente existen y su relevancia dentro la organización.
- Evaluar las medidas de mitigación o prevención de ciberseguridad que han empleado las empresas del sector.
- Presentar una propuesta de mejoras tecnológicas para la elusión de ataques de ciberseguridad.

MARCO TEÓRICO:

Con la digitalización que el país ha venido implementando en diferentes sectores y aspectos luego de pandemia, es indudable que los sectores de la agroindustria no traten de alinearse a esta actualización para mantenerse en vanguardia tecnológica o mejorar su eficiencia y productividad, aunque esto conlleve a un incremento en la exposición de ciber amenazas.

Cada día el tema de seguridad de la información y activos tecnológicos es un tema que cobra más relevancia, sin embargo, muchas veces puede ser complicado para las entidades pequeñas tener en claro los parámetros claves que se necesitan dentro de un ambiente de tecnología y esto origina deficiencias en sus controles de accesos, cambios a programas o bases de datos e incluso sus redes estén totalmente vulnerables a intrusiones externas de sus usuarios**.**

Es por esto que la ex ministra de telecomunicaciones, Viviana Maino presento el siguiente argumento, en su plan de estrategia nacional de ciberseguridad

"Las tecnologías digitales son indispensables para un Ecuador moderno, potenciando cada vez más nuestras empresas, nuestros servicios y nuestra administración públicos, y ofrecen oportunidades para que cada ciudadano se beneficie de la transformación digital. Como país hemos hecho esfuerzos en los últimos años para ampliar y mejorar el acceso a Internet de nuestra población, empresas y administración pública en todo el país y para acelerar el desarrollo económico y social en toda la sociedad" (Maino, 2022, pág. 7)

Con el presente marco teórico se tiene como objetivo brindar las bases de teoría y conceptos afines a la ciberseguridad, tomando en cuenta las normativas o practicas actuales relevantes dentro del entorno del sector agroalimentario de Daule.

La ciberseguridad ha ganado gran auge en los últimos años y es el punto clave de inversión de las entidades grandes y pequeñas a nivel mundial, está definida como "la ciencia de la computación encargada del desarrollo y la implementación de los mecanismos de protección de la información y de la infraestructura tecnológica." **(Christian Camilo Urcuqui, Melisa Garcia Peña, Jose Luis Osorio, Andrés Navarro, 2018)**. Debido a que su principal objetivo es mantener o preservar la confidencialidad, integridad y la continuidad de la información manejada bajo cada entidad, pues como indica el Socio de Risk Assurance Patricio Ramón "Ya se toma conciencia de que se requiere más allá de la infraestructura, que el perímetro ya no es solo la infraestructura o la nube. Ahora, el usuario es un nuevo perímetro que hay que proteger'' **(Ramon, 2022)**.

Una de las aliadas de la ciberseguridad es la "Seguridad de la Información" que hace énfasis en proteger la información de una entidad en cualquiera de sus formas como escrita, óptica, digital, etc. ante cualquier perdida o vulneración por ende la afectación a esta incide de manera directa. Además, va en conjunto de la "Seguridad Informática" que se relaciona netamente a respaldar y asegurar los sistemas de información automatizada.

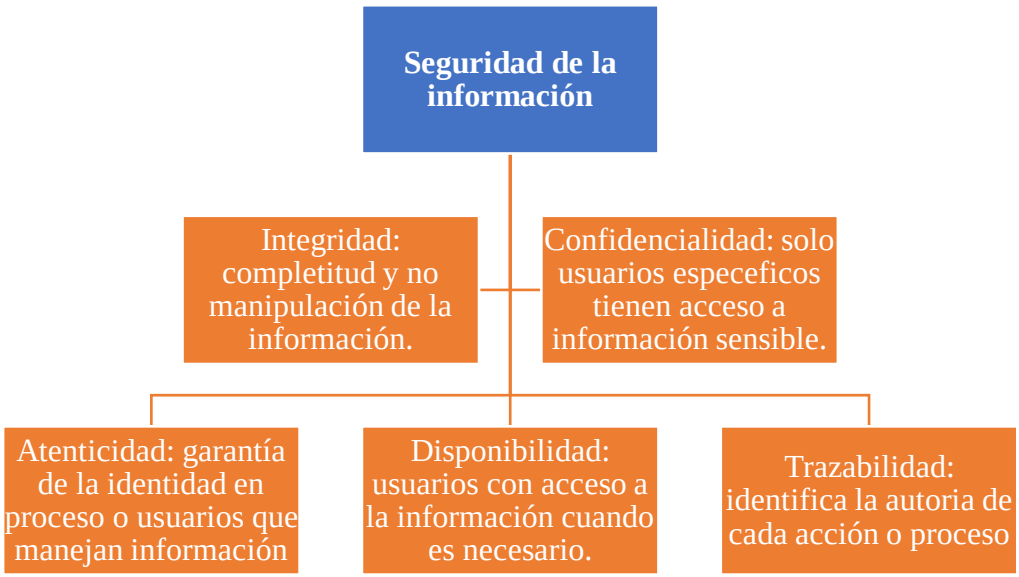

Ilustración 3: Pilares de la Seguridad de la Información – fuente: propia

La gestión de la seguridad de seguridad de la información es el conjunto de actividades para asegurar la madurez de la entidad de acuerdo con su seguridad con la finalidad de analizar los riegos y gestionarlos.

