Vigilada Mineducación

CARACTERIZACIÓN DE LA CIBERSEGURIDAD DE ACTIVOS DIGITALES EN EMPRESAS EXPORTADORAS DE CAFÈ EN EL VALLE DEL CAUCA – COLOMBIA, AÑO 2024

CHARACTERIZATION OF CYBERSECURITY OF DIGITAL ASSETS IN COFFEE EXPORTING COMPANIES IN THE CAUCA VALLEY - COLOMBIA, YEAR 2024

.

Autor:

JORGE HUMBERTO MAYORGA SANCHEZ

SANDRA LORENA GÓMEZ CARDONA

UNIVERSIDAD EAFIT

ESCUELA DE ADMINISTRACIÓN

MAESTRÍA EN ADMINISTRACIÓN DE RIESGOS - MBA

PEREIRA

2024

CARACTERIZACIÓN DE LA CIBERSEGURIDAD DE ACTIVOS DIGITALES EN EMPRESAS EXPORTADORAS DE CAFÈ EN EL VALLE DEL CAUCA - COLOMBIA, AÑO 2024

CHARACTERIZATION OF CYBERSECURITY OF DIGITAL ASSETS IN COFFEE EXPORTING COMPANIES IN THE CAUCA VALLEY - COLOMBIA, YEAR 2024

.

Autor:

JORGE HUMBERTO MAYORGA SANCHEZ

SANDRA LORENA GÓMEZ CARDONA

Director:

JORGE HARLEY GUERRERO, P.H.D

Trabajo de grado para optar al título de:

MAGISTER EN ADMINISTRACIÓN DE RIESGO

UNIVERSIDAD EAFIT

ESCUELA DE ADMINISTRACIÓN

MAESTRÍA EN ADMINISTRACIÓN DE RIESGOS - MBA

PEREIRA

2024

TABLA DE CONTENIDO

LISTADO DE TABLAS

Resumen

Esta investigación, como objetivo principal, describe la manera en que se encuentran establecidos los procesos de ciberseguridad de los activos digitales en las empresas exportadoras de café en el municipio de Cartago. Lo anterior encaminado a presentar recomendaciones según los resultados arrojados. El marco teórico presenta una amplia gama de planteamientos y de postulados vinculados a los temas de ciberseguridad, los activos digitales, y la gestión del riesgo. Su aspecto metodológico hace referencia a un tipo cualitativo, de la mano de la naturaleza exploratoria - descriptiva de la misma, que, en conjunto con la aplicación de una entrevista semiestructurada, permitieron a los investigadores responder los objetivos planteados.

Los resultados que arrojó el proceso de indagación permiten indicar que, a pesar de que en las diferentes empresas indagadas se llevan acciones incipientes relacionadas a la ciberseguridad de los activos digitales, se puede afirmar que no existe una cultura de ciberseguridad, y que aspectos como el conocimiento de los activos digitales, la evaluación de riesgos, las políticas y los protocolos de ciberseguridad, la capacitación y la concientización, las herramientas y las tecnologías, y por último, el cumplimiento normativo, se encuentran establecidos de manera muy incipiente en este sector empresarial, destacándose que en solo algunas empresas, todo lo vinculado a la ciberseguridad lo realizan para el marco de SCS BASC, y/o el SGCS Sistema de Gestión de Control y Seguridad. Por esto se hace necesario presentar las recomendaciones, para que, de esta manera, estas empresas le brinden la importancia que se debe a la ciberseguridad de los activos digitales.

Palabras clave: Activos Digitales, Ciberseguridad, Empresas, Exportadoras,

Summary

The main objective of this research is to describe the way in which the cybersecurity processes of digital assets are established in coffee exporting companies in the municipality of Cartago. The above is aimed at presenting recommendations according to the results obtained. The theoretical framework presents a wide range of approaches and postulates linked to cybersecurity issues, digital assets, and risk management. Its methodological aspect refers to a qualitative type, hand in hand with its exploratory - descriptive nature, which, together with the application of a semi-structured interview, allowed the researchers to respond to the stated objectives.

The results produced by the investigation process allow us to indicate that although, in the different companies investigated, incipient actions related to the cybersecurity of digital assets are carried out, it can be stated that there is no culture of cybersecurity, and that aspects such as knowledge of digital assets, risk assessment, cybersecurity policies and protocols, training and awareness, tools and technologies, and finally, regulatory compliance, are established in a very incipient way in this sector. business, highlighting that in only some companies, everything related to cybersecurity is carried out within the framework of SCS BASC, and/or the SGCS Control and Security Management System. For this reason, it is necessary to present recommendations so that these companies give the importance due to the cybersecurity of digital assets.

Keywords: Digital Assets, Cybersecurity, Companies, Exporters,

1.INTRODUCCIÓN

A nivel organizacional, la administración de riesgos se constituye en un aspecto de gran relevancia al momento de garantizar la sostenibilidad y la continuidad de las empresas, al tiempo que se protegen sus activos y su reputación. Para Auditool (2011), esta administración es importante debido a que a través de ella se optimizan los recursos vinculados al patrimonio institucional y a la seguridad de la organización. Por ende, es importante contar con las herramientas suficientes para cuidar los patrimonios que tanto les ha costado a las empresas consolidar.

Partiendo de lo anterior, y prosiguiendo con Auditool (2011), entre los componentes de este tipo de administración se ubica la identificación, evaluación, control y monitoreo y revisión de los riesgos. En el caso del componente de la identificación, se desglosa el establecimiento de riesgos de índole financiero, estratégico, políticos, reputacionales, legales, operativos, entre otros. Entre los operativos se derivan riesgos de fraude, los de cadena de suministro y los tecnológicos, siendo estos últimos los relacionados a los sistemas de orden informático, las fallas de los softwares, los ciberataques, entre otras situaciones.

En lo concerniente a las organizaciones del sector cafetero en Colombia, y tomando como referente lo expuesto por Revista Portafolio (2015), estas se encuentran expuestas en su mayoría a riesgos financieros y operativos, especialmente a consecuencia de la falta de mano de obra y de los fluctuantes cambios en los precios del producto. En la revisión de la literatura no se evidencia sobre riesgos tecnológicos en este sector, lo cual llama la atención debido al impacto económico que representa esta actividad en el país. En este orden de ideas, y según el Portal Concafé (2023), en el año 2020 las exportaciones de este producto alcanzaron una cifra astronómica de 13.9 millones de sacos de 60kg, equivalente a una cantidad de 2,654 millones de dólares estadounidenses, generando la inquietud sobre el manejo que este sector económico le brinda a la ciberseguridad de sus activos digitales, que, a su vez, es una de las columnas de su patrimonio.

2.SITUACIÓN OBJETO DE ESTUDIO

En la actualidad, la tecnología es un aliado estratégico para el desarrollo de las actividades en cualquier empresa. Por medio de esta, se puede realizar un sinfín de procesos, entre los que se pueden encontrar: la contabilidad y finanzas, análisis de datos, marketing digital, automatización de los procesos, logística y gestión de la cadena de suministros, entre otros. A consecuencia de que, en la revisión documental, no se encontró mucho material sobre la manera en que las empresas del sector cafetero en Colombia llevan a cabo los procesos de ciberseguridad de su patrimonio digital, se hace necesario indagar la manera en que estas desarrollan los procesos vinculados a la protección de su patrimonio digital, especialmente la de sus activos digitales.

Relacionado al tema, se presenta lo expuesto por la Policía Nacional de Colombia (2020) sobre el cibercrimen en el país. De esta manera se expone que en el año 2019 se presentaron un total de 17.531 crímenes de naturaleza cibernética, destacándose el hurto por medios informáticos en primer lugar y que hace referencia al hurto de dinero que se encuentra en las cuentas bancarias; en el segundo lugar se muestra la violación de datos personales, convirtiéndose esto en una amenaza para las empresas y los ciudadanos por medio del robo de la identidad; en el tercer puesto se ubica el acceso abusivo a sistemas informáticos, que consiste en comprometer los sistemas de orden informático, alcanzando el acceso a los mismos y; por último, la transferencia no consentida de activos, ejemplificando una conducta criminal que se caracteriza por la sustracción de dinero o la transferencia de importantes activos financieros de las víctimas.

Entre las poblaciones de mayor exposición a este tipo de ataques, la Policía Nacional de Colombia (2020) ha identificado que la mayoría de estos se encuentran dirigidos a entidades o personas que representen un factor de desarrollo económico de gran envergadura. Así, se muestra al sector de las pymes (pequeñas y medianas empresas), entidades de orden financiero, y grandes compañías de distintas actividades económicas. Una de las tendencias de los ciberataques hace referencia a lo conocido como Ataques BEC. Prosiguiendo con lo establecido por la Policía Nacional de Colombia (2020), estos se constituyen de una de las amenazas de mayor peso a la cadena de suministros de las empresas, siendo uno de los pilares de la cotidianidad y el funcionamiento de las empresas. Por lo anterior, es necesario que los procesos comunicacionales con los proveedores externos, socios, aliados estratégicos o clientes, se desarrollen en entornos que se caractericen por su seguridad y confianza, garantizando de esta manera la integridad de los correos

electrónicos, los servicios de mensajería instantánea que se utilicen, las cuentas bancarias, las bases de datos, movimientos bancarios, entre otros aspectos.

En Colombia, los montos promedio de las pérdidas por estos ataques comprende cifras entre los 300 y 5.000 millones de pesos, según el tamaño de la empresa atacada. De igual manera, las modalidades de mayor uso son la suplantación del gerente y la suplantación de los clientes. Otra de las tendencias de los ciberataques hace referencia a los Ransomware. Para IBM (2024), estos se constituyen de un software malicioso (malware) que se encarga de restringir el acceso a los datos o los sistemas informáticos, en su mayoría a través de los cifrados de los archivos, para luego solicitar un pago generalmente por medio de criptomonedas para la restauración del acceso a la información o la liberación del sistema. Este crimen es común en personas naturales y empresas. Según datos de la Policía Nacional de Colombia (2020), el país presentó el 30% de estos ataques en Latinoamérica en el año 2020, seguido de Perú con un 16%, México en un 14%, Brasil con un 11%, y, por último, Argentina en un 9%.