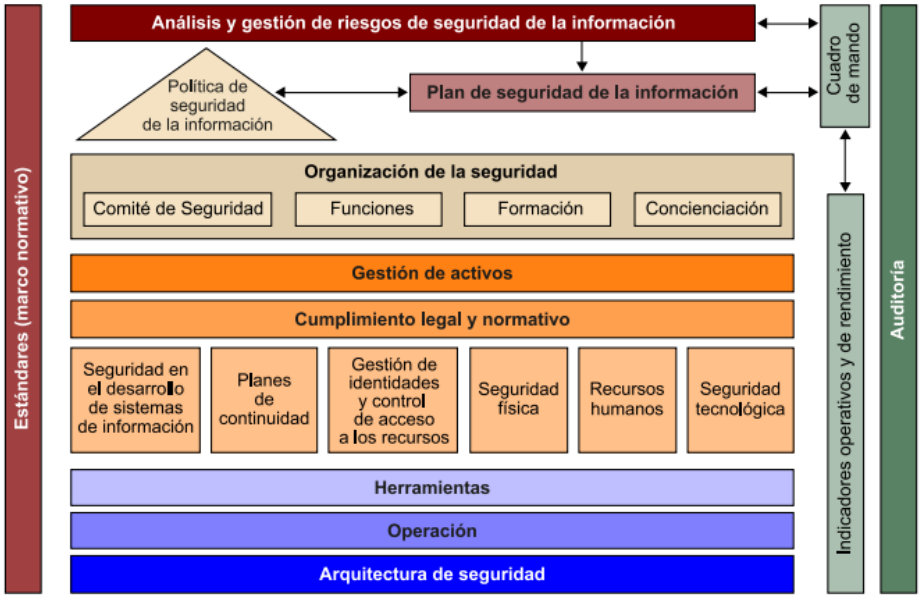

Ilustración 4: Proceso de la Gestión de Información (Gui, 2019)

De igual manera es clave mencionar los niveles de seguridad que se debe tener en las redes de estas entidades para estar protegidos ante ataques al entorno tecnológico, es importante saber que la seguridad una red puede combinar diferentes niveles de defensas en el perímetro para mantener los pilares de seguridad de la información intactos por este motivo se puede definir dos tipos de seguridad descritas de la siguiente manera:

SEGURIDAD FÍSICA: de acuerdo con lo que menciona Rubén Bustamante "La seguridad física se refiere a los controles y mecanismos de seguridad dentro y alrededor de la entidad o su centro de cómputo, así como los medios de acceso remoto" **(Sánchez, 2008)**, en pocas palabras ir orientado en proteger el hardware y los diferentes medios de almacenamiento de la data. La seguridad física se puede ver afectada por desastres, incendios, mala protección de los equipos (nivel de humedad menor a 65%), inundaciones y danos en el cableado.

SEGURIDAD LÓGICA: Este tipo de seguridad, según lo acotado por Rubén Bustamante "Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a las personas autorizadas" **(Sánchez, 2008)**

1. Controles de Acceso: estos deberían ser aplicados dentro de todos los sistemas, aplicativos, bases de datos o red que sean utilizado por la empresa y sus usuarios, debe tener la correcta identificación ligada a la autenticación con la finalidad de tener un mejor seguimiento de la actividad del usuario.

2. Identificación: está asociado al rol que se otorga según la función que va a cumplir el usuario, tiene mayor relevancia para detectar las actividades no autorizadas y tener el registro adecuado de cada transacción. Estas deben desactivadas siempre que el empleador sea desvinculado o modificado en casos de ascensos.

3. Roles: los roles son fundamentales para no tener problemas de segregación de funciones, es decir que la misma persona que hace cambio no puede tener todos los accesos o controles de los aplicativos dentro de otras áreas, etc. Deben estar asociados al rol que se le encarga al usuario desde que es contratado.

4. **Control de Acceso Interno:** se basa en el uso de buenas contraseñas para proteger las aplicaciones y datos. Se recomienda que estas sigan buenas prácticas como incluir mayúsculas, minúsculas, números, cambio frecuente.

5. **Transacciones:** están relacionadas con los controles que se siente al realizar o aplicar cambios dentro los aplicativos o sistemas de la empresa.

6. **Limitación a servicios:** implica una seria de configuraciones del administrados para definir quienes tienen acceso a modificación de los módulos de aplicaciones, además de los controles de lectura, escritura, ejecución, borrado, creación o búsqueda.

En cuestión de redes, deberían contemplar el uso de equipos que estén encaminados a la seguridad de estas como pueden ser redes LAN (Local Area Network) o WAN (Wide Area Network), para cada entidad financiera sea privada o gubernamental, por tal motivo es importante comprender que componentes básicos de una red sencilla como:

1. Routers: " Los routers permiten que todas las computadoras en red compartan una única conexión a Internet y actúa como distribuidor. Analiza los datos que se envían a través de una red" **(CISCO, 2021)**

2. Switch: "Un switch actúa como un controlador, que conecta computadoras, impresoras y servidores a una red en un edificio o campus. " **(CISCO, 2021)**

3. Firewalls: "dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. " **(CISCO, 2021)**

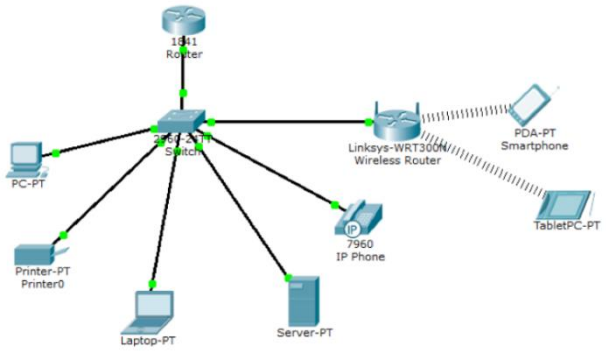

Ilustración 5: Red LAN - Fuente: propia

4. Access points: "permite que los dispositivos se conecten a la red inalámbrica sin cables, actúa como un amplificador para su red. " **(CISCO, 2021)**

A su vez, se debería tomar en cuenta el modelo de referencia con el cual se va a trabajar la red en mención ya que incorporan una arquitectura idónea contiene todas las características que pueden ser incorporadas a los sistemas. Para ello tenemos el modelo de referencia OSI basado en sistemas abiertos y conlleva la comunicación entre otros sistemas, basado en que función va a realizar cada capa y no acumular todas las acciones bajo una misma capa.

Arquitectura de Capas de TCP/IP	**Protocolos de Ejemplo**	**Dispositivos**
Aplicación, Presentación y Sesión (Capas 5-7)	Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP	Clientes, Firewalls
Transporte (Capa 4)	TCP, UDP	Clientes, Firewalls
Red (Capa 3)	IP	Router
Enlace de datos (Capa 2)	Ethernet (IEEE 802.3), HDLC	Switch, Punto de Acceso Inalámbrico, Modem, Modem DSL
Física (Capa 1)	RJ45, Ehternet (IEEE 802.3)	Hub, Repetidor, Cables

Ilustración 6: Capas del Modelo OSI - Fuente: (Cisco, 2018)

Adicional a esto, se cuenta con el modelo TCP o UDP que son protocolos de enrutamiento que funcionan básicamente agregando rutas a los routers en su tabla de enrutamiento para la subred direccionada y esta configuración es aprendida en cada router que compone la red para que pueda aplicarse el "next-hop" con la finalidad de selección la mejor ruta disponible y en caso de problemas con una ruta en específico pues la quita del enrutamiento para evitar loops.

El TCP es un protocolo basado en la CAPA 4 – Transporte del modelo OSI, donde se enfoca en recuperar errores, multiplexación por medio de puertos o control de flujos de sus segmentos. Su función se da multiplexando por números de puertos TCP y es basado en el

concepto "Socket" que debe contener una dirección IP, protocolo de transporte y un numero de puertos.

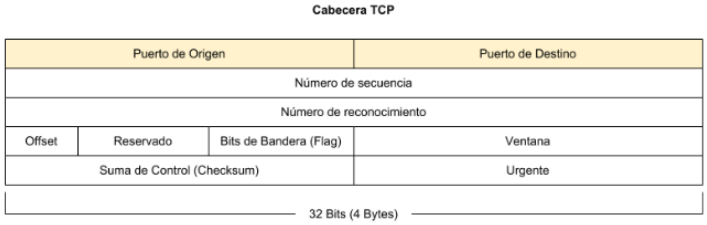

Ilustración 7: Cabecera TCP - (CISCO, 2021)

El protocolo UDP, también basado en la capa 4 de transporte del modelo OSI, tiene la función de multiplexar mediante puertos y transferir datos, además no está orientado a una conexión, por ende, no requiere intercambios de mensajes previos para iniciar la transferencia.

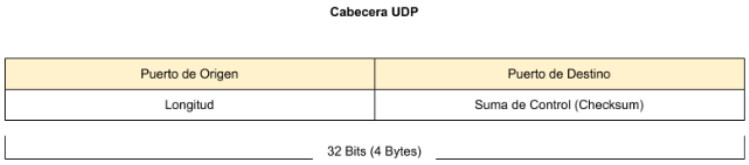

Ilustración 8: Cabecera UDP - (CISCO, 2021)

Como indica Esteban Bejarano en su artículo "La seguridad en redes está muy ligada a la continuidad del negocio" **(Esteban Bejarano,Carlos Andres Díaz, 2017).** Por eso era relevante tener en cuenta los conceptos básicos que precederán esta guía y entender que la seguridad global es la urgencia de proteger las redes contra ataques cibernéticos en todos sus niveles y así asegurar la disponibilidad del negocio.

Además, una red segura debe contar en la actualidad con equipos que aseguren la misma y que restrinjan el acceso que no está autorizado de acuerdo con el rol de usuarios, como se mencionó anteriormente uno de los componentes deben ser los firewalls que ayudan al bloqueo de las IPS, MAC o contenido del tráfico que entra o sale de nuestra entidad, sin embargo, al día de hoy también tenemos los siguientes:

IPS – Intrusion Prevention System: su función es prevenir y monitorear el tráfico de una red con la finalidad de detectar actividades anormales según políticas de la entidad, son relevantes para redes corporativas y gubernamentales por su rápida identificación de ciberataques.

WAF – Web App Firewall: basados firewalls que velan por el resguardo de aplicaciones netamente web de posibles ataques como pueden ser los DDoS.

VPN – Virtual Private Network: Son dos conexiones seguras de redes segura a través de internet que protege la información sensible del usuario.

Es importante asegurar o reforzar la seguridad lógica y física dentro del sector agroalimentario, un claro ejemplo de debilidad en estos pilares seria el ataque que tuvo la empresa agroalimentaria JBS FOODS, donde comprometieron gran cantidad de sus servidores ubicados en Australia y Estados Unidos debido a un ataque ransomware al no contar con el adecuado plan de recuperación, tuvo que suspender sus servicios por quince días y afrontaron un fuerte impacto en las ganancias económicas, además la empresa desembolso once millones de dólares para un rescate y acceder nuevamente a sus datos.

En su página oficial declaran que luego del evento, se tomaron las acciones necesarias como seguir su protocolo establecido por su equipo mundial de TI, suspensión de todos los servicios afectados y notificando a las autoridades de estado. Se indica que los servidores backup no fueron afectados, sin embargo, declaran que no tienen evidencia de que los datos de algún proveedor, cliente o empleados fueran comprometidos.

NORMAS O ESTÁNDARES PARA LA GESTION DE SEGURIDAD DE LA INFORMACIÓN

En la actualidad existen diferentes estándares internacionales para poder garantizar que la seguridad de la información sea adecuada, son aplicados en diferentes tipos de empresas sin importar la actividad o al sector que desempeñe, se describen los siguientes:

i) **Norma ISO - IEC 27000:** Según la organización de las ISO, esta norma está relacionada con:

" describir la visión general y el vocabulario de los sistemas de gestión de la seguridad de la información, haciendo referencia a la familia de normas de sistemas de gestión de la seguridad de la información (incluidas ISO/IEC 27003, ISO/IEC 27004 e ISO/IEC 27005), con términos y definiciones relacionados. " **(ISO: International Organization For Standardization, 2022)**.

En otras palabras, es un conjunto de estándares que brindan los fundamentos necesarios para un SGSI correcto. Para este estudio, tomaremos en cuenta las siguientes:

(a) ISO - IEC 27001: propone los lineamientos para el diseño de un sistema de gestión de seguridad de la información, incluyendo controles o procesos que mitiguen riesgos. Necesita ser certificada y documentación específica para ella.

(b) ISO – IEC 27002: brinda directrices que ayudan a la evaluación de los controles de ISO 27001, enfocándose en principios de iniciar o mejorar la gestión del SGSI.

ii) **CobIT: Control objectives for information and related technology:** se basa en un modelo que se centra su enfoque en controlar el gobierno de TI, abarca áreas de estrategia, diseño, operación y mejora de servicios continua.

iii) **ITIL: Information technology infrastructure library:** Es un marco que regula la gestión de servicios tecnológicos, enfocado en buenas prácticas. Actualmente se mantiene su versión cuatro que fue emitida en 2019, de acuerdo con Deloitte se encarga de dar las bases para la transformación digital y facilitar el empleo de las metodologías agiles. **(Roche, 2019)**

NORMATIVA LEGAL ECUATORIANA RELACIONADA A SEGURIDAD DE INFORMACIÓN.