El ataque DDOS, es otro tipo de ciberataque en el que distintos sistemas comprometidos se usan para la inundación de un servidor, un servicio o una red que presente gran flujo de tráfico, esto con el objetivo de que el servicio se convierta en inoperable. La consecuencia de lo anterior, es que el servidor se sobrecarga, por lo cual los usuarios no pueden acceder a este, generando situaciones como la pérdida de los ingresos y daños a la reputación de la empresa afectada. Tomando datos de la Policía Nacional de Colombia (2020), en el país en el año 2020 se reportaron una cantidad de 170 ataques de esa índole en varios tipos de empresas. Como último tipo de ataque, se presenta el Malware o software malicioso, siendo este caracterizado por ser un programa o un archivo que se concibe para hacer daño o comprometer el adecuado funcionamiento de los dispositivos, los sistemas o las redes. Este puede tener forma de virus, gusano, troyano, Spyware, Adware, entre otros. Pueden causar una gran cantidad de dificultades, entre las que se pueden encontrar la pérdida de los datos, llegando al robo de la información personal o de la empresa, al igual que la interrupción de los servicios que ofrece la organización. Para la Policía Nacional de Colombia (2020), este tipo de ataque ha crecido hasta un 612% en los últimos años en el país.

Lo expuesto hasta el momento, son solo algunas de las situaciones a las que las empresas se ven expuestas si no realizan adecuados procesos de ciberseguridad. En el caso de las empresas exportadoras de café, estas se destacan por manejar una cantidad significativa de información digital para el desarrollo de sus procesos de comercialización. Según la Federación Nacional de Cafeteros de Colombia (2023), en el mes de abril de este mismo año, se presentaron exportaciones por una cantidad de 213 millones de dólares, siendo los principales destinos los países de Estados Unidos, Canadá y Bélgica. Lo anterior sugiere realizar, por medio de

análisis de naturaleza descriptiva, la caracterización de los procesos de ciberseguridad de los activos digitales en las empresas exportadoras de café de la ciudad de Cartago - Valle del Cauca. Lo anterior a consecuencia de que no se tiene mucha información al respecto de este tipo de empresas, especialmente lo concerniente a los activos digitales, entendidos estos como esos recursos que se crean, almacenan y se distribuyen en formato digital y que contienen información sensible para las empresas, siendo pertinente cuidar estos ataques o delitos cibernéticos.

2.1 PREGUNTA DE INVESTIGACIÓN

Se presentan las siguientes preguntas de investigación:

¿Cómo se encuentran establecidos los procesos de ciberseguridad de activos digitales en empresas exportadoras de café en el municipio de Cartago - Valle del Cauca?

En lo vinculado a la sistematización de la pregunta problematizadora, se presentan las siguientes preguntas:

¿Cuál es el marco normativo y legal de la de la ciberseguridad de activos digitales en empresas del sector de la exportación de café?

¿Cómo están caracterizados los procesos de ciberseguridad de activos digitales realizados en este tipo de empresas?

¿Cuáles serían las recomendaciones para el fortalecimiento de los procesos de ciberseguridad en empresas exportadoras de café?

3.JUSTIFICACIÓN

En el municipio de Cartago existe una gran cantidad de empresas dedicadas a la exportación de café, teniendo en cuenta el minucioso manejo de datos digitales que utilizan para realizar sus actividades, es necesario que lleven a cabo procesos de ciberseguridad de los conocidos, tales como activos digitales, concepto que comprende toda la información relacionada a clientes, cuentas, contactos, contrataciones, entre otros aspectos.

Debido a la poca información que se obtuvo en la revisión de la literatura relacionada al tema, es pertinente averiguar de qué manera este tipo de empresas llevan a cabo los procesos vinculados a la ciberseguridad de los activos digitales, lo anterior bajo el marco de la Gestión del Riesgo.

Partiendo de lo anterior, se hace necesario determinar el marco normativo y legal de la ciberseguridad de activos digitales en empresas de este sector económico, lo anterior partiendo de un análisis documental sobre este aspecto. En segundo lugar, es importante caracterizar los procesos de ciberseguridad de los activos digitales en estas empresas, por medio de la realización de una entrevista semiestructurada dirigida a los encargados de la gestión de riesgo de estas empresas. Por último, teniendo como base los resultados arrojados por la caracterización, se presentan las recomendaciones para el fortalecimiento de los procesos de ciberseguridad para las exportadoras de café, y así promover aspectos relacionados a la Gestión del Riesgo, y la ciberseguridad empresarial.

4.OBJETIVOS

4.1 OBJETIVO GENERAL

Describir cómo se encuentran establecidos los procesos de ciberseguridad de activos digitales en empresas exportadoras de café en el municipio de Cartago.

4.2 OBJETIVOS ESPECÍFICOS

. Determinar el marco normativo y legal de la ciberseguridad de activos digitales en empresas del sector de la exportación de café en el municipio de Cartago.

. Caracterizar los procesos de ciberseguridad de activos digitales en este tipo de empresas.

. Presentar recomendaciones partiendo de los datos obtenidos para los procesos de ciberseguridad en las empresas objeto de estudio.

5.MARCO TEÓRICO

5.1 CIBERSEGURIDAD

En la actualidad, la ciberseguridad se constituye de un elemento importante para la protección de la información y de las infraestructuras tecnológicas de la información. A medida que la tecnología evoluciona, de igual manera también lo hacen las amenazas y los riesgos que se derivan del ciberespacio, situación que afecta a las personas, las organizaciones y los gobiernos. La emergente dependencia e interconexión hacia los sistemas digitales hace que el establecimiento de la ciberseguridad se convierta en una herramienta obligatoria para los usuarios de estas tecnologías, especialmente para las empresas.

Por ende, y de acuerdo con Caamaño y Gil (2020), los avances presentados por las Tecnologías de la Información y las Comunicaciones (TIC), han generado impactos positivos en la esfera mundial, específicamente en el campo de los negocios; al igual que en el progreso de las comunidades en los distintos contextos, también conllevan situaciones o aspectos no tan positivos, como lo son las amenazas de ciberataques, que en muchos casos se orientan a la obtención de beneficios económicos, políticos o particulares.

En Colombia, y desde la óptica de Cano (2022), la ciberseguridad en el país ha dejado de ser un tema futurista para convertirse en una oportunidad de aterrizar los desafíos y las realidades que emergen desde este tema. Por lo anterior, es necesario que la nación realice los ajustes necesarios para dar frente a las transformaciones digitales que se están gestando y así afrontar a los adversarios digitales que deseen sacar provecho a las vulnerabilidades presentadas en el mundo virtual colombiano.

Tomando como base lo expuesto por IBM (2023), la ciberseguridad engloba a cualquier tecnología, acción o práctica que se pone en uso para la prevención de los distintos ciberataques y la mitigación de sus impactos. Esta presenta como objetivo la protección de aspectos como los sistemas, las aplicaciones, los dispositivos de orden informático, los datos de carácter confidencial, los activos financieros y digitales de personas y empresas u organizaciones contra condiciones como los virus informáticos, los ataques provenientes de ransomware de alta tecnología, entre otros. Por el lado de Zendesk (2024), como ciberseguridad se entiende a ese conjunto de tecnologías y de prácticas que se diseñan para la protección de los sistemas y de los registros contra las amenazas de origen cibernético que se podrían presentar. El objetivo de esta es la preservación de aspectos como la integridad, la confidencialidad y la disponibilidad de la información digital. Desde lo planteado por Saavedra (2023), la ciberseguridad es el

conglomerado de procesos y de prácticas bajo un marco tecnológico que se enfoca en la protección de componentes del mundo digital y virtual, para minimizar los daños que los ciberataques puedan generar.

Prosiguiendo con Zendesk (2024), entre las características de este concepto se puede ubicar a la integridad, confidencialidad, disponibilidad de los datos; al igual que la respuesta oportuna ante los peligros y los riesgos que se presenten hacia estos. Al hablar de ciberseguridad, se desglosan conceptos que sirven para el entendimiento del mismo término. El primer concepto es el de Ciberdelincuente, tomando como referencia lo planteado por Incibe (2020), este hace referencia a esa persona que se dedica a realizar actividades de naturaleza delictiva, ya sea contra personas o sistemas informáticos, con el objetivo de generar daños económicos, personales o reputacionales por medio de prácticas como el robo, la filtración de información, averías de software o hardware, extorsión, entre otras acciones. Estas actividades, en su mayoría, se encuentran orientadas al alcance de fines económicos.

Prosiguiendo con lo planteado por Incibe (2020), el concepto de ciberataque se relaciona con el intento realizado por un ciberdelincuente de acceder a un sistema informático, sin permiso ni autorización, haciendo uso de distintas metodologías para realizar actividades con intenciones dañinas, como lo son el robo de la información, la extorsión o llanamente daños al sistema.

Desde la perspectiva de Aguilar (2021), la ciberseguridad es de vital importancia en el mundo actual, especialmente para el funcionamiento adecuado de las empresas, organizaciones y entidades, al igual que en la cotidianidad de las personas. Por ende, esta es importante debido a que protege los datos personales, previene los ataques cibernéticos, asegura la continuidad de los negocios, promueve los cumplimientos legales y normativos, fortalece la confianza en los consumidores o los clientes, protege la reputación empresarial u organizacional, fomenta la preparación ante emergencias, minimiza los impactos económicos que los ciberataques puedan generar. En otras palabras, la ciberseguridad es fundamental para la protección integral de la información de naturaleza digital.

La ciberseguridad presenta unos conceptos claves que son planteados por la CIA. Tomando como referente a Fortinet (2024), se expone la “Triada de la CID”, que comprende los principios de confidencialidad, integridad y disponibilidad. Este es un modelo del cual se basan los distintos sistemas de seguridad. A continuación, se explican estos principios:

. Confidencialidad: Comprende los esfuerzos provenientes de una organización y que se orientan a la garantía de privacidad que deben tener los datos. Para alcanzar esta condición, es fundamental controlar el acceso a la información con el fin de evitar el intercambio ilegal de datos, ya sea este accidental o incidental, y así, poder

asegurar la integridad de la información. Uno de los pilares al momento de mantener la confidencialidad es verificar que aquellas personas que no cuentan con la autorización pertinente, no tengan acceso a los activos importantes de las empresas.