Ecuador ha ido elaborando su normativa legar para la gestión de la información y medidas de ciberseguridad para todas las industrias dentro del territorio ecuatoriano. Se presentan algunas de las normas actuales y relevantes que se pueden ser consultadas en la página del MINTEL como:

1) ***Ley Orgánica de Protección de Datos Personales:*** Fue publicada dentro del registro oficial el 26 de mayo de 2021 y tiene la finalidad de garantizar el derecho a protección de la información personal de los ecuatorianos mediante regulaciones del uso y recolección de esta. Esta ley será aplicada a todo tipo de datos a nivel material y territorial, conlleva sanciones por incumplimiento. **(Asamblea Nacional , 2021)**

2) ***Acuerdo No 166 - Seguridad de Información:*** Propone políticas para gestionar la seguridad de la información dentro de las entidades públicas o privadas, se estima asignar un responsable para la supervisión de estas políticas y la gestión de riesgos. **(Acuerdo No 166, 2013)**

3) ***Acuerdo No. 006-2021 – Política de Ciberseguridad:*** Tiene el objetivo de crear un marco regulatorio que permita la buena gestión de los riesgos alineados a ciberseguridad, riesgos y la protección de los activos informativos, exigiendo a las entidades que identifiquen y evalúen proactivamente los riesgos y actualicen sus políticas continuamente. **(Acuerdo No 006-2021, 2021)**.

MARCO METODOLÓGICO

Métodos de investigación

La presente investigación emplea un nivel investigativo y descriptivo debido a que se conocerá la necesidad de comprender la practicas actuales y conceptos de la ciberseguridad en el sector agroalimenticio de Daule en el Ecuador. Cabe destacar, que este enfoque es crucial y relevante para lograr la identificación de las falencias que existen dentro del área tecnológica del sector mencionado y desarrollar una propuesta de mejora alineadas con las necesidades actuales de las industrias agroalimenticias en el país.

Tipo de investigación

El diseño de investigación contemplado para la presente es cualitativo, ya que permitirá exponer el estado actual de la ciberseguridad en el sector agroalimenticio del Cantón Daule, proporcionando una base consistente para el análisis. Por otro lado, empleará una investigación analítica para detalladamente estudiar cada punto o falencia a nivel de ciberseguridad dentro de las empresas del sector para brindar una propuesta para la correcta gestión dentro del área de tecnología, también comprenderá una investigación bibliográfica debido a la recopilación de información que resaltará las fuentes relevantes o conceptos para el presente con la finalidad de formular las correctas bases.

Técnicas e instrumentos

1. **Análisis documental:** Mediante la recolección documental fundamentada previamente, se procederá a analizar documentación visual para la correcta transcripción sobre la presente.

De acuerdo con estudios internacionales, se destaca al sector agro alimentario como un sector crítico y expuesto cibernéticamente, puesto que mantiene alrededor 2.5% del PIB europeo del conjunto de economía y se estima que un 25.5% del sector de manufacturas según el Ministerio de Agricultura, Pesca y Alimentación de España, lo que conlleva a uno de los sectores industriales y relevante para la economía de España y por esto atrae gran cantidad de ciber atacantes, debido al flujo de datos que manejan ligada a la industrialización.

Desde 2021 hasta la actualidad uno de los procesos dentro de las empresas agroalimentarias que sufren mayor afectación por ciber ataques son las cadenas de suministro, ya que sus áreas no presentan un nivel alto de ciber protección y por lo cual el nivel de impacto o daños suele ser elevado y repercute en el aspecto económico del mismo debido a las perdidas por paros en la producción.

Según un artículo español indica " El sector se encuentra en un momento de rápidos cambios" **(Fresno, 2024)**. Lo que indica que estas empresas están apresurándose a estar en vanguardia con la tecnología y están adaptando procesos de digitalización o implementando sistemas digitales como adecuación procesos con inteligencia artificial, robótica o IOT (internet de las cosas) entre otros.

Mediante este análisis se estima recopilar información acerca de las brechas o vulnerabilidades a las que se podrían exponer las empresas agroalimentarias de Daule con la

implementación de procesos cada vez más automatizados, contrastando así con empresas del sector de otras regiones o países, ya que hoy en día, este tipo de actualizaciones tecnológicas o de sus plataformas que no presenten un correcto paso a producción pueden ser debilidades o configuraciones vulnerables que puede propagar riegos a nivel de la empresa o de sus usuarios.

Se recolectó y estudió los procesos que dentro de la industria agroalimentaria tienen un despunte tecnológico y el cómo pueden ser vulnerados:

Riesgos Asociados a Nuevas tecnologías
Agricultura y Ganadería de Precisión
Inteligencia Artificial, IoT, Robótica, Espectrometría Multicanal. IP CAM,s. Drones. Satélite. Termografía. Medición RFID
• Ataques a equipos que almacenan o generan datos. • Captación de envío de datos no seguro. (man in the middle). • DoS con inhibidores de frecuencia
Almacenes automatizados
Robots móviles - Robots colaborativos - Plataforma SGA. Plataforma IA- CRM o ERP
• Vulnerabilidades PLC´s y HMI. Conexión IT-OT no segura. • Ausencia de segmentación redes. • Políticas acceso Internet insuficientes
Cuaderno Digital de Campo
WEB Apps o Dispositivos personales móviles (tablets/smartphones)
• Configuración insuficiente de conectividad o seguridad. • Sustracción de Identidad. • Debilidad en aplicaciones
Monitorización y tele gestión
RIA (Rich Internet Application) - - Inteligencia Artificial - Sensorización IoT - Gemelos Digitales
• Ataques DDoS • Vulnerabilidades en estaciones de trabajo y Servidores. • Configuración insuficiente de seguridad y conectividad.

• Falta de aislamiento de red OT (Operational Tecnology)
Robotización Líneas Producción
Robots, SCADA, PLC´s, HMI´s Plataformas MES
• Configuraciones por defecto de Controladores. • Sensores sin seguridad. • Políticas de Acceso a consolas de operación HMI

Tabla 1: Fuente: (Fresno, 2024) - Elaborado por autor.