. Integridad: Hace referencia a verificar si los datos son confiables y que estos se encuentren libres de alteraciones. Esta condición se sostiene solo si los datos tienen características como autenticidad, precisión y confianza.

. Disponibilidad: A pesar de que los datos presenten confidencialidad e integridad, en ocasiones estos pueden ser considerados inútiles, al menos que tengan disponibilidad para esas personas en la organización y a los clientes a los cuales se les presta el servicio. En otras palabras, los sistemas, las redes y las aplicaciones deben de funcionar al momento en que se necesiten.

Los tipos de ciberseguridad también son comprendidos como los dominios relacionados a estos procesos, y se encuentran en las infraestructuras de la tecnología de la información. Parafraseando a IBM (2023), los tipos de ciberseguridad más comunes, son los siguientes:

. La seguridad de infraestructura crítica: Esta se encarga de la protección de aspectos como los sistemas informáticos, el conjunto de redes, los datos y los activos digitales de los que depende la seguridad nacional, económica y pública de una determinada sociedad. Como ejemplo de lo anterior, se encuentra lo desarrollado en Estados Unidos por el Instituto Nacional de Estándares y Tecnología, la Agencia de Seguridad de Infraestructura y Ciberseguridad y la CIA.

. La seguridad de red: Esta se orienta a evitar los accesos no autorizados a las redes, al tiempo que detecta y contiene los ciberataques y las violaciones de seguridad en estas mismas. A su vez, también ayuda a garantizar que el personal autorizado posea acceso pertinente y seguro a los recursos de la red que demanden.

. La seguridad de punto final: Los conocidos como *endpoints,* que comprenden los servidores, los ordenadores de escritorio y portátiles, los dispositivos móviles, son las principales entradas de los ciberataques. Por ende, la seguridad en los endpoints es la protección para estos dispositivos y los usuarios contra los ciberataques, como también es la protección contra aquellos que hacen uso de los endpoints para perpetuar ciberataques.

. La seguridad de aplicaciones: Estas protegen a las aplicaciones que son ejecutadas en las mismas, al igual que en las nubes, para evitar accesos no autorizados y el uso indebido de los datos y las aplicaciones vinculadas. De igual forma, se encarga de la prevención de las debilidades en los diseños de las

aplicaciones que son utilizadas por los hackers, cuyo fin es realizar las infiltraciones en la red.

. La seguridad en la nube: Esta se encarga de la protección de los servicios y activos que se encuentran en la nube de una empresa, estos pueden ser las aplicaciones, los datos, el almacenamiento, las herramientas encargadas de desarrollo, los servidores de naturaleza virtual, y la infraestructura disponible en la nube. A grandes rasgos, este tipo de seguridad funciona bajo el modelo de la responsabilidad compartida, se caracteriza por la protección de los servicios que presta, al igual que de la infraestructura que se usa para el servicio. Por lo anterior, es el cliente el único responsable de la protección de los activos digitales que almacena.

. La seguridad de la información: Comprende la protección del total de toda la información de naturaleza importante que se puede encontrar en una organización, estos podrían ser los archivos y datos digitales, documentación física, hasta las expresiones de origen humano contra los accesos ilegales, la circulación, el uso no autorizado. La protección de los activos digitales es uno de los subconjuntos de la seguridad de la información y de las medidas de infosec vinculadas a los procesos de ciberseguridad.

. La seguridad móvil: Esta es un conjunto de disciplinas y tecnologías para los conocidos, como dispositivos móviles y teléfonos inteligentes, por lo cual incluye la gestión de las aplicaciones para móviles, al igual que la gestión de movilidad empresarial. Desde hace poco tiempo para acá, este tipo de seguridad se encuentra vinculada a los endpoints.

Partiendo de lo presentado por IBM (2023), las amenazas más comunes a la ciberseguridad son las siguientes:

. Malware: Esta es la abreviatura que se utiliza para describir al software malicioso, y comprende un código de software o un programa de origen informático que fue diseñado de forma malintencionada para ocasionar un daño a un sistema informático y a los usuarios de estos. En la actualidad, una gran cantidad de ciberataques comprende un malware.

. Ransomware: Este hace referencia a un prototipo de malware que se encarga de encriptar los datos, como también el dispositivo de una víctima, amenazando con mantenerlos de forma encriptada, al menos que la víctima pague una extorsión al encargado del ataque.

. Phishing: Estos se constituyen de un conjunto de ataques por medio de los correos electrónicos, de voz o de texto, que se encargan de engañar a los usuarios para que los descarguen y así, adquirir un malware, que se caracteriza por ser mensajes fraudulentos y en su mayoría, solicitan a los usuarios el restablecimiento de las

contraseñas o los datos de la tarjeta de crédito. Este tipo de estafas es una de las más sofisticadas del mundo de la ciberdelincuencia.

. Las amenazas internas: Estas presentan su origen en usuarios con autorización, los contratistas, o socios comerciales que, de alguna manera u otra, realizan el uso indebido de su acceso legal o aquellas cuentas que han sido secuestradas por los ciberdelincuentes. Estas son de difícil detección a consecuencia de que presentan las evidencias de actividad autorizadas, haciéndose indetectables para las herramientas encargadas de identificar las distintas amenazas.

. Ataques de denegación de servicio distribuido (DDoS): Estos ataques se caracterizan por realizar intentos de bloqueo a un servidor, a un sitio web, o a una red por medio de la sobrecarga de tráfico, que normalmente se realiza desde una botnet, que se encarga de realizar los secuestros por medio de los malware.

Para IBM (2023), las siguientes son las prácticas más pertinentes al establecer una adecuada ciberseguridad para las personas o las empresas. Por ende, estas se constituyen de:

. La formación de concienciación sobre seguridad: Es ideal que en las empresas se realicen capacitaciones vinculadas al tema de ciberseguridad, en aras de promover el entendimiento de las acciones percibidas como inofensivas. Estas acciones pueden comprender el simple uso de la contraseña o el uso inadecuado de la información que se encuentra en las redes sociales, que aumentan la posibilidad de que se realicen ciberataques. Este tipo de capacitaciones abarcan la conciencia sobre la importancia de la seguridad, de la mano con las políticas de la seguridad podrían promover en los empleados una toma de conciencia sobre el uso de los datos de origen empresarial y personal confidenciales. De igual manera, estas actividades podrían ayudar a la identificación de ciberataques y sus características más notorias.

La gestión de identidad y acceso: Esta es la encargada de la definición de los roles, como también de los privilegios a los accesos para los usuarios, en conjunto con las condiciones con las cuales se bridan o se niegan estos privilegios. Entre estas tecnologías se puede encontrar a la autenticación de los multifactores, que exigen las credenciales, un nombre de un usuario, y una contraseña. En algunos casos se exige más de una credencial.

La gestión de la superficie de ataque: Este comprende el análisis minucioso o el monitoreo continuo del conjunto de las vulnerabilidades de la ciberseguridad, al igual que de los posibles vectores de ataque de los cuales se comprende la superficie de ataque de una empresa. Una de las ventajas de esta metodología es que se realiza desde la óptica de un hacker, en vez de la perspectiva de la víctima,

permitiendo la evaluación de los riesgos desde las oportunidades que emergen de un atacante malicioso.

La Detección, prevención y respuesta a amenazas: En la actualidad, la Inteligencia Artificial ha sido un aporte fundamental para la identificación y afrontamiento de los ataques proyectados, en curso o reales, cabe anotar que es humanamente imposible contener todos los ciberataques. Entre las tecnologías utilizadas se puede encontrar a la SIEM, la SOAR y la EDR, siendo estas utilizadas como un segmento del plan formal de respuesta a los incidentes.

La recuperación ante desastres: Esta comprende la capacidad que presenta la empresa o la personas de recuperarse ante la catástrofe generada por los ciberataques. Lo anterior podría comprender las conmutaciones por error direccionadas a las reanudaciones de las operaciones, posterior a un ataque ransomware.

En los procesos de ciberseguridad se puede encontrar una gran cantidad de herramientas que se usan para la protección de los datos o los también conocidos como los activos digitales. Para Teijeiro (2023), algunas de las de mayor uso, son:

. Los firewalls: Estas se constituyen como las primeras líneas de defensa de los procesos relacionados a la ciberseguridad. Realizan funciones de barrera entre las redes privadas y los tráficos no autorizados provenientes de fuentes externas, como lo es el caso del Internet. La función principal es la protección de las redes contra los intentos de acceso sin autorización, las intrusiones y los ataques.

. Las herramientas de ciberseguridad: antivirus: Los antivirus son una gran ayuda al momento de la detección y la eliminación de los malwares, entre los que se pueden encontrar los spyware, los virus, entre otros, que se encargan de la infección de los sistemas y el hurto de la información de naturaleza sensible. Estos antivirus hacen uso de algoritmos y firmas para eliminar las amenazas antes de que hagan daño, algunos de estos, realizan análisis heurísticos de orden avanzado.

. Los Sistemas de Detección de Intrusiones (IDS): Estas se encargan de realizar el monitoreo continuo de las redes, con el fin de identificar actividades o acciones sospechosas. Al momento en el que se identifican actividades consideradas como sospechosas, se generan alertas para que los encargados de la ciberseguridad, lleven a cabo acciones.

. Los Sistemas de Prevención de Intrusiones (IPS): Estas son extensiones de los Sistemas de Detección de Intrusiones, y se ubican mucho más allá, llegando no solo a la detección de las intrusiones, también tomando medidas para el bloqueo de estas intrusiones. Son fundamentales para detener los ataques en tiempo real, al tiempo que protege la red con todo tipo de amenazas.