Además, es clave recalcar que las pymes y las micro pymes del sector son las también un blanco para ciberataques como indica José Manuel Fresno, especialista en sistemas y ciberseguridad:

"El ciberdelincuente ha encontrado en las pymes un nicho en el que sus ataques obtienen un alto nivel de éxito al no tener que vencer medidas de seguridad complejas y robustas como las que se encuentran desplegadas en las grandes compañías. El resultado: 7 de cada 10 ciberataques en España se dirigieron a pymes" ***(Fresno, 2024)***.

ANÁLISIS DE LAS MEDIDAS DE MITIGACIÓN Y LOS ATAQUES MÁS PROPENSOS EN RELACIÓN CON LA CIBERSEGURIDAD DENTRO DE LOS PROCESOS DE LA EMPRESAS AGROALIMENTARIAS DE DAULE- ECUADOR.

De acuerdo con el autor Mata, una empresa del sector agroalimentario se puede definir como "una organización que participa directamente o como intermediaria en la producción agraria, procesamiento industrial" **(Mata, 2018)**. De igual manera, el Ministerio de Agricultura, Ganadería, Acuacultura y Pesca (MAGAP), define en 2006 a las empresas de agroindustria o agro alimentos como empresas que realizan un conjunto de actividades para el acondicionamiento,

transformación, conservación de los productos. Además, también conlleva las actividades que están relacionadas con la producción de bebidas, alimentos, entre otros **(Cortez, 2020)**

En el estudio ejecutado por Debbie Anchaluisa, se destaca que la industria agroalimentaria ecuatoriana ha venido experimentando cambios relevantes a nivel de estructuras de producción, aspectos sociales, ecológicos y tecnológicos **(Anchaluisa Guzmán, 2018)**. Con relación a los cambios dentro del ambiente tecnológico, en el estudio de Fernando Intriago, resalta que, en el sector agroalimentario o agroindustrial, se deberían efectuar mejoras en el uso de TICs y en toda su maquinaria inteligente y se ha convertido en una necesidad dentro de las empresas del sector en el país. A la vez, dentro de estos avances en tecnología se presentan una debilidad puesto que, al momento de ir tras nuevas tecnologías, sería difícil su implementación por no contar con los recursos económicos necesarios para poder aplicar cambios y tener robustez o aseguramiento de los nuevos sistemas tecnológicos aplicados. **(Intriago Mendoza, 2019)**

Actualmente el sector agroalimentario es uno de los pilares que genera mayor economía dentro del país, las empresas del sector agroalimentario en Daule tienen como finalidad que sus procesos industrializados sean cada vez más inteligentes ya que el Cantón en mención, a la actualidad es muy vulnerable en temas de ciberseguridad dentro de sus procesos estipulados y con funcionamiento establecido. Según la revista Forbes Ecuador, indica que para el 2025, el 45% de las organizaciones dentro de esta industrian habrán sufrido ataques en sus softwares en sus cadenas de suministro o producción **- (Forbes Ecuador, 24).**

Como expone Carlos Cortez en su investigación, se tienen 82 pequeñas empresas comprendidas en el sector agroalimentario dentro del sector de Daule, las cuales cuentas con sus

registros dentro del Ministerio de Agricultura, Ganadería, Acuacultura y Pesca (MAGAP) como parte de una población actual del sector para la posible utilización de esta investigación.

Empresas agroalimentarias de Daule

N°	**Nombre de agroindustria**	**Dirección**
1	AGRO. IND. ARROCERA El JIGUAL	RECINTO JIGUAL
2	JOSEFINA	LAS MARAVILLAS
3	SAN VICENTE	JIGUAL
4	JESUS DEL GRAN PODER	LOS LOJAS
5	LIBERTAD	JIGUAL
6	SAN ANTONIO	LOS LOJAS
7	ALVARADO	LAUREL
8	ROSITA	LOMA DE LEON
9	ROSA MARÍA	AV. PRINCIPAL
10	SAN IGNACIO	LOMA DE LEON
11	EL EDEN	AV. PRINCIPAL
12	SAN CARLOS	LA AURORA
13	DON HUMBERTO	Km. 2 ½ DAULE
14	YOLANDITA	Km. 12 ½ SAMBOR
15	FABRICIO	LAS MARAVILLAS
16	ROBERTO CARLOS	Km. 12 ½ SAMBOR
17	ANA ELVIRA	Km. 42 DAULE - G
18	ROSITA	JIGUAL
19	LAS MARAVLLAS	LAS MARAVILLAS
20	IND. ARROC RA NUEVO MILENIO	Km. 17 ½ LA PUNT
21	AMERICA	LAS MARAVILLAS
22	MARÍA BELEN	Km. 20 LA PUNTIL
23	LA PREFERENCA	LAS MARAVILLAS
24	CAPRICHO	JUAN BAUSTISTA
25	DIVINO NIÑO	COCAL
26	SANDRITA	JUAN BAUSTISTA
27	SAN ENRIQUE	LA T DE SALITRE
28	SAN VICENTE	Recinto EL PORVEN
29	LA PROMESA	LAS MARAVILLAS
30	LOS ÁNGELES	VIA A LA ALBORA
31	CONSUELO	CASCOL
32	SANTA RITA	VIA A LA ALBORA
33	DOÑA LETICIA	LIMONAL
34	RICHARD	VIA A LA ALBORA
35	SAN JACINTO	Recinto LA ALBOR
36	SANTA ROSA	LA T DE SALITRE
37	MI JESUS	LA T DE SALITRE
38	NARCISA	Recinto COCAL
39	SAN PEDRO	LA T VIA A GYE.
40	MARTHA VERONICA	Km. 17 ½ LA PUNTILLA
41	JHONNY GONZALO	BAJO GRANDE
42	AGRICOLA BATAN S.A.	Km. 38 VIA A DAULE
43	VIRGEN NARCISA DE JESUS	PAJONAL
44	LUZ AMERICA	NAUPE
45	AGRICOLA RONQUILLO	NAUPE
46	CARMITA	NAUPE
47	LINA MERCEDES	SANTA ROSA
48	LUIS ENRIQUE	Recinto FLOR MARIA
49	ARROCERA EL REY	HDA. LA ESPERANZA
50	CATHERINE THALIA	EL SALTO
51	VOLUNTAD DE DIOS	Km. 53 GYE/ SANTA LUCIA
52	NAYID GRACIELA	Km. 53 GYE/ SANTA LUCIA
53	LORENA PATRICIA	PREDIO SAN FRANCISCO
54	CHINA	DAULE
55	PATRICIA ALEXANDRA	Recinto EL TINTAL
56	ANGELITA	LAUREL
57	TRES HERMANOS	Recinto EL PORVENIR
58	MARGARITA CECILIA	Recinto SANTA ROSA
59	SARA PATRICIA	Recinto EL JIGUAL
60	DIOSELINA	Recinto LOS QUEMADOS
61	MERENGUE	Recinto LOS QUEMADOS
62	MONTE SINAI	Recinto COCAL
63	TIO ADAN	GUARUMAL
64	KATTY DEL CARMEN	Recinto LA LORENA
65	TRES HERMANOS	ENTRADA A CASCOL
66	VOLUNTAD DE DIOS	Km. 12 LA PUNTILLA
67	MARIA DE LOURDES	Km. 10 DAULE/ SANTA LUCIA
68	KATHERINE MERCEDES	LAUREL
69	FUENTES	LAUREL/ SABANA GRANDE
70	SANTA LUCIA	Recinto NAUPE
71	SAN VICENTE	Recinto YARUMI