Las herramientas de ciberseguridad como los escáneres de vulnerabilidades, son las encargadas de la identificación de las dificultades en la seguridad de los sistemas y aplicaciones. Una de las características es que evalúan de manera pertinente las infraestructuras en aras de encontrar vulnerabilidades y proporcionar las recomendaciones para su debida corrección.

Las herramientas de gestión de identidad y de acceso (IAM), que son fundamentales para la garantía correspondiente a que solo las personas con autorización presenten el acceso a los sistemas, como también a los datos sensibles. Este tipo de herramientas promueven la adecuada administración de los usuarios, como también de sus derechos de acceso, esto permite la gestión de las contraseñas, los dos factores autenticados, y, por último, la puesta en marcha de las políticas de acceso.

Los análisis de tráfico de red, orientados a la supervisión y análisis del tráfico presente en una red, para así, poder identificar los comportamientos sospechosos. Esto es de vital importancia para la optimización de las redes.

Las herramientas de análisis de malware se enfocan en desarrollar análisis minucioso de los archivos y del software, con el fin de encontrar malware. Por lo anterior, se presentan técnicas como la emulación y el análisis del comportamiento para establecer malwares que podrían pasar por los antivirus tradicionales.

Por último, las Herramientas de Autenticación Multifactor (MFA), se orienta a añadir capas adicionales de seguridad, a través de la solicitud de distintas maneras de autenticación, antes de dar permiso para el acceso a los distintos sistemas y aplicaciones. Lo anterior puede hacer referencia a la solicitud de una contraseña, de una tarjeta, o de una huella digital o un reconocimiento facial. Esta herramienta es de gran efectividad al momento de la prevención de accesos no autorizados.

5.2 ACTIVOS DIGITALES

Actualmente, los activos digitales se constituyen de un aspecto fundamental para el éxito y la competitividad de las distintas organizaciones. Tomando como referente a ISDI Digitalent Group (2023), este tipo de activos comprenden aquellos elementos de gran valor que se presentan en formato digital. Por lo anterior, puede incluir documentos con distinta información, imágenes, datos, aplicaciones, videos, entre otros aspectos. Son de gran importancia en esta era tecnológica y digital, siendo utilizados en diferentes contextos desde el sector empresarial, hasta las personas naturales. Estos abarcan diferentes formas, desde los tangibles hasta los intangibles. La importancia de estos descansa en la capacidad que presentan para su almacenamiento, los métodos de compartir, su flexibilidad para ser modificados y distribuidos por medio de las diferentes plataformas o herramientas digitales.

Por el lado de Docusing (2021), a estos se les conoce como esos archivos que son sustitutos del papel, y que se caracterizan por el almacenamiento de los

documentos que han sido elaborados de manera digital. Al mismo tiempo, y desde la óptica de los archivos digitales, son entendidos como los ficheros de naturaleza electrónica que se destacan por presentar datos, imágenes, videos u otros tipos de consolidación de información. A diferencia de los archivos de índole físico, estos solo se presentan en formato electrónico, almacenándose en dispositivos como los discos duros, nubes, entre otros. Estos presentan como ventajas que permiten su fácil y rápido acceso por medio de las bibliotecas digitales, al igual que su capacidad de ser compartido de manera adecuada. Presentando lo expuesto por Inprovider (2024), los archivos digitales se constituyen de esas representaciones electrónicas de las informaciones que se encuentran almacenadas en un medio digital. Por ende, estos no ocupan un espacio físico, encontrándose en los dispositivos de almacenamiento como lo son los computadores, los servidores en la nube, entre otros. Estos pueden guardar información fundamental para una empresa, organización o persona natural, ofreciendo una flexibilidad nunca antes vista en lo relacionado a la gestión de la información legal.

La gestión adecuada de estos activos, optimiza los procesos de productividad, y la sinergia entre los distintos equipos, esto como consecuencia de que ayuda al acceso rápido, pertinente y estructurado de la información. A su vez, estos pueden generar valor estratégico y económico por medio de su utilización en diferentes procesos de la empresa, como lo son las tomas de decisiones, planeación estratégica, estrategias de innovación, entre otros.

Prosiguiendo con ISDI Digitalent Group (2023), entre las características de los activos digitales, se ubican las siguientes: el formato digital, la capacidad de almacenamiento y de acceso en línea, su capacidad de escalabilidad, lo que permite ser de fácil distribución. Estos van acompañados de metadatos que permiten tener conocimiento de aspectos como las fechas de creación y algunas descripciones, también pueden ser editados y modificados y de fácil distribución. En lo correspondiente a su clasificación, ISDI Digitalent Group (2023), expone la siguiente:

. Datos de usuario: Referente a la información personal del usuario.

. Datos organizacionales: Comprende la información de orden empresarial vinculada a los procesos de ventas, las operaciones, talento humano, las finanzas, entre otros.

. Datos de investigación: Concerniente a los datos provenientes de investigaciones o de procesos experimentales.

. Derechos de autor: Relacionados a la protección de obras de naturaleza creativa como las provenientes de las artes.

. Marcas registradas: Las patentes de productos, marcas y servicios y que engloban los símbolos, logotipos o nombres que los identifica.

Entre otros activos digitales se encuentran las criptomonedas, los tokens, los archivos multimedia, las cuentas de redes sociales, los dominios web, los archivos multimedia, los softwares empresariales, los certificados digitales, las claves criptográficas, entre otros.

Retomando a Inprovider (2024), se expone que, al momento de establecer aspectos como la calidad y la integridad de estos archivos, se hace necesario el desarrollo de los siguientes componentes:

. La legibilidad: Estos deben caracterizarse por la legibilidad, fundamentados en un software estándar, y así no depender del uso de aplicaciones concretas para realizar el acceso a la información que estas presentan.

. La integridad: Los contenidos de este tipo de archivos, no deben ser cambiados sin la correspondiente autorización, lo anterior en aras de garantizar la fiabilidad que debe de tener la información, la pertinencia de esta, y así, prever el adecuado uso de la misma.

. Los metadatos: Estos deben de caracterizarse por la inclusión de enlaces que permitan identificar aspectos vinculados a la creación, a la modificación y a la autoría de los documentos, y de los archivos digitales, en aras de facilitar el acceso a la información proveniente del archivo digital, y así realizar el rastreo del historial.

. Los formatos estándar: Se debe hacer uso de formatos comunes y abiertos para evitar la obsolescencia tecnológica y facilitar el acceso a la información que comprende el archivo.

La importancia de estos activos radica en que son una fuente valiosa de información para el entendimiento de los distintos segmentos de mercado, promueve los procesos de colaboración interna en las empresas en aras del mejoramiento de la productividad, y finalmente, optimiza los recursos organizacionales.

Partiendo de lo expuesto por Vida Fernández (2022), la gobernanza del riesgo digital se encuentra conformada por ese conjunto de procesos, de estructuras y de políticas de índole organizativo que una empresa, organización o entidad debe determinar para la gestión y la mitigación de los riesgos vinculados a las tecnologías y las transformaciones digitales. Por lo anterior, esto hace referencia a procesos como la protección de la información, la privacidad de los datos, y la ciberseguridad, todo bajo el marco regulatorio adecuado.

Los componentes esenciales de la gobernanza comprenden:

. La identificación de riesgos: Sugiere la evaluación y la clasificación de los riesgos digitales que afectan a la empresa, entidad u organización, estos pueden ser dificultades en los sistemas, no acatamiento de las normas, o ser víctimas de ciberataques.

. La evaluación de los riesgos: Comprende el análisis de la probabilidad, al igual que del impacto de los riesgos que se identifiquen para su posterior priorización.

. El desarrollo de políticas: El establecimiento de las políticas y las directrices concretas que indiquen la manera pertinente con la cual se le debe dar manejo a los riesgos de naturaleza digital, y las medidas que se deben poner en uso para su mitigación.

. La implementación de los controles: Se deben concretar los controles, al igual que las medidas vinculadas a la seguridad con miras a la protección de los archivos de orden digital para la minimización de los riesgos.

. El monitoreo y la revisión: Los procesos de supervisión continuos del entorno digital, al igual que la revisión de las políticas y de los procesos en aras de asegurar su efectividad ante las amenazas que se presenten.

. La cultura organizacional: Es fundamental promover la cultura de la concienciación sobre la seguridad digital en todo el talento humano de la organización, esto debido a que una gran cantidad de incidentes se encuentran vinculados con fallas humanas.

. El cumplimiento regulatorio: Son los procesos de monitoreo encaminados a que la organización o empresa realice el cumplimiento de toda la normatividad vinculada con la seguridad de naturaleza cibernética, al igual que la protección de los datos.

En conclusión, esta gobernanza es el eje para que las empresas y las organizaciones se protejan de todas las amenazas cibernéticas, y así, garantizar la sostenibilidad del negocio, y mantener la buena reputación de estas.

5.3 GESTION DE RIESGO

Para un mejor entendimiento de este concepto, es necesario presentar, en primer lugar, lo que es un riesgo. Según SafetyCulture (2024), como riesgo se entiende a esa posibilidad de que un evento ocurra y que incidan de manera negativa en el funcionamiento y objetivos de la organización, incluye la incertidumbre sobre las pérdidas que esto genere, al igual que las posibilidades de que se convierta en oportunidades en beneficio de la empresa. Prosiguiendo con SafetyCulture (2024), la gestión de riesgo se aborda como ese proceso mediante el cual se desarrollan acciones como la identificación, la evaluación y la minimización del impacto que los

riesgos puedan presentar. De otro modo, se entiende como los procesos por los cuales las organizaciones realizan la identificación de los peligros y las amenazas potenciales para la toma de medidas, en aras de la eliminación o la reducción de las posibilidades de que estos acontezcan.

Por lo anterior, todas las organizaciones, sean del tamaño que sean, deben desarrollar la gestión de riesgo. Esto como consecuencia de que, además de lo expuesto, también ayuda al establecimiento de las estrategias de orden preventivo y de contingencia adecuadas para la mitigación de los impactos. Entre los riesgos se pueden encontrar a los financieros, los de seguridad, reputación, entre otros, comprendido esto en una amplia gama. Al momento en que una empresa implementa una estrategia integral de la gestión del riesgo, esta se protege de los diferentes peligros. La preparación garantiza una respuesta adecuada ante cualquier situación amenazante y promueve la capacidad de resiliencia y de adaptación ante los desafíos proveniente del entorno empresarial en la actualidad.