72	SANTA CLARA	DAULE – SANTA I	*78*	LENY	Recinto GUARUMAL
73	SAN JOSE	Recinto PECHICHE/	*79*	KATTY NICOLK	Km. 54 GYE – SANTA LUCIA
74	FABIOLA	Km. 22 LA PUNTIL	*80*	SAN ANTONIO	Km. 13 LA PUNTILLA
75	SAN JOSE	Recinto PECHICHE/	*81*	SAN FRANCISCO	Recinto LA VUELTA/ LAUREL
76	SAN VICENTE	Recinto EL PORVEI	*82*	YANCO	Km. 54 GYE – SANTA LUCIA
77	GLORIA MATILDE	Km. 43 ½ GYE – DAULE			

Tabla 2: Empresas Pymes del Sector Agroalimentario de Daule - Elaborado por autor - Fuente: (Cortez, 2020)

En la actualidad estas empresas del sector agroalimentario en Daule, deberían estar actualizadas con procesos de industria 4.0, que según el artículo de Kirk Freire, son procesos desarrollados con el fin de que todos los procesos de producción dentro de estas empresas sean inteligentes y que se estima que para nuestro país se convierta en tendencia a mediano plazo ya que aún el panorama no es el correcto y se presentan tanto el país como las empresas de este sector agroalimentario en Daule muchas vulnerabilidades en los procesos, estructuras y funcionamiento en relación a ciberseguridad. **(Freire López, 2017)**, puesto que, muchas de estas empresas como se mencionó en la investigación de Intriago no tienen el presupuesto para llevar medidas de mitigación ante ataques de ciberseguridad de una manera especializada, en la tabla 3 se detallan los mecanismos o medidas de mitigación necesarias y los diferentes escenarios en los cuales son aplicados.

Mecanismos de Mitigación	**Escenarios de aplicación**				
	Gestión de acceso e identidad	Seguridad en el puesto de trabajo	Seguridad en aplicaciones y datos	Seguridad en los sistemas	Seguridad de la red
Software preventivo de malware y fraude		x	x	x	x
Auditoría interna y/o externa de sistemas	x		x		x
Certificación normativa		x	x	x	x
Contingencia		x	x	x	x
Control de acceso y autenticación	x				
Cumplimiento legal	x	x	x		
Inteligencia de seguridad			x	x	x
Prevención de fuga de información		x	x		x
Protección de las comunicaciones		x	x	x	x
Seguridad en dispositivos móviles		x			x

Tabla 3:Mecanismos de Mitigación de Ciberseguridad en empresas del Sector Agroalimentario en Daule. Elaborado por autor - Fuente: (Freire López, 2017)

CARACTERIZACIÓN Y RELEVANCIA DE LOS CIBERATAQUES QUE SE PRESENTAN EN EL SECTOR AGROALIMENTARIO EN DAULE.

Dentro de la ciberseguridad, se puede describir cualquier tipo de práctica que sea ejecutada por un persona natural u organizaciones para dañar, atacar o filtrar información o los sistemas en general. Uno de los ataques más recurrentes que se han podido presentar en las empresas agroalimentarias dentro del sector en mención, son los malwares que como indica en autor Kirk Freire en su artículo, son códigos maliciosos que actúan con la finalidad de dañar los sistemas de la información sin permisos o consentimientos de los usuarios. **(Freire López, 2017)**. Usualmente estos son ocasionados de manera remota.

De igual manera los autores Pulla y Padilla, indican en su informe Integración de Soluciones de Ciberseguridad, que con la transformación digital en las empresas de todo tipo sector del país, incluyendo el agroalimentario, conlleva a que las amenazas vayan creciendo a pasos agigantados y también indica que hay que poner atención a los malwares, dentro de ellos a los Ransomware ya que un ataque de estos puede afectar directa o indirectamente la economía, prestigio o confianza de una entidad. **(Pulla, Cristian Bolivar Bacuilima; Padilla Pineda, Willian Alfonso., 2023)**.

Entre ambos estudios se identifica que los ataques que pueden presentarse con mayor frecuencia y de mayor relevancia para este sector agroalimentario en Daule, mismo que está empezando a ser introducido al mundo tecnológico, son los siguientes:

I. **Virus comunes:** Son programas que alteran el código de otros para tomar el control de archivos dentro de un sistema, la velocidad de propagación es más baja que los gusanos.

II. **Caballos de troya:** Es un software que realiza acciones sin el consentimiento de los usuarios, robando información y permitiendo al atacante el acceso remoto al sistema, causa más daño que un virus común mencionado previamente.

III. **Spyware:** Programas que son diseñados con la finalidad de recopilar información privada sin el permiso de los usuarios y pueden manipular la navegación en internet.

IV. **Gusanos de red:** Es un tipo de programa maligno cuyo método de propagación es el internet o recursos de las redes, motivo por él se extiende rápidamente mediante correos electrónicos, mensajes instantáneos y busca afectar otros dispositivos dentro de la misma red.