Para Martin (2024), el objetivo de la gestión de riesgo hace referencia a la protección de una empresa y organización enfocada a las posibles amenazas y pérdidas que ponen a peligrar con su funcionamiento. Retomando a SafetyCulture (2024), en la gestión de riesgo se pueden encontrar pasos como:

. La identificación de los riesgos: Hace referencia al reconocimiento de los riesgos de mayor prevalencia que podrían afectar a una organización, ya sean estos los operativos, los legales, reputación, entre otros.

. La evaluación de los riesgos: Comprende los análisis de la probabilidad de que sucedan al igual que el impacto que generarían al momento de presentarse.

. El tratamiento de los riesgos: Se constituye del desarrollo y la implementación de planes, direccionados a la reducción, transferencia, aceptación o evitación de los riesgos, incluyendo al mismo tiempo el establecimiento de los controles o políticas concretas.

. El monitoreo y la revisión: Hace parte del establecimiento de un sistema continuo, para el monitoreo de los riesgos, al igual que de la eficacia de las estrategias que se han implementado, realizando adecuaciones a las acciones solo en los casos en que sea pertinente. Así, se establece que la gestión de riesgos es la base de la toma de decisiones de naturaleza informada, los procesos de planificación estratégica y de la sostenibilidad a un plazo largo en cualquier empresa u organización.

Retomando nuevamente a Martin (2024), entre las prácticas más comunes en los procesos de la gestión de riesgo, se puede encontrar a:

Los riesgos financieros que se vinculan con los procesos de pérdida del capital o de los ingresos de una empresa o persona, y que a su vez incluyen los riesgos de

mercado, los de crédito y los de liquidez. Los riesgos operativos que se encuentran relacionados a los fallos en los procesos de naturaleza interna, los sistemas o el talento humano en los eventos externos que inciden en la operatividad en una organización. Los riesgos estratégicos que se vinculan con las decisiones de alto orden que impactan de manera directa en la dirección o en el éxito a un plazo largo en las organizaciones.

De igual manera, también se encuentran los riesgos de cumplimiento que se desprenden de la necesidad de dar cumplimiento a cabalidad a las leyes, las regulaciones, y las políticas. Al mismo tiempo pueden generar sanciones a nivel legal o perdidas en la reputación de la persona o la empresa. En lo relacionado a los riesgos técnicos, se encuentran muy vinculados a las fallas en la tecnología, los sistemas de información y a las herramientas que la organización en su cotidianidad acostumbra a utilizar.

En concordancia con lo anterior, los riesgos reputacionales son esos que hacen referencia a las pérdidas de aspectos como la credibilidad y la confianza por parte de la clientela, los socios y/o el público. Por parte de los riesgos de mercado, estos representan a esos cambios en los entornos del mercado que podrían incidir en el valor de los activos, o en el rendimiento financiero. Los riesgos de proyecto se constituyen en los aspectos vinculados a la incertidumbre en proyectos concretos, que se traducen en incumplimientos, retrasos y sobrecostos en los objetivos. Por último, se ubican los riesgos de ciberseguridad, que comprenden las amenazas a la información, y a las infraestructuras tecnológicas, aquí se pueden encontrar los ataques cibernéticos, las violaciones de datos, entre otras situaciones.

De esto último, se desprende lo que se conoce como Gestión de Riesgo Digital, que para la IBM (2024) se consolida en los procesos que se encargan de la identificación, la priorización, la gestión y la supervisión de los riesgos provenientes de los sistemas de información. En la actualidad, las empresas utilizan lo que se conoce como la gestión de riesgos cibernéticos, que se encarga de la protección de los sistemas de información frente a los ataques u otro tipo de amenazas, ya sean estas físicas o digitales.

6. MARCO METODOLÓGICO

6.1 TIPO DE ESTUDIO

El presente proceso investigativo se basa en un tipo cualitativo. Según Hernández, Fernández y Baptista (2006), este tipo de investigación se enfoca en la comprensión de los significados subjetivos de los individuos en un contexto particular. Se caracteriza por no manejar datos numéricos por medio de estrategias como las observaciones, las entrevistas semiestructuradas y la revisión documental. Prosiguiendo con estos mismos autores, también es exploratoria - descriptiva, a consecuencia de que se aborda una problemática de la cual no se cuenta con mucha información y que se desea describir de una manera minuciosa. En este tipo de investigación se obtiene la información por medio de herramientas como las entrevistas semiestructuradas, la observación y la revisión documental.

6.2. SUJETOS Y/O MUESTRA

Para efectos de este proceso, se tienen en cuenta los encargados de la administración del riesgo de las empresas exportadoras de café del municipio de Cartago - Valle del Cauca. Por lo anterior, se cuenta con una cantidad de seis (6) empresas exportadoras como muestra para este proceso investigativo.

6.3. INSTRUMENTOS Y TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

Partiendo de lo expuesto con anterioridad, se presentan los siguientes instrumentos y técnicas de la recolección de la información:

. Entrevistas semiestructuradas: Es pertinente la realización de entrevistas semiestructuradas a los encargados de la administración de riesgo de las empresas objeto de estudio.

. Revisión documental: Revisar todos los documentos relacionados a la temática, ya sean estos las políticas, los procedimientos, los antecedentes, informes organizacionales de la ciberseguridad, entre otros.

La siguiente tabla presenta los instrumentos y las técnicas de recolección de la información. La entrevista semiestructurada se encuentra en el Anexo A.

Tabla 1. Instrumentos y técnicas de recolección de la información

Objetivo específico	**Variable**	**Instrumento**	**Tipo de variable**	**Escala de medición**
. Determinar el marco normativo y legal de la ciberseguridad de activos digitales en empresas del sector de la exportación de café en el municipio de Cartago.	Normatividad vinculada a la ciberseguridad de los activos digitales: Leyes, Decretos, Normas, Guías y Protocolos.	Revisión bibliográfica y documental.	Cualitativa	Nominal
Caracterizar los procesos de ciberseguridad de activos digitales en este tipo de empresas.	Activos digitales. Evaluación de Riesgos. Políticas y Protocolos de Ciberseguridad. Capacitación y Concientización. Herramientas y Tecnologías. Cumplimiento Normativo.	Entrevista semiestructura-da.	Cualitativa	Nominal
Presentar recomendaciones partiendo de los datos obtenidos para los procesos de ciberseguridad en las empresas objeto de estudio**.**	Recomendaciones para los procesos de ciberseguridad de los activos digitales.	Revisión bibliográfica y documental.	Cualitativa	Nominal

Fuente: Elaboración propia de los autores (2024).

7. RESULTADOS

7.1 DETERMINAR EL MARCO NORMATIVO Y LEGAL DE LA CIBERSEGURIDAD DE ACTIVOS DIGITALES EN EMPRESAS DEL SECTOR DE LA EXPORTACIÓN DE CAFÉ EN EL MUNICIPIO DE CARTAGO.

En lo concerniente al primer objetivo específico, se llevó a cabo una detallada revisión documental, con el fin de determinar el marco normativo y legal que se encuentra relacionado con la ciberseguridad de activos digitales en empresas del sector de la exportación de café en el municipio de Cartago, Valle del Cauca, Colombia. Por consiguiente, en la siguiente tabla se muestran los resultados del proceso de búsqueda.

Tabla 2. Marco normativo y legal de la ciberseguridad de activos digitales en Colombia

Aspecto normativo	Descripción
Ley 1266 de 2008 (Diciembre 31)	Del Congreso de la República**.** En esta ley se establecen las disposiciones generales sobre el manejo de la información financiera y crediticia, por lo anterior se incluyen los campos relacionados a la protección de los datos personales, que son fundamentales para la ciberseguridad, concretamente en el manejo de clientes y de los proveedores.
Ley 1341 de 2009 (Julio 30)	Del Congreso de Colombia. En esta ley, se hace promoción del acceso y del uso de las telecomunicaciones y de las tecnologías de la información, por lo cual se establece el marco para el desarrollo de la sociedad de la información y las comunicaciones. De igual manera, se establecen las normas para la ciberseguridad. Se crea la Agencia Nacional del Espectro.
Ley 1581 de 2012 (Octubre 17)	Del Congreso de Colombia. En esta ley se hace regulación de la protección de datos personales en el país. Por ende, las empresas que manejan este tipo de datos de los clientes, deben garantizar el cumplimiento de esta normatividad a través del establecimiento de medidas que garanticen la seguridad de esta

	información, al igual que el respeto por la privacidad de los usuarios.
Ley 1908 de 2018 (Julio 9)	Del Congreso de Colombia. En esta ley se presenta la tipificación de los delitos informáticos en Colombia, al tiempo que se busca el fortalecimiento de las medidas hacia el control cibernético, lo anterior para la protección de las empresas y de los usuarios en las distintas formas de ataques informáticos.
Política Nacional de Seguridad Digital (MinTIC)	En Colombia, esta política se encuentra a cargo del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y en la cual se establecen las directrices en aras de la protección de la información y de los sistemas críticos, incluidos los relacionados al sector agrícola y al de la exportación.
Decreto 1078 de 2015 (Mayo 26)	Del Presidente de la República de Colombia. Por el cual, se realiza la compilación de las normas del sector de las TIC, a la vez que establece las regulaciones para la protección de los datos, y las medidas de seguridad en el uso de las tecnologías.
Decreto 620 de 2020 (Mayo 02)	Del Presidente de la República. Por el cual se regulan aspectos relacionados con la seguridad digital y la protección de datos.
ISO/IEC 27001 (2022)	Esta es una norma emanada por la Organización Internacional de Normalización (ISO), y comprende aspectos como: La Gestión de la Seguridad de la Información, Evaluación de los Riesgos, Mejora Continua, Adecuación de las Necesidades Organizacionales, y la Certificación.
ISO/IEC 27002 (2022)	Es un estándar internacional que hace parte de la serie de ISO/IEC 27000 emanada por la Organización Internacional de Normalización (ISO), y se encarga de proporcionar directrices y

	buenas prácticas para la implementación de los controles de seguridad de la información en las organizaciones.