V. **Ransomware:** Este tipo de malware esta caracterizado por bloquear el acceso de los archivos cifrados dentro de un sistema y suele exigir un rescate para restablecer el acceso.

VI. **Adware:** programas basados en mostrar anuncios no solicitados, especialmente en aplicativos gratuitos y estos pueden recolectar información personal del usuario dentro de la entidad.

VII. **Riskware:** Aplicaciones legitimas que pueden ser peligrosas si caen en los accesos o control equivocado, un claro ejemplo sería los programade control remoto o gestor de contraseñas.

PROPUESTA DE MEJORAS TECNOLOGICAS PARA LA ELUSIÓN DE CIBERATAQUES.

Esta propuesta de mejoras tecnológicas brindas las pautas que las pymes del sector agroalimentario del sector requieren para mejorar su área de tecnología de manera interna con la finalidad de prevenir ataques cibernéticos o tener un plan de contingencia ante cualquier amenaza.

1. DEFINIR QUE CONTEMPLA UNA AUDITORÍA INTERNA DE CIBERSEGURIDAD

Una auditoría de ciberseguridad conlleva evaluar en este caso las entidades del sector agroalimentario mediante el entendimiento del ambiente de TI, tener en claro y determinar en qué estado de ciberseguridad se encuentran y cuáles serían las falencias que están afrontando sus sistemas informáticos, los usuarios o sus políticas de seguridad como indica la firma PwC en su artículo Cybersecurity disclosures and the role of internal Audit "*En la actualidad, muchas empresas no están debidamente preparadas para revelar información sobre sus procesos de evaluación, identificación y gestión de los riesgos materiales de ciber amenazas"* **(Cyber & Privacy Innovation Institute PwC, 2023)**. Esta guía define como tener estos controles de manera interna por ende estarán basadas en la normativa de la ISO 27001.

1.1.1. OBJETIVOS Y PLANIFICACIÓN

Cuando realizamos el entendimiento del ambiente de TI, se procede a definir los criterios, recursos y herramientas a utilizar para llevar a cabo el propósito de esta y definir un cronograma para efectuar la auditora en el tiempo determinado.

1.1.2. RECOPILAR INFORMACIÓN – EVIDENCIAS

Se analiza y se solicitan evidencias a los usuarios del área de tecnología para evaluar con mejor enfoque los riesgos o amenaza a la que está expuesta la entidad. Los métodos claves para recopilar información son la documentación, evaluación de evidencias, revisión de políticas de seguridad, entre otros.

1.1.3. ANÁLISIS DE LAS EVIDENCIAS E INFORMACIÓN

A detalle estudia solo la información relevante de la entidad como su estructura organizacional de TI, objetivos del proceso tecnológico, inventarios de hardware o software, diagrama de redes, prueba de los controles de accesos y bitácoras de cambios a programas.

1.1.4. INFORME FINAL DE LA AUDITORÍA

En esta fase final se elabora el documento final donde se presentan los resultados, conclusiones y recomendaciones correctivas para la mejora continua de la seguridad informática, el mismo debe ser preciso y objetivo basado en las evidencias.

2. EVALUACIÓN MEDIANTE FORMULARIOS PARA EL ENTENDIMIENTO DE TI

Se elaboraron los formularios generales que pueden ser usados para realizar un entendimiento básico de las diferentes áreas de tecnología dentro de las pymes del sector agroalimentario para tener un amplio panorama de cómo está conformada a nivel factor humano y tecnológico.

2.1.1. FORMULARIO DE ENTENDIMIENTO DE TI

La finalidad de aplicar este formulario nos detalla las áreas y su responsable, además de entender la descripción de cargo y un poco de las políticas de seguridad o que aplicaciones maneja

y si existe algún tipo de interfaz manual o automática para cada proceso, todo para tener un mejor reconocimiento de nuestra área de tecnológica.

2.1.2. FORMULARIO DE HISTÓRICO DE INCIDENTES DE TI

Este formulario tiene como finalidad aplicar un acercamiento a las falencias de que ha presentado la entidad y por ende nos adentra a sus procesos correctivos y como mitigan las fallas que se les presentan. Es decir que no ayudara a llevar un seguimiento a fallas y ataques, que equipos fueron afectados, su causa, frecuencia y que acción fue aplicada para contingencia de futuros incidentes.

2.1.3. EVALUACIÓN DE TÉCNICAS DE CIBERSEGURIDAD

Abarca un recorrido a las operaciones y tecnología de la empresa, podremos analizar que tipos vulnerabilidad podemos presentar y según la dimensión de la empresa proponer diferentes pruebas de penetración o ethical hacking. Para esto se recomienda indagar sobre diagramas y accesos de red, revisión de firewalls, equipos, infraestructura y segregación de redes. Además, es clave tener definidos procesos de calendarización, y respaldo de información, planes de capacitación en relación con ciberseguridad y planes de contingencia o recuperación ante desastres.

3. IDENTIFICACIÓN DE PROBLEMAS

Basado en los formularios aplicados a los problemas más comunes que se catalogarían como deficiencias de TI son los siguientes:

- Deficiencia en la función de Segregación de funciones.
- No definir su organigrama y manual de funciones.

- Falta de políticas del área de tecnología.
- Sistemas operativos obsoletos.
- Falta de un diagrama de redes adecuado.
- No contar con el mapeo de sus aplicativos.
- Mal control de accesos o cambios a sus aplicativos, sistemas, bases de datos.
- No programación de pruebas para prevención de ataques como implementación de hacking ético, pruebas de pentesting o no documentación de su plan de continuidad y contingencia.

4. PLAN DE CONTIGENCIA

Para las entidades de este sector debe ser primordial contar con un plan de contingencia ya que es una de las herramientas de planificación o gestión de los procedimientos a seguir ante ataques o vulneraciones y es clave para velar por la integridad de la información.

Por este motivo la finalidad de usarlo es preparar a la entidad y a sus usuarios, pues si un ciberataque se presenta el sistema en general se ve comprometido y se debe responder de forma correcta.

CONCLUSIONES

En este análisis, se concluye que las empresas del sector agroalimentario a nivel mundial como en el país, actualmente están propensas a un riesgo cibernético o debilidades en su infraestructura debido a la actualización de procesos acompañados de la tecnología que pueden ocasionar arduas consecuencias si las medidas necesarias de prevención como auditar de manera interna no son tomadas.