Fuente: Elaboración propia de los autores.

Lo presentado permite identificar, que por parte del gobierno nacional se han desarrollado acciones para la garantía de la ciberseguridad en el territorio colombiano. De igual manera, también se observan normas internacionales como la ISO, que son de gran importancia al momento de emitir certificaciones en estos aspectos relacionados a la ciberseguridad.

7.2 CARACTERIZAR LOS PROCESOS DE CIBERSEGURIDAD DE ACTIVOS DIGITALES EN ESTE TIPO DE EMPRESAS

En este capítulo, se exponen los resultados de la aplicación de la entrevista semiestructurada en aras de caracterizar los procesos de ciberseguridad de activos digitales en las empresas exportadoras de café. En aras de guardar la confidencialidad en los nombres de estas empresas, se les asignará el código E acompañado de un número para el desarrollo de los análisis cualitativos y sus interpretaciones. A continuación, se presentan las empresas con sus respectivos años de funcionamiento, y con su tipo.

Tabla 3. Datos de las empresas objeto de estudio

Código	Años de Funcionamiento	Tipo de empresa
E1	Más de 50 años	Privada
E2	Más de 5 años	Privada
E3	Más de 35 años	Privada
E4	Más de 35 años	Privada
E5	8 años aproximadamente	Privada
E6	34 años	Privada

Fuente: Elaboración propia de los autores.

Esta tabla, permite establecer que son seis (6) las empresas que forman parte de este estudio, todas de tipo privado y con un intervalo de funcionamiento de los 8 a los 50 años. Para mayor comprensión del lector, se anexará un glosario de aquellos términos que se encuentran en inglés, traducidos al castellano con su significado (Anexo B).

Tabla 4. Características de los procesos de ciberseguridad de los activos digitales en este tipo de empresas

Característica	Interpretación
Activos digitales	En la población indagada, se puede identificar que un poco más de la mitad de las empresas abordadas, sí presentan conocimientos sobre los activos digitales. En este orden de ideas, entre los activos digitales que se manejan en las empresas, se encuentra en la base de datos de clientes, proveedores y empleados, informaciones de contacto, correos electrónicos, WhatsApp, Tax id, direcciones de ubicación física, cuentas bancarias, portales contables, estudio de mercado exportados, dominio propio, página web, blog, programas contables, modelos operativos. Sobre los procesos de gestión y almacenamiento de los activos digitales, se presenta que, en la mayoría de los casos, no tienen ningún proceso definido, toda la información está almacenada en la nube de Microsoft y una muy pequeña en físico, no hay backup offline. En otros casos, toda la información es de responsabilidad del director general, y, por último, se presenta la codificación de la información para el fácil acceso de los perfiles de acceso en el Cloud y en el Drive, presentándose también toda la información en archivo físico.
Evaluación de Riesgos	Solo una pequeña parte de las empresas estudiadas, manifiestan realizar procesos de evaluación de riesgos, vinculados a la ciberseguridad. Al mismo tiempo, sobre la frecuencia de estas evaluaciones, las empresas exponen que se realizan periódicamente, tomando como base los procesos de SCS BASC (Business Alliance for Secure Commerce). Para finalizar, sobre los riesgos identificados

	en estas evaluaciones, se puede encontrar a posibles hackeos de cuentas de correo, tienen dominio propio, pero muchos procesos se realizan desde cuentas de Gmail y Hotmail, algunas cuentas utilizadas son de personas que ya no trabajan en la empresa, no cuentan con perfiles de usuario, y no hay manual de procesos definidos. De igual forma, se presentan el ransomware, secuestro de la información y por consiguiente, extorsión cibernética, violación de datos y el fishing ceo.
Políticas y Protocolos de Ciberseguridad	En lo vinculado a las políticas y los protocolos de ciberseguridad identificados, menos de la mitad de las empresas exponen contar con estos aspectos, los cuales abarcan campos tales como la cadena de suministro en el sector del Café, dando prioridad al cumplimiento de los requisitos legales, reglamentarios y normas aplicables, comprometidos con el mejoramiento continuo del SGCS BASC(Business Alliance for Secure Commerce),todo ello a través de la gestión del riesgo y promoción de la seguridad en el uso de tecnologías de la información. Por último, se ha planteado que estos están integrados con el programa SGCS Sistema de Gestión de Control y Seguridad. Por el lado de las empresas que aún no cuentan con estos aspectos, se plantea que están en proceso de establecer programas relacionados a la ciberseguridad.
Capacitación y Concientización	En menos de la mitad de las empresas intervenidas, se realizan capacitaciones sobre los temas de ciberseguridad. De igual manera, se plantea que la frecuencia es permanente y se realiza bajo el marco de la gobernanza y la cultura corporativa, promocionándose

	por medio de los canales virtuales como blog de acceso público. Sobre las acciones para fomentar la cultura de la ciberseguridad dentro de las empresas, se expone que se promueve la integración de todos los procesos vinculados al SGCS (Business Alliance for Secure Commerce), el control de riesgo, la seguridad física, la seguridad cibernética y la gestión de datos.
Herramientas y Tecnologías	En lo pertinente a las herramientas y la tecnología utilizadas para la ciberseguridad en estas empresas**,** se puede encontrar a los dominios propios, el antivirus actualizado, el Office licenciado, para los procesos de pago se hace uso de los Tokens, los cuales descansan en poder de una sola persona, los cifrados de información, y el corta fuego. Durante el proceso de exportación, solo una empresa manifestó que cuentan con una persona responsable del proceso, la cual solicitó a la aseguradora que sugiriera medidas de protección para su posterior proceso de implementación.
Cumplimiento normativo	Solo una de las empresas indagadas, expone que dentro del programa de SGCS (Business Alliance for Secure Commerce), se asegura el cumplimiento de las regulaciones de seguridad aplicables al gremio. Esta misma empresa expone que el cumplimiento de estas regulaciones, se verifica por medio del mismo SGCS BASC(Business Alliance for Secure Commerce).

Fuente: Elaboración propia de las autoras.

Sobre los activos digitales en este tipo de empresas, la anterior tabla permite evidenciar que un poco más de la mitad de la población indagada, sí presenta conocimientos sobre estos aspectos. Entre los activos digitales de mayor manejo en este sector, se pueden encontrar en lo expuesto por: E1*: "Base de datos de*

clientes, proveedores y empleados, informaciones de contacto correos electrónicos, WhatsApp, Tax id, direcciones de ubicación física, cuentas bancarias, portales contables", y los expuestos por E3: "*Bases de datos de clientes, proveedores y empleados, estudio de mercado exportador, correos electrónicos, dominio propio, página web, blog, programa contable, modelo operativo"*. Lo anterior permite evidenciar que, en este sector empresarial, se presenta una tendencia a utilizar los mismos activos digitales, todos estos direccionados a contener información de gran importancia para los procesos de la empresa, coincidiendo plenamente con lo presentado por Docusing (2021).

En lo relacionado a los procesos de gestión y de almacenamiento de estos activos digitales, se expone lo manifestado por E1: *"No tienen ningún proceso definido, toda la información está almacenada en la nube de Microsoft y una muy pequeña en físico. No hay backup offline*", al igual que lo planteado por E2: *"Todo tiene backup en el cloud y también físico como archivo. La información está en responsabilidad del director general del proceso de exportaciones".* En este orden de ideas, una nube en el mundo digital hace referencia a ese modelo que permite el acceso a varios recursos informáticos por medio de internet, no cuenta con servidores físicos, razón por la cual, los datos se almacenan en servidores o espacios remotos (nubes), que pueden ser accedidos en línea. Lo anterior converge con lo presentado por IBM (2023), sobre los distintos tipos de ciberseguridad, en especial, la seguridad en la nube que se encarga de la protección de los datos que se encuentran alojados en la nube.

En lo correspondiente al "backup", este debe entenderse como esas copias de seguridad que se realizan en el mundo virtual o digital, concretamente hace referencia al proceso de duplicar los datos, de la manera en que la información pueda ser recuperada en caso de un daño, robo o fallo en el sistema.

En lo concerniente a la evaluación de riesgos, se presenta que solo una pequeña parte de la población estudiada, lleva a cabo estos procesos. Por lo anterior, estos se desarrollan tomando como referente los procesos de SCS BASC. El SCS BASC (Business Alliance for Secure Commerce), es una apuesta de naturaleza internacional que tiene como objetivo, el fomento de la seguridad en las cadenas de suministros y en el comercio internacional, encontrándose esto justificado en lo manifestado por E4: *"Como miembro de la cadena de suministro en el sector del café, se da prioridad al cumplimiento de los requisitos legales reglamentarios y normas aplicables, comprometidos con el mejoramiento continuo del SGCS BASC, a través de la gestión del riesgo y promoción de la seguridad en el uso de tecnologías de la información".* En la evaluación de riesgos, este hace referencia a un conjunto de pasos que ayudan a la identificación, el análisis y la gestión de los riesgos, vinculados a los procesos de seguridad en campos, como la logística y el comercio. La importancia de realizar los procesos de evaluación de riesgos coincide

con lo manifestado por SafetyCulture (2024), siendo este el eje principal de los procesos relacionados a la gestión de los riesgos. Lo anterior se evidencia en lo expuesto por E3: *"Periódicamente según proceso del SCS"*, y E4: "*Periódicamente según proceso del SCS BASC".*

Por último, sobre las amenazas identificadas se presentan los hackeos de las cuentas de correo, el ransonware y el secuestro de información con fines extorsivos. Lo anteriormente expuesto converge con lo expuesto por Policía Nacional de Colombia (2020), sobre el hackeo, el ransonware y el secuestro de información con fines de extorsión, como las amenazas más comunes a las que se deben de enfrentar las empresas en el país. Esto coincide con lo manifestado por E2: *"Posibles hackeos de cuentas de correo, ransomware, secuestro de la información y por consiguiente extorsión cibernética, violación de datos, fishing ceo"*

Sobre las políticas y los protocolos de ciberseguridad, se encuentra que estos se presentan parcialmente establecidos en solo algunas de las empresas analizadas, se caracterizan por abarcar campos vinculados a la cadena de suministro del gremio del café, y se realizan bajo el marco del SGCS BASC(Business Alliance for Secure Commerce), y el SGCS Sistema de Gestión de Control y Seguridad, según lo encontrado en E4: *"Como miembro de la cadena de suministro en el sector del café, se da prioridad al cumplimiento de los requisitos legales reglamentarios y normas aplicables, comprometidos con el mejoramiento continuo del SGCS BASC, a través de la gestión del riesgo y promoción de la seguridad en el uso de tecnologías de la información".*

El SCS BASC (Business Alliance for Secure Commerce), como se expuso con anterioridad, es una propuesta de índole internacional que se orienta en la promoción de la seguridad de las cadenas de suministro y del comercio internacional. Por el lado del SGCS, o Sistema de Gestión de Calidad de la Seguridad, se entiende como ese marco de gestión que muchas organizaciones lo utilizan para garantizar que los procesos vinculados con la seguridad y la calidad de los productos o de los servicios que se ofrecen, sean lo suficientemente eficaces, al tiempo que cumplan con determinados estándares.

En lo pertinente al campo de capacitación y concientización, se encuentran en pequeñas cantidades la realización de capacitaciones sobre los temas de ciberseguridad, bajo el marco de la gobernanza y la cultura corporativa. Esto se puede observar en lo manifestado por E3: *"Permanentemente como gobernanza y cultura corporativa, se promociona por canales virtuales como blog de acceso público".* En lo referente a las acciones vinculadas al fomento de la cultura de la ciberseguridad, esta se integra a todos los procesos del SGCS, según lo manifestado por E3: *"Promoviendo la integración de todos los procesos en el SGCS, control de riesgo, seguridad física seguridad cibernética, gestión de datos*".

Retomando que el SGCS presenta como objetivo principal, el mejoramiento continuo de aspectos como la calidad y la seguridad, en aras de minimizar los riesgos y garantizar la satisfacción de los clientes. Estos sistemas pueden presentar procesos como la identificación de los riesgos, la planificación de las acciones de orden preventivo y correctivo, la capacitación del talento humano, y por último, el cumplimiento de las normatividades y las regulaciones adecuadas. Según Vida Fernández (2022), la gobernanza debe presentar aspectos como la identificación de los riesgos, la cultura organizacional, y el cumplimiento regulatorio.

Sobre las herramientas y tecnologías utilizadas para los procesos de ciberseguridad, se presenta a los dominios propios, antivirus, el office licenciado, el corta fuego, los cifrados, entre otros. Lo anterior, según lo manifestado por E2: *"Software licenciado, Antivirus actualizado, Cifrado de información",* y E3: *"Antivirus actualizado, Cortafuego, Software licenciado".* Lo expuesto con anterioridad converge con lo manifestado por Teijeiro (2023), sobre la utilización de antivirus y software como herramientas de ciberseguridad.

Por último, sobre el cumplimiento normativo, se presenta que solo una de las empresas analizadas utiliza el SGCS BASC como herramienta para el cumplimiento de las regulaciones. Lo anterior se puede evidenciar en E3: *"Dentro del programa SGCS, asegura el cumplimiento de las regulaciones de seguridad aplicables al gremio los procesos*". Lo anterior hace referencia a las normas ISO, vinculadas en este caso a la ciberseguridad.

7.3 Presentar recomendaciones partiendo de los datos obtenidos para los procesos de ciberseguridad en las empresas objeto de estudio

En lo concerniente a la protección de los activos digitales en empresas exportadoras de café en Colombia, se presentan las siguientes recomendaciones:

. La evaluación de riesgos: Desarrollar análisis minucioso de los riesgos para poder establecer las vulnerabilidades en los procesos y sistemas digitales.

. Realizar la clasificación de los activos digitales de mayor importancia, y realizar la priorización de la protección de aquellos activos digitales que son la base de la operación de la empresa.

. La capacitación del personal: Realizar capacitaciones de manera regular al talento humano, sobre temas relacionados a la ciberseguridad, reconocimiento de amenazas, y el fomento de las buenas prácticas.

. Promover la cultura de ciberseguridad en el interior de la empresa, enfatizando en la importancia en la seguridad de la información.

. La seguridad de la red: Desarrollar la implementación de herramientas como los firewalls, al igual que de sistemas de detección de las intrusiones para la protección de la red de las empresas.

. Realizar monitoreo sobre la seguridad de las redes WI-FI, para verificar que estas verdaderamente sean seguras. Por lo anterior, se pueden utilizar contraseñas complejas o las medidas de cifrado.

. El control de acceso: Realizar el establecimiento de las políticas de control de los accesos que limiten el acceso a la información de naturaleza sensible, solo para los empleados que realmente la necesiten.

. Utilizar métodos de autenticación de multifactorial para el incremento de la seguridad en el acceso a los sistemas considerados como críticos.

. La actualización de software y sistemas: Actualizar constantemente los sistemas informáticos y los softwares con los últimos programas de seguridad.

. Realizar la implementación de un programa de gestión de las vulnerabilidades con el objetivo de identificar y corregir supuestas brechas que se presenten.

. Respaldos de Información: Hacer copias de seguridad de manera periódica de esa información que se considere como crítica, y verificar que estas copias sean guardadas de forma adecuada.

. Verificar de manera periódica los procesos de restauración de los respaldos.

. Plan de respuesta a incidentes: Realizar un plan de respuestas a incidentes que manifieste la manera en que la empresa afronta una violación en su seguridad.

. La realización de simulacros y de ensayos con el fin de verificar si el personal se encuentra debidamente preparado ante un incidente real.

. Cumplimiento Normativo: Verificar que la empresa dé cumplimiento a las normativas, y a las regulaciones nacionales e internacionales con la ciberseguridad, y la protección de los datos.

. Realizar monitoreos enfocados a establecer si la empresa podría adaptar las mejores prácticas en la industria, como también las políticas de seguridad vinculadas a las mismas.

. El monitoreo y la auditoria: Realizar la implementación de las herramientas de monitoreo adecuadas para la supervisión de la actividad en la red, y así identificar comportamientos o movimientos sospechosos.

. Realizar auditorías de manera regular para la evaluación de la efectividad de las acciones relacionadas a la ciberseguridad, y desarrollar los ajustes que sean pertinentes.

. La colaboración con expertos: Se hace pertinente contemplar la contratación de personal experto en temas de ciberseguridad, o desarrollar alianzas estratégicas con empresas especialistas en dichos temas, para el mejoramiento de las estrategias de seguridad.

. Permanecer al tanto de las tendencias y de las amenazas emergentes en el tema de ciberseguridad, por medio de foros, o de asociaciones pertinentes del sector.

La implementación de las anteriores recomendaciones permitirá que las empresas exportadoras del Café puedan proteger sus activos digitales, y así puedan alcanzar la reducción de esta clase de ataques.

CONCLUSIONES

Esta investigación permite concluir que lo concerniente al aspecto normativo de la ciberseguridad de activos digitales en Colombia, se encuentra constituido por leyes tales como la 1266 de 2008, relacionada al manejo de la información crediticia y financiera; la 1341 de 2009, vinculada a la promoción del acceso a las tecnologías de la información y las telecomunicaciones; ley 1581 de 2012, que presenta la protección de datos personales, entre otras. En este aspecto se encuentra la necesidad de que las empresas realicen su proceso de certificación, teniendo en cuenta lo solicitado en la ISO/IEC 27001, y la ISO/IEC 27002. Lo anterior en aras de que se acrediten en ciberseguridad, bajo el marco de las normas internacionales.

Al desarrollar el proceso de caracterización de los procesos de ciberseguridad de activos digitales en empresas exportadoras de café en Colombia, es importante que permita conocer más acerca de la protección de la información sensible. Lo anterior como consecuencia de que este tipo de empresas se caracterizan por manejar información relacionada a los proveedores, clientes, transacciones, contactos, entre otros datos de naturaleza financiera. Por ende, una falla en los procesos de ciberseguridad podría generar robos de este tipo de información, lo que conllevaría a causar daños de índole económica y reputacional a la empresa.

De igual manera, también permite ahondar en el entendimiento de aspectos como el cumplimiento normativo de los procesos de ciberseguridad, la seguridad de la cadena de suministro a consecuencia de que, en el gremio del café, se encuentran involucradas una gran cantidad de actores, por ende, la ciberseguridad no solo protege a la empresa u organización como tal, también lo hace con los socios comerciales de estas, para garantizarles seguridad en la cadena de suministro.

Una de las características más notorias de la ciberseguridad, es que afecta directamente el campo reputacional de las empresas u organizaciones. Por lo anterior, los distintos clientes y socios buscan tener alianzas con empresas que realizan la protección de sus datos y activos digitales, debido a que al momento en que se presente un error en esos campos, se afectarían las relaciones comerciales, como también la confianza del consumidor.

Otro de los aspectos que permite esta caracterización, es la identificación de las diferentes vulnerabilidades, riesgos y amenazas presentes. Al momento en que se comprenden de forma profunda estos aspectos, las empresas se ven obligadas a desarrollar medidas de implementación proactivas para la prevención de ataques de origen cibernéticos, por medio de acciones como la compra de un software de seguridad, los procesos de capacitación del personal, y las políticas vinculadas a los accesos controlados.

Por último, el conocer cómo se dan los procesos de ciberseguridad de activos digitales en este tipo de empresas, fortalece campos como la resiliencia organizacional, el impulso a la innovación, y el crecimiento hacia el comercio electrónico, ejes fundamentales de la adaptación de las empresas al cambiante entorno comercial y tecnológico. Se considera que lo más importante de este proceso, es evidenciar la necesidad de que en estas empresas se desarrolle la ciberseguridad de los activos digitales, esto con el fin de evitar situaciones que podrían atentar contra la sostenibilidad de la misma.