Mediante la presente, se resalta que las pequeñas o medianas empresas del sector recién están teniendo un despunte tecnológico, por esta razón se examinaron e identificaron los tipos de ataques a los que están propensas son vulnerables y se concluye que, a la actualidad, el ataque más relevante al que pueden estar expuestas por falta de medidas de seguridad robusta, son los Ransomware.

Dentro del artículo también se evaluaron las distintas debilidades relevantes a las que están expuestas las empresas de dicho sector en el área tecnológica, entre estas tenemos la falta de políticas de seguridad, sistemas obsoletos, controles de accesos y contraseñas deficientes, carencia de planes de contingencia o recuperación ante desastres. A la vez, se presentaron mecanismos de mitigación y los diferentes escenarios de aplicación que las empresas del sector han empleado.

Finalmente, el objetivo de esta guía se cumple ya que satisface a la necesidad de las entidades agroalimentarias de Daule, brindado estrategias para la gestión y corrección de las falencias que se presentan dentro de su área de tecnología, proponiendo lo necesario para conocer su ambiente de TI, como están gestionando las seguridades físicas o lógicas y desde ahí empezar a fortalecer sus debilidades permitiendo estar en constante evolución a través de la mejora continua.

Bibliografía

Acuerdo No 006-2021. (2021). *POLÍTICA NACIONAL DE CIBERSEGURIDAD - PNC.* Quito: Memorando Nro. MINTEL-SGERC-2021-0134-M.

Acuerdo No 166. (2013). *Politica de Seguridad de la Información.* Quito.

Anchaluisa Guzmán, D. S. (Septiembre de 2018). ANÁLISIS DEL IMPACTO DE APLICACIÓN DE LA NIIF 9 EN LA CONTABILIZACIÓN DE CUENTAS POR COBRAR EN UNA EMPRESA AGROINDUSTRIAL DE LA PROVINCIA DEL GUAYAS. Guayaquil, Guayas, Ecuador.

Asamblea Nacional . (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS.* Quito.

Christian Camilo Urcuqui, Melisa Garcia Peña, Jose Luis Osorio, Andrés Navarro. (2018). *Ciberseguridad: un enfoque desde la ciencia de datos.* Cali: Editorial Universidad Icesi.

Cisco. (2018). *Conceptos básicos de seguridad de red para pymes.* Obtenido de Cisco.com: https://www.cisco.com/c/dam/global/es_es/solutions/small-business/pdf/smb_network-security_checklist.pdf

CISCO. (2021). *https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/networking-basics.html*.

Cortez, C. A. (Junio de 2020). Sistema de información gerencial para el control de costos de empresas del sector agroindustrial del cantón Daule. Guayaquil, Guayas, Ecuador.

Cyber & Privacy Innovation Institute PwC. (Agosto de 2023). *Cybersecurity disclosures and the role of internal audit.* Obtenido de PwC: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/sec-final-cybersecurity-disclosure-rules/cybersecurity-and-internal-audit.html

Esteban Bejarano,Carlos Andres Díaz. (2017). *Seguridad en Redes.* 2017: Fundación Universitaria del Área Andina -Areandino.

Forbes Ecuador. (2024 de Enero de 24). *Por qué los ciberataques a la cadena de suministro serán más frecuentes en 2024.* Obtenido de Forbes Digital: https://www.forbes.com.ec/innovacion/por-ciberataques-cadena-suministro-seran-mas-frecuentes-2024-n47111

Freire López, K. B. (18 de Septiembre de 2017). Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad. Guayaquil, Ecuador.

Fresno, J. M. (09 de Enero de 2024). *Artica*. Obtenido de Artica: https://www.articai.es/ciberseguridad-en-la-industria-agroalimentaria/

Gui, S. G. (2019). *Introducción a la Seguridad de la Información .* Cataluña: Universitat Oberta de Catalunya.

Intriago Mendoza, F. R. (06 de Mayo de 2019). La mecanización agrícola y su impacto en el desarrollo agropecuario del Ecuador. Manabí, Ecuador.

ISO: International Organization For Standardization. (2022). *ISO/IEC 27000: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Obtenido de ISO: Online Browsing Platform: https://www.iso.org/obp/ui/en/#iso:std:82875:en

Kaspersky. (2022). *Boletín final de seguridad de Kaspersky .* Obtenido de Kaspersky: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2022_sp_final.pdf

Maino, V. (2022). *ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR.* Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf

Martín, J. (18 de Julio de 2022). *La ciberseguridad se hace fuerte en la cadena agroalimentaria.* Obtenido de Unir: https://www.unir.net/empresa/revista/ciberseguridad-industria-alimentaria/

Mata, C. A. (ABRIL de 2018). ANÁLISIS DEL CONTROL DE CALIDAD EN LOS PROCESOS DE ALMACENAMIENTO Y CONSERVACIÓN DE ARROZ Y MAÍZ EN LAS EMPRESAS AGROINDUSTRIALES DEL CANTÓN DAULE. GUAYAQUIL, ECUADOR.

Pulla, Cristian Bolivar Bacuilima; Padilla Pineda, Willian Alfonso. (2023). *Intragración de Soluciones de Ciberseguridad En Software Libre Como Alternativa Accesible para Pymes.* Cuenca, Ecuador. .

Ramon, P. (12 de Diciembre de 2022). Ciberseguridad: planificar la estrategia de defensa. (M. Alvarado, Entrevistador)

Revista IT AHORA. (22 de Abril de 2023). *Es momento de elevar la Ciberseguridad en las PYMES en Ecuador.* Obtenido de IT Ahora: https://itahora.com/2024/04/22/es-momento-de-elevar-la-ciberseguridad-en-las-pymes-en-ecuador/#:~:text=El%20escenario%20digital%20en%20Ecuador,cibern%C3%A9ticos%20en%20el%20%C3%BAltimo%20a%C3%B1o.

Roche, J. (2019). *ITIL V4.* Obtenido de Deloitte: https://www2.deloitte.com/es/es/pages/technology/articles/itil-v4-que-hay-de-nuevo-viejo.html

Sánchez, R. B. (2008). *Seguridad en Redes.* Universidad Autonoma del Estado de Hidalgo.