En las empresas objeto de estudio se pudo evidenciar que campos como el conocimiento sobre los activos digitales, la evaluación de riesgos, las políticas y los protocolos de ciberseguridad, la capacitación y la concientización, las herramientas y las tecnologías, y por último, el cumplimiento normativo, se encuentran establecidas de manera muy incipiente en este sector empresarial, destacándose que en solo algunas empresas, todo lo vinculado a la ciberseguridad lo realizan para el marco de SCS BASC, y/o el SGCS Sistema de Gestión de Control y Seguridad.

Se hace necesario profundizar mucho más sobre el tema de la ciberseguridad en este sector económico, debido a que el presente trabajo de investigación se puede percibir como un punto de inicio para el posterior desarrollo de otras indagaciones, en aras de que la temática sea abordada desde un punto de mayor complejidad, y así abrir nuevos campos de conocimiento para el beneficio de las empresas, y de los estudiosos de la gestión de riesgo

REFERENCIAS

Aguilar, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior, *Estudios Internacionales,* (198), 169–197.

Auditool (2011, enero, 07). Control Interno. Auditool. https://www.auditool.org/blog/control-interno/importancia-de-la-administracion-de-riesgos

Caamaño, E. y Gil, R. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional, *NOVUM*, 1(10), 61 - 80. https://orcid.org/0000-0003-0280-1453

Cano, J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030, *Revista Científica General José María Córdova*, 20(40), 815–832. https://doi.org/10.21830/19006586.866

Concafé (2023, julio,23). El café de Colombia: Un tesoro cafetero que impulsa la economía y enamora los sentidos. Concafé. https://concafe.es/el-cafe-de-colombia-un-tesoro-cafetalero-que-impulsa-la-economia-y-enamora-los-sentidos/#:~:text=En%202020%2C%20las%20exportaciones%20de,la%20balanza%20comercial%20del%20pa%C3%ADs.

Digitalent Group (2023, diciembre, 14). Activos digitales: por qué son importantes para tu empresa. Digitalent Group. https://www.isdi.education/es/blog/activos-digitales-por-que-son-importantes-para-tu-empresa#:~:text=%C2%BFQu%C3%A9%20son%20los%20activos%20digitales,contextos%2C%20desde%20empresas%20hasta%20individuos.%C2%B4

Docusing (2021, marzo, 2). Archivo digital: 6 ventajas de utilizarlo. *Docusing https://www.docusign.com/es-mx/blog/archivo-digital*

Federación Nacional de Cafeteros de Colombia (2023). *Informe Mensual de Exportaciones.* Federación Nacional de Cafeteros de Colombia. https://federaciondecafeteros.org/app/uploads/2023/05/Informe-Expos-Abril.pdf

Fortinet (2024). Tríada CIA: confidencialidad, integridad y disponibilidad. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/cia-triad#:~:text=Las%20tres%20letras%20de%20la,significan%20confidencialidad%2C%20integridad%20y%20disponibilidad.

Hernández, R. Fernández, C. y Baptista, P. (2006). *Metodología de la Investigación*. 6ta edición. Ediciones Mc. Graw – Hill.

IBM (2023). ¿Qué es la ciberseguridad? IBM. https://www.ibm.com/es-es/topics/cybersecurity

IBM (2024). ¿Qué es el ransomware? IBM. https://www.ibm.com/es-es/topics/ransomware

Incibe (2020). *Glosario de términos de ciberseguridad.* Incibe. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Inprovider (2024, junio, 4). Archivo Digital: Cómo Gestionarlo. *Inprovider. https://blog.inprovider.com/archivo-digital*

ISDI Digitalent Group (2023, diciembre, 14). Activos digitales: por qué son importantes para tu empresa. *ISDI Digitalent Group*, https://www.isdi.education/es/blog/activos-digitales-por-que-son-importantes-para-tu-empresa

Martin, S. (2024, junio,05). Gestión del Riesgo. Comunicación y medios para la prevención y la mitigación de desastres en América Latina. *Comminit.* https://www.comminit.com/gestion-del-riesgo/content/stephanie-l-martin

Policía Nacional de Colombia (2020). *Tendencias del cibercrimen en Colombia 2019 -2020.* Policía Nacional de Colombia. file:///C:/Users/T/Desktop/Cyber/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Revista Portafolio (2015, junio, 04). Sector cafetero se enfrenta a un grave problema. ¿Cuál es? *Revista Portafolio*. https://www.portafolio.co/economia/finanzas/sector-cafetero-enfrenta-grave-problema-40414

Saavedra, B. (2023). *Desafíos y Amenazas a la Seguridad en América Latina*. Paul Eduardo Vera. Coordinador. Centro de Estudios Estratégicos del Ejército del Perú / Strategic Studies Institute - U.S. Army War College / Centro de Estudios Hemisféricos de Defensa William J. Perry.

SafetyCulture (2024, junio,29). ¿Qué es la gestión de riesgos?. *SafetyCulture. https://safetyculture.com/es/temas/gestion-de-riesgos/*

Teijeiro, L. (2023). Principales herramientas de ciberseguridad. Tokio School. https://www.tokioschool.com/noticias/herramientas-ciberseguridad/

Vida Fernández, J. (2022). La gobernanza de los riesgos digitales: Desafíos y avances de la regulación de la inteligencia artificial, *Cuadernos de derecho transaccional, 14*, (1). 498-503. https://heinonline.org/HOL/LandingPage?handle=hein.journals/cudetns14&div=25&id=&page=

Zendesk (2024, marzo,01). ¿Qué es la ciberseguridad y cuál es su relación con la IA? Zendesk. https://www.zendesk.com.mx/blog/ciberseguridad/

ANEXO A

ENTREVISTA SEMIESTRUCTURADA PARA LA CARACTERIZACIÓN DE LOS PROCESOS DE CIBERSEGURIDAD DE ACTIVOS DIGITALES EN EMPRESAS EXPORTADORAS DE CAFÉ

Cordial saludo, en la siguiente entrevista se manejarán aspectos vinculados a la ciberseguridad de activos digitales en empresas exportadores de café. Por favor, le solicitamos su valiosa colaboración respondiendo de manera honesta estas preguntas. ¡Muchas gracias!

Nombre de la empresa: _____

Años de funcionamiento: _____

Tipo de empresa: _____

¿Conoce qué es un activo digital? (Activos Digitales)

SI _____

NO _____

Solo en caso de una respuesta positiva, por favor diligenciar las siguientes preguntas:

¿Qué tipos de activos digitales se manejan en esta empresa? (Activos Digitales)

_____
_____
_____
_____
_____
_____
_____
_____

¿Cuál es el proceso de gestión y almacenamiento que realiza la empresa de estos activos digitales? (Activos Digitales)

_____
_____
_____
_____
_____
_____

_____
_____

¿Realizan las evaluaciones de riesgo en lo correspondiente a la ciberseguridad? (Evaluación de Riesgos)

SI _____

NO _____

Solo en caso de una respuesta positiva, por favor diligenciar las siguientes preguntas:

¿Cuál es la frecuencia con la cual se realizan estas evaluaciones de riesgo? , ¿Estas evaluaciones son cualitativas o cuantitativas?(Evaluación de Riesgos)

_____
_____
_____
_____
_____
_____
_____
_____

¿Cuáles han sido los principales riesgos cibernéticos identificados en la operación de esta empresa? (Evaluación de Riesgos)

_____
_____
_____
_____
_____
_____
_____
_____

¿Se cuenta con políticas formales de ciberseguridad? (Políticas y Protocolos de Ciberseguridad)

SI _____

NO _____

Solo en caso de una respuesta positiva, por favor diligenciar las siguientes preguntas:

¿Cuáles son los aspectos que abarcan estas políticas? (Políticas y Protocolos de Ciberseguridad)

_____
_____
_____
_____
_____
_____
_____
_____

¿Existen en la empresa protocolos definidos para el manejo de incidentes de ciberseguridad? (Políticas y Protocolos de Ciberseguridad)

_____
_____
_____
_____
_____
_____
_____
_____

¿Se realizan capacitaciones sobre temas en ciberseguridad para el personal? (Capacitación y Concientización)

SI _____

NO _____

Solo en caso de una respuesta positiva, por favor diligenciar las siguientes preguntas:

¿Cuál es la frecuencia de estas capacitaciones y qué temas se tratan? (Capacitación y Concientización)

_____
_____
_____
_____
_____
_____
_____
_____

¿Cuáles son las acciones con las cuales se fomenta la cultura de la ciberseguridad dentro de esta empresa? (Capacitación y Concientización)

¿Cuáles son las herramientas de ciberseguridad que se utilizan en esta empresa? (Herramientas y Tecnologías)

¿Durante el proceso de exportación se realiza la implementación de tecnologías concretas para la protección de los activos digitales? (Herramientas y Tecnologías)

¿Cumple con alguna normativa relacionada a la ciberseguridad? (Cumplimiento Normativo)

_____
_____
_____
_____

¿Por medio de qué procesos se verifica el cumplimiento de esta normativa? (Cumplimiento Normativo)

_____
_____
_____
_____
_____
_____
_____
_____

¿Tiene algo más para agregar sobre los procesos de ciberseguridad en esta empresa?

_____
_____
_____
_____
_____
_____
_____
_____

Agradeciendo su tiempo y colaboración.

ANEXO B. GLOSARIO DE TÈRMINOS

Backup offline: Copia de seguridad sin conexión.

Cloud: Nube, espacio virtual para guardar información.

Drive: Lugar que se constituye de una plataforma gratis, en la que se pueden almacenar archivos y acceder a ellos desde cualquier lugar de la nube.

Fishing: (Pescar), es la técnica que es utilizada por los ciberdelincuentes para lanzar anzuelos a sus víctimas y esperar a que alguien caiga en ello.

SCS BASC: (Business Alliance for Secure Commerce): Es una apuesta de naturaleza internacional, que tiene como objetivo el fomento de la seguridad en las cadenas de suministros y en el comercio internacional.